

University of Mississippi

eGrove

Guides, Handbooks and Manuals

American Institute of Certified Public
Accountants (AICPA) Historical Collection

2006

CPA's handbook of fraud and commercial crime prevention

Tedd Avey

Ted Baskerville

Alan Brill

Follow this and additional works at: https://egrove.olemiss.edu/aicpa_guides



Part of the [Accounting Commons](#), and the [Taxation Commons](#)

Recommended Citation

Avey, Tedd; Baskerville, Ted; and Brill, Alan, "CPA's handbook of fraud and commercial crime prevention" (2006). *Guides, Handbooks and Manuals*. 821.

https://egrove.olemiss.edu/aicpa_guides/821

This Book is brought to you for free and open access by the American Institute of Certified Public Accountants (AICPA) Historical Collection at eGrove. It has been accepted for inclusion in Guides, Handbooks and Manuals by an authorized administrator of eGrove. For more information, please contact egrove@olemiss.edu.

The CPA's Handbook of
Fraud
and
Commercial Crime
Prevention

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

**The CPA's Handbook of Fraud
and Commercial Crime Prevention**

AICPA

AICPA

Tedd Avey, CPA, CA • Ted Baskerville, CA • Alan Brill, CISSP

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

The CPA's Handbook of
Fraud
and
Commercial Crime
Prevention

AICPA

Tedd Avey, CPA, CA • Ted Baskerville, CA • Alan Brill, CISSP

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

**The CPA's Handbook of
Fraud
and
Commercial Crime
Prevention**

Tedd Avey, CPA, CA•IFA, CFE • Ted Baskerville, CA•IFA, CFE • Alan Brill, CFE, CISSP

AICPA

NOTICE TO READERS

The CPA's Handbook of Fraud and Commercial Crime Prevention does not represent an official position of the American Institute of Certified Public Accountants, and it is distributed with the understanding that the authors and publisher are not rendering legal, accounting or other professional services in this publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2000, 2001, 2002, 2003, 2004, 2005, and 2006 by
American Institute of Certified Public Accountants, Inc.
New York, NY 10036-8775

First edition published March 2000. Sixth revision, November 2006.

All rights reserved. Checklists and sample documents contained herein may be reproduced and distributed as part of professional services or within the context of professional practice, provided that reproduced materials are not in any way directly offered for sale or profit. For information about the procedure for requesting permission to make copies of any part of this work, please visit www.copyright.com or call (978) 750-8400.

1 2 3 4 5 6 7 8 9 0 PP 0 9 8 7 6

Table of Contents

Preface

Acknowledgments

About the Authors

- 1 Managing the Risk of Fraud**
 - 1.1 The Nature and Extent of Fraud
 - 1.2 Fraud Risk Factors
 - 1.3 Internal Controls and “Fraud-Proofing”
 - 1.4 Detecting and Preventing Fraud in Books of Account
 - 1.5 A New Environment for Fraud Risk Detection and Enforcement
 - 1.6 Risk Management Checklist

- 2 Promoting an Ethical Environment**
 - 2.1 Ethics: A Framework
 - 2.2 Ethical Environment Checklist

- 3 Insurance Against Fraud**
 - 3.1 Financing the Risk of Fraud
 - 3.2 Fraud Insurance
 - 3.3 Important Provisions in Commercial Crime Policies
 - 3.4 Insured’s Responsibilities in the Event of a Loss
 - 3.5 The Insurer
 - 3.6 Fraud Insurance Checklist

- 4 Computer Security and System Recovery**
 - 4.1 The Role of Computers in Modern Corporations
 - 4.2 Management’s Security Issues
 - 4.3 Physical Security
 - 4.4 Logical Security
 - 4.5 System Recovery

-
- 4.6 Management's Responsibilities in a Security Program
 - 4.7 Computer Security Checklist


 - 5 Internal Fraud**
 - 5.1 Asset Misappropriation from Within
 - 5.2 Sales and Collection Cycle
 - 5.3 Acquisition and Payment Cycle
 - 5.4 Payroll and Personnel Cycle
 - 5.5 Inventory and Warehousing Cycle
 - 5.6 Capital Acquisition and Repayment Cycle
 - 5.7 Cash Misappropriation

 - 6 External Fraud for Personal Gain**
 - 6.1 Fraud Perpetrated by Outsiders
 - 6.2 Individuals Versus Individuals and Corporations
 - 6.3 Individuals Versus the Government
 - 6.4 Individuals Versus Financial Institutions
 - 6.5 Individuals Versus Insurance Companies

 - 7 Commercial Crime**
 - 7.1 Overview
 - 7.2 Forms of Commercial Crime
 - 7.3 Prevention of Commercial Crime

 - 8 Computer Crime and Computer Criminals**
 - 8.1 Overview
 - 8.2 Computer-Related Crimes
 - 8.3 A Brief History of Computer Crime
 - 8.4 Computer Crime Today
 - 8.5 Fraud and the Internet
 - 8.6 Computer Criminal Profiles
 - 8.7 Controls for Preventing and Detecting Computer Crime
 - 8.8 Computer Fraud, Computer Evidence, and the Science of Computer Forensics

-
- 8.9 Selected Computer Crimes
 - 8.10 Conclusion
 - 8.11 Computer Crime Checklists
- 9 Dealing With a Known or Suspected Fraud**
- 9.1 Overview
 - 9.2 The Five-Step Investigative Approach
 - 9.3 Forensic Accountants
 - 9.4 Dealing With a Known or Suspected Fraud Checklist
- 10 Reducing the Risk of Financial Statement Fraud**
- 10.1 The Pervasive Nature of Financial Statement Fraud
 - 10.2 Kinds of and Motives for Financial Statement Fraud
 - 10.3 Special Areas of Financial Statement Fraud
 - 10.4 Predictors of Financial Statement Fraud
 - 10.5 Regulatory Responses to Financial Statement Fraud
 - 10.6 Audit Deficiencies and Audit Failures
 - 10.7 Guidance for Auditors
 - 10.8 Checklist: Detection of Financial Statement Fraud
 - 10.9 Checklist: Sarbanes-Oxley
- 11 Corporate Security: Threat and Crisis Management**
- 11.1 Overview
 - 11.2 The Threat
 - 11.3 Planning and Prevention
 - 11.4 Crisis Management
 - 11.5 Corporate Security Checklists
 - 11.6 The Kroll October 2001 Survey on Security Risk Management
- 12 Bankruptcy Fraud**
- 12.1 Overview
 - 12.2 The Bankruptcy Process
 - 12.3 Fraud in Bankruptcy Filings
 - 12.4 Elements of Bankruptcy Fraud

- 
- 12.5 Kinds of Bankruptcy Fraud
 - 12.6 Punishment Provisions
 - 12.7 Referral of Bankruptcy Fraud
 - 12.8 Bankruptcy Fraud Checklist

13 Detecting Procurement Fraud

- 13.1 Understanding the Procurement Process
- 13.2 Screening Procurement Contracts
- 13.3 Scrutinizing Suspect Procurement Contracts
- 13.4 In-Depth Examination of Suspect Procurement Contracts
- 13.5 Reporting Fraud in Procurement Contracts

14 Identity Theft and Corporate Identity Fraud

- 14.1 Introduction
- 14.2 Laws to Combat Identity Theft
- 14.3 How Thieves Steal Your Identity
- 14.4 Personal Identity Theft
- 14.5 Corporate Identity Theft
- 14.6 Cyber Identity Theft
- 14.7 Conclusion
- 14.8 Checklist: Detection of Personal Identity Theft and Corporate Identity Fraud

Fraud Sector-by-Sector (See *Fraud Prevention Checklists CD-ROM 2006-2007*)

Statement on Auditing Standards (SAS) No. 99, Consideration of Fraud in a Financial Statement Audit (See *Fraud Prevention Checklists CD-ROM 2006-2007*)

Glossary

Bibliography (Suggested References)

Fraud Prevention Checklists CD-ROM

Contents

*The CD Toolkit includes Checklists corresponding to the following Chapters.
The files on the CD are labeled by Chapter, for easy reference.*

Chapter 1: Risk Management Checklist

Chapter 2: Ethical Environment Checklist; Sample Mission Statement; Sample Organizational Code of Conduct

Chapter 3: Fraud Insurance Checklist

Chapter 4: Computer Security Checklist

Chapters 5, 6, and 7 do not have any corresponding Checklists.

Chapter 8: Computer Crime Checklists (Evaluating a Company's Data Management Policies; Evaluating the Corporate Environment for Computer-Crime-Friendly Characteristics; and the State of Authentication Checklist); Sarbanes-Oxley and Internal Control Over IT

Chapter 9: Dealing With a Known or Suspected Fraud Checklist

Chapter 10: Detection of Financial Statement Fraud Checklist; Sarbanes-Oxley Checklist

Chapter 11: Corporate Security Checklists (Comprehensive Risk Assessment; Threat and Crisis Management; and Financial Issues to Address When Disaster Strikes)

Chapter 12: Bankruptcy Fraud Checklist; Exhibit A—Bankruptcy Schedules (PDF); Exhibit B—Proof Claim Form; Exhibit C—Bankruptcy Referral Letter

Chapter 13: Procurement Fraud Checklist

Chapter 14: Detection of Personal Identity Theft and Corporate Identity Fraud Checklist

Industry Sector-by-Sector Checklists:

- Construction
- Financial Services
- Government
- High Technology
- Manufacturing
- Media and Communications
- Nonprofit
- Professional Services
- Real Estate
- Recreation
- Natural Resources
- Retail
- Small Business

- Transportation
- Wholesale
- Brokers and Dealers
- Employee Benefit Plans
- Health Care Organizations
- Insurance Companies
- Investment Companies

Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (PDF file of SAS, plus additional information).

Fraud Resources

This folder contains a number of practical tools to assist with fraud-related issues in business—from planning an ethics training program, to implementing privacy policies and procedures using the AICPA/CICA Privacy Framework.

Ethics and Fraud in Business. This folder contains four expert commentaries to serve as guidance to other CPAs.

- **Resource 1:** Implementing An Ethics Strategy
- **Resource 2:** Designing An Ethics Training Program
- **Resource 3:** AICPA/CICA Privacy Framework (Including the AICPA/CICA Trust Services Privacy Principle and Criteria)
- **Resource 4:** Evaluating the Independent Auditor: Questions to Consider

Fraud in Business: *Cases*. This folder includes 16 cases depicting a range of fraudulent schemes and behaviors.

Internet Fraud Resources. This folder includes four files containing additional fraud resources, internet links and other valuable information.

- **Resource 5: Management Override of Internal Controls: *The Achilles' Heel of Fraud Prevention***—A report from the members of the AICPA's Antifraud Programs and Controls Task Force.
- **Resource 6: Audit Risk Alert Highlights (2005–2006).**
- **Resource 7: AICPA Antifraud & Corporate Responsibility Center**—This resource center will give you the tools and information you need to combat fraud—whatever your role in the business community.
- **Resource 8: AICPA's Audit Committee Effectiveness Center**—A key element in the corporate governance process of any organization is its audit committee. The AICPA's *Audit Committee Effectiveness Center* provides additional guidance and tools to make audit committee best practices actionable.

PREFACE

The CPA's Handbook of Fraud and Commercial Crime Prevention (the Fraud Handbook or *Handbook*) is the new model for every company. The *Handbook* provides CPAs with practical information, checklists, and examples to help identify and respond to fraud in the workplace. Although it is impossible to eliminate the risk of fraud completely, effective prevention policies and internal controls can reduce opportunities for fraud to occur. At the same time, the adoption of easy to implement detection methods can help uncover fraud in the early stages, minimize losses, and enable those affected by fraud, particularly CPAs or financial managers responsible for fraud prevention, to react to fraud in a way that could solve or mitigate the problem rather than contributing to it.

FRAUD HANDBOOK

The focus of this *Handbook* is fraud prevention and it is written by CPAs for CPAs. The authors, each having nearly 40 years of insight and practical experience developing and implementing fraud prevention and detection programs throughout the world, have combined their expertise in specialized areas to write what many consider to be the paradigm of fraud prevention guidance. Since prevention cannot be realized without understanding how fraud is perpetrated and concealed, the material in this *Handbook* has been written to explain to CPAs the nature and extent of fraud and to provide fraud prevention techniques. In addition to the core topics of fraud prevention and methods of combating specific kinds of fraud, two chapters are devoted to computer security and the unique kinds of crimes and criminals related to computer crimes.

This *Handbook* has been carefully designed to address not only the “whys” or reasons that fraud exists, but also the “hows” or the methods by which fraud takes place. The *Fraud Handbook* provides invaluable guidance and tools for preventing fraud from ever occurring in the first place. Highlights of the *Handbook's* coverage are outlined below.

Managing the Risk of Fraud (*Chapter 1*)

Chapter 1 describes fraud risk: understanding it and guarding against the threat posed by it. The specific factors that affect fraud risk are addressed, including the key internal controls—basic, supervisory and audit—that help prevent fraud. Since detecting and preventing fraud in books of account is key to any prevention strategy, there is a section devoted exclusively to this topic, with fraud and AICPA Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 316), covered in relation to fraud auditing.

A comprehensive and practical “Risk Management Checklist” is included at the end of the chapter with specific risk factors as they relate to internal control.

Promoting an Ethical Environment (*Chapter 2*)

Because an ethical environment is a key element in any effective prevention strategy, this chapter includes the steps that can be taken to promote an ethical environment within an organization, and thereby reduce the risk of fraud. A sample code of ethics and business conduct, which can be

reproduced and/or adapted for use in any organization, is included on the CD-ROM, along with an ethical environment checklist.

Insurance Against Fraud (formerly Risk Financing and Fidelity Insurance) *(Chapter 3)*

Risk management is a key component of fraud awareness and is essential for providing protection against potentially catastrophic risks, including fraud-related losses. Every organization must identify its risks and implement a strategy that balances the cost of potential losses with the cost of an acceptable level of risk management. Chapter 3 examines risk financing and reviews the kinds of insurance coverage generally available against employee fraud and dishonesty. It also highlights some of the issues found in insurance policies, common exemptions, and some of the important duties of the insured.

In addition, the chapter provides a step-by-step guide to making a claim after the discovery of the dishonest act. A "Fraud Insurance Checklist" is included as well.

Computer Security and System Recovery *(Chapter 4)*

Adequate computer security is an indispensable fraud prevention tool. Chapter 4 provides a comprehensive overview of computer security, including physical security, logical security, and system recovery. A checklist is also included with this chapter.

Internal Fraud *(Chapter 5)*

Chapter 5 addresses the various ways fraud is committed against an organization by a perpetrator from within that organization, meaning, by officers, managers, or employees—the most common form of fraud. Frauds are classified according to the various accounting cycles to which they relate: sales and collection, acquisition and payment, payroll and personnel, inventory and warehousing, and capital acquisition and repayment. Since cash is the focal point of most entities, a separate section is devoted to cash misappropriation.

External Fraud for Personal Gain *(Chapter 6)*

Fraud can also be committed against organizations by suppliers, professional con artists, and other outside perpetrators. Chapter 6 covers the various ways frauds are committed against small businesses and individuals, the government, and financial institutions, such as banks and insurance companies. Case studies are included to clarify the various kinds of fraud perpetrated by outsiders.

Commercial Crime *(Chapter 7)*

In addition to being victimized by fraud, organizations can also be the perpetrators of fraud. Chapter 7 provides the various forms of commercial crime and methods of preventing them. The crimes considered include false advertising, industrial espionage and trade secret theft, insider trading, securities fraud, organizational bribe giving. Interesting and informative case studies are included to exemplify the different kinds of commercial crime.

Computer Crime and Computer Criminals (*Chapter 8*)

Although it has created very few genuinely “new” frauds, the computer has dramatically changed the environment in which fraud is committed. Chapter 8 describes the nature of computer crimes and computer criminals and details the controls that prevent and detect computer fraud. The chapter includes a comprehensive discussion of the role and responsibility of IT to ensure compliance with the Sarbanes-Oxley Act of 2002 and how the COSO framework is integral to meeting SOX requirements. The section, “Fraud and the Internet” describes the characteristics of the Internet that make it an inadvertent facilitator of fraud as well as steps to take to avoid being victimized. The topic of computer forensics and making the best use of it in investigations is covered. A “Computer Crime Checklist” and a “Sarbanes-Oxley and Internal Control Over IT Checklist” appear at the end of the chapter.

Dealing With a Known or Suspected Fraud (*Chapter 9*)

Chapter 9 familiarizes CPAs with forensic accounting and the techniques of fraud investigation. Beginning with the fundamental concepts of forensic accounting, this chapter details a straight forward five-step investigative process and also provides interview techniques and guidance on how to conduct them—to help CPAs understand the role of forensic accountants and others involved in fraud investigations. A comprehensive checklist of steps to be followed in a fraud investigation is included at the end of the chapter.

Reducing the Risk of Financial Statement Fraud (*Chapter 10*)

The costs of financial statement fraud have been realized with the revelations in the marketplace and the media that once respected companies (and the darlings of Wall Street) were built on fraudulent manipulation of their financial statements. The resulting aftermath has included stock market upheaval, huge financial losses for investors and employees, and additional oversight demands and actions from regulatory agencies. The costs of financial statement fraud have never been more in focus than now.

In today’s business environment, it is more important than ever for financial professionals to understand financial statement fraud and how it might be used to deceive boards of directors and audit committee members, senior management, auditors, and investors.

Chapter 10 focuses on the pervasive nature and special areas of financial statement fraud, including, COSO’s Internal Control—Integrated Framework, preventive and detective controls under Sarbanes-Oxley, typical frauds related to misappropriation of assets, example audit procedures, the impact of SAS 99, and the new regulatory environment. A comprehensive Financial Statement Fraud Checklist and Sarbanes-Oxley Checklist are included at the end of the chapter.

Corporate Security: Threat and Crisis Management (*Chapter 11*)

Although most corporations have formal plans for fire and systems disasters, many would be forced to improvise if confronted by an emergency, whether man made or natural. Chapter 11 identifies the types of threats a business faces and addresses the primary issues involved in preventing or detecting such threats. Since there are certain threats that no plan can anticipate, this chapter also includes emergency, business resumption, and physical security planning. This comprehensive chapter concludes with a useful checklist.

Bankruptcy Fraud (Chapter 12)

For CPAs to understand bankruptcy fraud, it is necessary to understand the bankruptcy process. Chapter 12 begins with a discussion of insolvency, the filing process and the bankruptcy petition, then identifies fraud in bankruptcy filings, provides thorough descriptions of the elements of bankruptcy fraud and details various kinds of bankruptcy fraud. In addition, this invaluable chapter discusses punishment provisions and the necessity of the mandatory referral report. The comprehensive checklist at the end of the chapter is organized according to elements and kinds of bankruptcy fraud. Selected bankruptcy forms are available on the *Fraud Prevention Checklists CD-ROM*.

Detecting Procurement Fraud (Chapter 13)

Procurement fraud is one of the most difficult white-collar crimes to detect. All too many companies refuse to entertain the thought that their team of loyal employees could harbor fraudsters. When fraud strikes, the management team is taken by surprise. Regrettably, it is only after the insurance company has refused to pay the employee fidelity claim, that it decides to implement tighter controls and actively seek to deter fraud among its employees. Much of the damage caused by procurement fraud can be easily combated by separation of employee duties coupled with surprise audits and continuing management oversight.

Chapter 13 provides the specific tasks and controls needed to combat it: Procurement Fraud Detection and Investigation, Screening Procurement Contracts, In-depth Examination of Suspect Procurement Contracts, and Reporting Fraud in Procurement Contracts. The chapter includes red flags in various areas under scrutiny. The chapter concludes with a Procurement Fraud Checklist.

Identity Theft and Corporate Identity Fraud (Chapter 14)

Identify theft is touted as “. . . A Critical National and Global Threat.” According to the FTC the most common cases of ID theft involved credit card fraud, followed by phone or utility fraud; bank fraud; employment-related fraud; government document or benefit fraud and loan fraud. It is a growing problem both for consumers and businesses. Chapter 14 is a practical guide to ID theft. The Appendix offers a useful checklist to detect personal and corporate identity theft and fraud.

Though fraud experts estimate that more than 75 percent of frauds are undetected, it's difficult to reach a precise number because fraud not only evades detection by company management, but also goes unreported or underreported in many instances. Companies do not disclose their losses resulting from fraud for many reasons, including that they are embarrassed that they have been defrauded, or they want to keep the bad news from investors, clients, and customers.

It is with this in mind that the *Fraud Handbook* is written. Perhaps because fraud is so under reported, many companies think it will never happen to them. Unfortunately, an organization unwilling to consider that its personnel, agents, or vendors could act dishonestly is a fraudster's dream. What better environment to exploit than one in which your guard is down?

The *Fraud Handbook* is an invaluable, practical guide to assist you in preventing fraud from ever occurring in the first place.

FRAUD SECTOR-BY-SECTOR (*See Fraud Prevention Checklists CD-ROM*)

This comprehensive section outlines a breakdown of fraud in the different sectors, complete with checklists and fraud vulnerability grids for each of the following sectors:

- Construction
- Financial services
- Government
- High technology
- Manufacturing
- Media and communications
- Nonprofit
- Professional services
- Real estate
- Recreation
- Natural resources
- Retail
- Small business
- Transportation
- Wholesale
- Brokers and Dealers
- Employee Benefit Plans
- Health Care Organizations
- Insurance Companies
- Investment Companies

STATEMENT ON AUDITING STANDARDS (SAS) NO. 99, *Consideration of Fraud in a Financial Statement Audit* (*See Fraud Prevention Checklists CD-ROM*)

The complete text version of the current SAS No. 99 is provided on the *Fraud Prevention Checklists CD-ROM 2006–2007* included with the *Handbook*. SAS No. 99 is provided in portable document format (PDF) and is readable with Adobe Acrobat Reader. You can download the reader from <http://www.adobe.com/products/acrobat/readstep.html> if you do already have it installed on your computer.

BIBLIOGRAPHY (SUGGESTED REFERENCES)

This alphabetical listing of the most current and relevant sources of information, including a separate section for Web sites and books, pertaining to fraud, commercial crime, and other closely related topics is included for further reading.

GLOSSARY

The comprehensive glossary is an effective quick-reference tool that provides an alphabetically arranged listing of definitions and explanations for all fraud-related terms and kinds of fraud.

ACKNOWLEDGMENTS

The CPA's Handbook of Fraud and Commercial Crime Prevention is the work of many individuals. The authors would especially like to thank Paul Dopp, Pat Woytek, Kip Hamilton, Todd Horn, Dave Iverson, Tae Kim, Ron Gélinas, Angela Fernandes, and all the others at Kroll Inc. for their assistance.

We wish to extend a special thanks to the Editor of this *Handbook*, Patricia M. Adamson, MA, MIST, of Kroll, for her editing of the original version and the annual updates.

We would also like to acknowledge the Canadian Institute of Chartered Accountants and, in particular, Peter Hout, who was responsible for overseeing the development and publication of *The Accountant's Handbook of Fraud and Commercial Crime*, on which this *Handbook* is based.

We are grateful to a long list of other individuals and companies who assisted in either the creation or the annual updating of this *Handbook*, including Joe Wells and the Association of Certified Fraud Examiners, and Michael J. Ramos.

ABOUT THE AUTHORS

Tedd Avey, BComm, CPA, CA•IFA, CFE. For almost thirty years, Tedd's name has been synonymous with forensic and investigative accounting, the very profession he helped to develop and grow. In 1976, he co-founded the first Canadian partnership devoted exclusively to forensic and investigative accounting. Since then, he has presided over some of the most important national and international fraud investigations of the last quarter century. He has written numerous articles and books on the subject, including co-authoring *The Accountant's Handbook of Fraud and Commercial Crime*, and *The CPA's Handbook of Fraud and Commercial Crime Prevention*, a publication of the American Institute of Certified Public Accountants. Tedd's practice is focused primarily on complex and large-scale corporate investigations and commercial litigation throughout Canada, the United States, Europe, and the Middle East, and includes cases ranging from several million to hundreds of millions of dollars. Tedd is an accomplished speaker and seminar leader on fraud detection and prevention to accountants and law enforcement personnel throughout North America and major cities around the world.

Tedd co-authored the foundation chapters of this *Handbook*.

Ted Baskerville, BA, CA•IFA, CFE, is a Principal in the Toronto office of Kroll Inc. For more than 20 years, Ted has provided risk management, forensic accounting, and litigation support to clients in a wide range of industries and all levels of government throughout North America, Europe, the Middle East and Asia. From 1998 to 2003, Ted was head of the Forensic Accounting Practice of Kroll Lindquist Avey, a division of Kroll Inc., covering the United Kingdom and Europe from the London office. Ted has conducted hundreds of investigations into corporate fraud, money laundering, false insurance claims and regulatory violations as well as employee dishonesty, secret commissions, and other forms of management and employee corruption. He is a well-respected consultant in civil litigation and arbitration cases involving loss of income, partnership and shareholder disputes, breach of contract, breach of fiduciary duty, insurance claims for employee dishonesty, and civil fraud. He has qualified as an expert witness in proceedings in the United Kingdom, the Island of Jersey, Canada, Austria, and Singapore. Ted has presented seminars on fraud awareness, insurance claims, and investigative accounting techniques to the insurance and financial services industries, the legal and corporate communities, law enforcement personnel, members of government ministries, accounting groups, and other professional associations.

Ted authored the Manufacturing and Natural Resources chapters in the Fraud Sector-by-Sector section, co-authored Chapter 3, Insurance Against Fraud, and sections on the Sarbanes-Oxley Act of 2002 and internal control.

Alan Brill, BA, MBA, DPS (ABD), CFE, CISSP, is Senior Managing Director at Kroll Ontrack, the technology services unit of Kroll Inc. Alan founded the High Tech Investigations and Computer Forensic Group worldwide of Kroll. He has an international reputation in the areas of computer and communication security, and technology-crime investigation. His work has ranged from major information security reviews for multi-billion dollar corporations, to criminal investigations of computer hackers and computer-facilitated frauds. He and his team consult with financial institutions and corporations to apply their knowledge of what *really* goes wrong in information security to help prevent security incidents. Alan is a frequent speaker at conferences and has

been featured in both print and broadcast media. He has written books and articles and has been called as an expert witness in numerous computer forensic cases.

Alan authored Chapter 4, Computer Security and System Recovery, and Chapter 8, Computer Crime, Computer Criminals and Computer Evidence.

Paul Dopp, CPA, CGA, CFE, a Principal of Tauber & Balsler, P.C., an Atlanta-based CPA firm, has more than twenty years' experience in forensic and investigative accounting, corporate investigations, litigation support and due diligence services, with his case experience including civil, criminal and regulatory matters. Paul has significant international engagement experience, having conducted forensic accounting assignments in Canada, the U.S., the Caribbean, and Asia. He has given presentations to professional organizations and law enforcement personnel regarding the investigative issues of fraud and white collar crime and has written articles on forensic accounting related topics, such as procurement fraud and electronic fraud.

Paul co-authored Chapter 1, Managing the Risk of Fraud and Chapter 13, Detecting Procurement Fraud.

Hazel de Burgh, BMath, CA•IFA, CFE, is a Principal of Kroll Inc. in Toronto. Hazel has worked exclusively in forensic and investigative accounting since 1986 focusing on commercial litigation and corporate investigations, many of which have involved multi-million dollar cases. Hazel's areas of expertise include procurement fraud, asset tracing and the assessment of financial issues in complex commercial litigation. Hazel has led numerous presentations on these and other forensic accounting topics to internal audit professionals, corporate executives, lawyers and law enforcement personnel. In addition to writing articles for various trade publications, Hazel co-wrote a manual on procurement fraud.

Hazel authored Chapter 11, Corporate Security: Threat and Crisis Management, and co-authored Chapter 13, Detecting Procurement Fraud.

Lynford Graham, CPA, PhD, CFE is a consultant in accounting and auditing matters and audit methodology located in Short Hills, New Jersey. With more than 25 years of public accounting experience in audit practice and National policy development groups, he was formerly a Partner and the Director of Audit Policy for BDO Seidman, LLP, and was a National Accounting & SEC Consulting Partner with Coopers & Lybrand, responsible for the technical issues research function and database, auditing research, audit automation and audit sampling techniques. Prior to joining BDO Seidman LLP, Dr. Graham was an Associate Professor of Accounting and Information Systems and a Graduate Faculty Fellow at Rutgers University in Newark, New Jersey. Dr. Graham is a recent past member of the AICPA Auditing Standards Board. He is a Certified Fraud Examiner and a member of the Association of Certified Fraud Examiners. His numerous academic and business publications span a variety of topical areas including information systems, internal controls, expert systems, audit risk, audit planning, fraud, sampling, analytical procedures, audit judgment and international accounting and auditing. Dr. Graham holds an MBA in Industrial Management and Ph.D. in Business and Applied Economics from the University of Pennsylvania, (Wharton School).

Lyn provided technical updates to Chapters 1, 8, and 10.

David Harwood, CA•CIRP, is a Principal in the Toronto office of Kroll Zolfo Cooper LLC, a division of Kroll Inc. David is both a Licensed Trustee in Bankruptcy and a Chartered Insolvency and Restructuring Practitioner with more than twenty years' experience in the turnaround and

restructuring field. During his career, David has negotiated with creditors, performed loan analyses, reorganized operations in preparation for sale and seen companies through the courts under the Companies' Creditors Arrangement Act. Much of his international practice has focused on developing strategies for restructuring government financial institutions and organizing bailouts for private institutions in trouble following the collapse of the national currency.

David co-authored Chapter 12, Bankruptcy Fraud.

William (Bill) L. Jennings, BS, CPA, CFE, is also a licensed Private Detective. Bill has more than twenty years' experience investigating fraud and other financial crimes, forensic accounting, business-controls development, public accounting and auditing. His case experience includes investigations of securities fraud, embezzlement, commodities fraud, bank fraud, money laundering, health care fraud, drug theft, equipment theft, purchasing fraud, theft by conversion, and public corruption for corporations, attorneys, the U.S. Justice Department, and state and local prosecutors. Bill writes articles and speaks regularly on fraud topics and other white-collar crime prevention and detection. Bill authored Chapter 3, Promoting an Ethical Environment, and co-authored both Chapter 10, Reducing the Risk of Financial Statement Fraud and Chapter 12, Bankruptcy Fraud.

David H. Judd, BS, CPA, is a Partner with Neilson Elggren LLP and former Partner of Arthur Andersen LLP. He has more than twenty years' experience in public accounting, specializing in bankruptcy, litigation services, and investigative accounting. David's casework has focused on bankruptcy matters for both Chapter 7 and Chapter 11 filings, which includes services as trustee, accountants for the trustee, court-appointed examiner, accountants for the examiner and accountants for the creditors. In addition, David has performed investigative accounting services relating to fraud, embezzlement, and mismanagement, and has provided expert witness testimony. David co-authored Chapter 12, Bankruptcy Fraud.

Todd Neilson, BS, CPA, is a founding Partner of Neilson Elggren LLP, and former Partner of Arthur Andersen LLP. He is one of the nation's foremost experts on bankruptcy and investigative accounting with more than twenty-five years' combined experience in public, private and government accounting. He also served as a Special Agent with the FBI, where he specialized in accounting investigation of white-collar and organized crime. Due to his unique expertise, Todd has been called as an expert witness in numerous forensic accounting and fraud litigation cases. Todd is much in demand as a speaker and seminar leader on fraud and bankruptcy-related topics. In addition to co-authoring the AICPA Consulting Services Practice Aid "Providing Bankruptcy and Reorganization Services", Todd has written articles for professional journals such as *Bankruptcy Litigation Counselor*.

Todd co-authored Chapter 12, Bankruptcy Fraud.

Pamela J. Parizek, JD, has more than 12 years' experience as a lawyer in the private sector, as a regulator in the enforcement division of the US Securities and Exchange Commission, and as a manager in a major international accounting firm. She has managed complex cases and investigations involving the antifraud, books and records, and internal control provisions of US securities laws. As a member of the bar in several jurisdictions, she has argued before state, federal and appellate courts, has testified before Congress, and has conducted discovery and depositions in litigated matters, arbitration proceedings and regulatory investigations. Pamela specializes in the investigation of financial crimes, securities fraud and accounting irregularities.

Pamela co-authored Chapter 10, Reducing the Risk of Financial Statement Fraud.

Samuel D. Porteous, JD, MBA, is a Managing Director and Manager for China of Kroll Inc. based in Shanghai. Since 1989, Sam has concentrated on economic and commercial intelligence, in addition to white collar and organized crime in both the corporate and government sectors. Sam's casework also includes fraud prevention, crisis management, asset tracing, due diligence, hostile takeovers, terrorist financing, and risk assessment. He has conducted major investigative and analytical assignments involving fraud and business intelligence in mainland China and throughout South East Asia. Sam has been accepted by the courts as an expert witness on intelligence and organized crime issues on numerous occasions. His articles on financial sanctions, economic crime, commercial intelligence, money laundering, terrorist fundraising and doing business in China have been published in newspapers, academic and professional journals, and in government publications in the United States, Europe, Canada and China.

Sam co-authored Chapter 14, Identity Theft and Corporate Identity Fraud.

Daniel W. Ray, CPA, CFE, CIRA, is a Director in the Litigation Services Group in the San Francisco office of Hemming Morse, Inc. As a CPA and former Special Agent for the FBI, Dan has concentrated on forensic accounting, fraud investigation, and bankruptcy-related cases for more than nineteen years of his professional career. His combined expertise in accounting and fraud investigations has enabled Dan to assist attorneys in the areas of document discovery, analysis of business and accounting records, deposition assistance, and development of trial exhibits. As a CPA, Dan has worked as a consultant and expert witness in civil and criminal cases and has assisted both prosecution and defense, testifying in federal, state, and local courts.

David M. Shapiro, CPA, MBA, JD, BA, is a Manager in the Financial Litigation Consulting practice for the New York office of Kroll Inc. David has combined his legal and accounting backgrounds to concentrate on forensic accounting and litigation support since 1993. In addition, he has eight years' prior experience in the investigation and prosecution of frauds and related criminal conduct as a Special Agent for the FBI in New York, and Assistant Prosecutor in New Jersey. David's casework includes criminal prosecutions and civil litigation involving businesses and professional practices. He has testified in depositions of matters in federal and state courts arising from dissident shareholder actions. David has presented training seminars on litigation support and compliance programs.

David authored the Financial Services, Construction and Government chapters in the Fraud Sector-by-Sector section.

Ches Somers, BA, is a Senior Investigator in the Toronto office of Kroll Associates, a division of Kroll Inc. He specializes in complex white-collar crime, general business and due diligence investigations, in addition to intelligence gathering. Ches spent twenty-nine years of his career with the Royal Canadian Mounted Police, where he attained the rank of Inspector. Twenty-five of these years were devoted to investigating commercial crime. Ches's practice involves large-scale investigations involving fraud, bankruptcy and insolvency, and crimes in the banking industry. His casework includes cheque kiting, prime-bank instrument fraud, employee fraud, inter-provincial and international fraud, and money laundering. Ches has made numerous presentations on topics from white-collar crime, major case management, ethics in policing, investigative and interviewing techniques, and court-brief preparations to employee theft and fraud, vendor fraud asset tracing and secret omissions, employer-employee relations and privacy issues in criminal investigations.

Ches co-authored Chapter 14, Identity Theft and Corporate Identity Fraud.

Howard Silverstone, CPA, FCA, CFE, is a Principal in the Philadelphia office of Kroll Inc. Howard has concentrated on forensic and investigative accounting since 1985, and has experience working on hundreds of forensic accounting and claims assignments both in North America and internationally. He has been involved in every aspect of cases, including planning, detailed analysis, assistance with all phases of discovery, and expert testimony at deposition and trial in connection with loss assessment, fraud, and related financial issues. His cases include economic damages, fraud investigations, fidelity bond analysis and surety matters, among many others. A native of the United Kingdom, Howard is a member of the Pennsylvania Institute of Certified Public Accountants. Howard co-authored the book, *Forensic Accounting and Fraud Investigation for Non-Experts*, published by John Wiley & Sons, Inc.

Howard co-authored Chapter 3, Insurance Against Fraud.

Patricia Woytek, BA, MIS, CPA, specializes in forensic and investigative accounting at Kroll, Inc. Philadelphia. For almost twenty years, Pat has specialized in complex financial and forensic analyses of financial statements, tax returns, accounting records, contracts, and agreements. Her casework includes fidelity and surety losses, directors' and officers' negligence, business income losses, lost profits and economic damages, commercial damage calculations, corporate fraud investigations, damages in breach of contract disputes, and damages caused by financial institution failures. Pat has also written for *The Risk Report*, published by the International Risk Management Institute and has given numerous speeches on the subject of fraud.

Patricia co-authored Chapter 3, Insurance Against Fraud.

Howard Zandman, CPA, is a Principal of Tauber & Balsler, P.C., an Atlanta-based CPA firm. During his distinguished 30-year career, Howard has specialized in insurance loss claims, with a focus on business interruption, inventory loss and valuation, review of financial condition relative to motive for arson or fraud, loss of income resulting from personal injury, employee dishonesty, product liability and third-party liability claims. Howard is recognized as an expert in insurance loss accounting and business interruption claims and has testified as an expert witness in both federal and state jurisdictions. An experienced public speaker, Howard has given numerous workshop and seminar presentations on topics involving insurance loss accounting to a variety of professional organizations.

Howard authored the Small Business chapter in the Fraud Sector-by Sector section.

CHAPTER 1:

Managing the Risk of Fraud

| | | |
|-------|--|----|
| 1.1 | The Nature and Extent of Fraud | 3 |
| 1.1.1 | Definitions | 3 |
| 1.1.2 | Magnitude of the Threat | 3 |
| 1.1.3 | Sources of the Threat..... | 5 |
| 1.1.4 | The Causes of White Collar Crime | 5 |
| 1.1.5 | Understanding the Risk..... | 7 |
| 1.1.6 | Guarding Against the Threat..... | 9 |
| 1.2 | Fraud Risk Factors | 10 |
| 1.2.1 | Generic Risk Factors | 11 |
| 1.2.2 | Individual Risk Factors | 12 |
| 1.2.3 | High Fraud-Low Fraud Environments | 15 |
| 1.3 | Internal Controls and “Fraud-Proofing” | 18 |
| 1.3.1 | Defining Internal Control Objectives | 18 |
| 1.3.2 | Basic Controls | 18 |
| 1.3.3 | Supervision | 20 |
| 1.3.4 | Audit | 22 |
| 1.4 | Detecting and Preventing Fraud in Books of Account..... | 23 |
| 1.4.1 | The Auditor’s Duty to Detect Fraud | 23 |
| 1.4.2 | Fraud and Statement on Auditing Standards No. 99 | 24 |
| 1.4.3 | Fraud Auditing Versus Financial Statement Auditing | 25 |
| 1.4.4 | Fraud Auditors Versus Financial Statement Auditors..... | 27 |
| 1.4.5 | The Risk of Fraud | 27 |
| 1.5 | A New Environment for Fraud Risk Detection and Enforcement | 28 |
| 1.5.1 | The Winds of Change | 29 |
| 1.5.2 | The Sarbanes-Oxley Act of 2002 | 29 |



| | | |
|-------|--|----|
| 1.5.3 | PCAOB Auditing Standard No. 2 and the COSO Framework | 29 |
| 1.5.4 | Issues for Smaller Entities and Private Companies | 31 |
| 1.5.5 | Post Sarbanes Implementation Effectiveness | 32 |
| 1.6 | Risk Management Checklist..... | 32 |

CHAPTER 1:

Managing the Risk of Fraud

1.1 THE NATURE AND EXTENT OF FRAUD

1.1.1 Definitions

The key word used in most dictionaries to define fraud is *deception*. In the broadest sense of the word *fraud*, this definition may be sufficient. However, in the context of this *Handbook*, a slightly more restrictive definition is appropriate. Fraud is *criminal deception intended to benefit the deceiver financially*. Both of the qualifiers in this definition are necessary—that is, the deception must be *criminal* in nature and involve *financial benefit*.

Criminal Deception

The qualifier *criminal* is necessary to exclude certain deceptions that may financially benefit the deceiver—for example, the mild overstatement of one’s skills on a job application; however, this kind of transgression will not be examined in this *Handbook*. Although such an overstatement could be labeled *fraudulent* in the broadest sense of the word, it can hardly be described as criminal.

Note that, for purposes of this definition, the word *criminal* is not used in a strict legal sense. Rather, it refers to a seriously “wrong” action taken with malicious intent. Thus, even if perpetrators of fraud are able to avoid successful criminal prosecution—for example, because a particular jurisdiction has lax laws or enforcement, or because of some legal technicality—their actions are still considered “criminal” for purposes of this *Handbook*.

Financial Benefit

The qualifier *financial benefit* is necessary to exclude certain types of criminal deception that we do not commonly think of as fraud and, therefore, they are not addressed in this *Handbook*—for example, a wealthy bigamist failing to disclose a previous marriage.

The financial benefit accruing to the fraudster from an action need not be direct for that action to be considered fraudulent. Indirect financial benefits are also possible, for example, environmental criminals (fraudsters) who dump toxic waste into rivers to avoid higher disposal costs and falsify records to conceal their actions.

1.1.2 Magnitude of the Threat

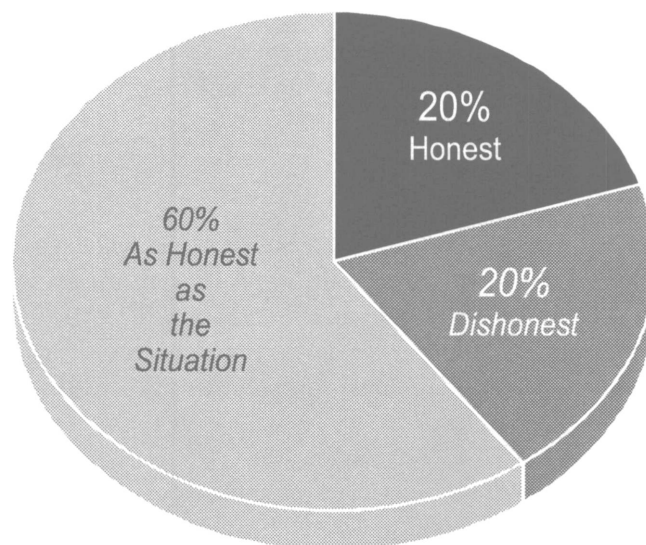
Because the essence of fraud is deception, determining its prevalence is problematic. Many frauds go undetected—probably more than 75 percent—and many frauds that are detected are not reported. It is virtually impossible to compile reliable statistics under these circumstances.

Simply based on the largest reported frauds—for example, the recent corporate scandals (Enron, Worldcom, et al), the U.S. savings and loan scandal, BCCI, Ivan Boesky, and Michael Milken—it is safe to say that fraud in the United States runs into the billions of dollars. In its 2006 *Report to the Nation: Occupational Fraud and Abuse*, the Association of Certified Fraud Examiners estimates 5 percent of revenues (approximately \$652 billion) will have been lost to fraud in the United States in 2006. In 2004, lost revenues were estimated at 6.¹

Macro statistics are not particularly meaningful, however, even if you could obtain accurate statistics. The fact is that the threat of fraud depends largely on the circumstances, that is, the environment in which it takes place. Let's begin with a view of personal integrity, as illustrated by Figure 1-1, "One View of Personal Integrity."

Figure 1-1. One View of Personal Integrity

One View of Personal Integrity



Views of commitment to personal integrity vary, and the percentage figures shown are not definitive. Some views suggest a more even split between the three categories, while others state that the honest and dishonest categories may be as low as 10 percent each. However, all of these views point to one important conclusion: Exclusive reliance on the honesty of individuals is the surest way to be victimized. More than half the population—actually, probably more than two-thirds—is quite capable of committing dishonest acts in the right (or should we say wrong?) environment.

The importance of creating an environment that discourages fraud brings us back to the question, What is the magnitude of the threat? The answer is: *the threat of fraud is as big as it is allowed to be.*

¹ 2006 ACFE Report to the Nation on Occupational Fraud and Abuse Association of Certified Fraud Examiners, 2006.

1.1.3 Sources of the Threat

The magnitude of the fraud threat is only one dimension contributing to the extent of the problem. The breadth of the fraud threat—that is, the various sources of fraud—must also be considered. A truly comprehensive prevention strategy must address the full spectrum of fraud sources.

You can classify the sources of the fraud threat as either internal or external. These threats may or may not involve collusion, which can be defined as an agreement between two or more persons to defraud another or to obtain something forbidden by law. A brief description of the two sources of fraud threat follows.

Internal Sources

Internal opportunities to commit fraud differ from company to company. Some typical examples, which illustrate the broad nature of these internal opportunities, include the following:

- Officers of a company create false financial reports to improve their own performance measurement.
- Managers inflate their expense accounts or turn a blind eye to supplier fraud in exchange for kickbacks.
- Other employees commit fraud such as embezzlement, cash skimming, or accounts receivable lapping.
- Corporate directors defraud a company's shareholders through fraudulent financial reporting, stock market manipulation, or insider trading.
- Employee theft/misappropriation of assets, which may involve collusion with outside vendors or suppliers.

External Sources

Typical examples of external opportunities to commit fraud include the following.

- Suppliers falsify or duplicate invoices.
- Competitors victimize a company through industrial espionage or price fixing.
- Con artists defraud a company with schemes involving products, services, or investment opportunities that never materialize.
- Customers commit fraud through false credits posted to their accounts or through rebate coupon frauds.

See Figure 1-2, "How a Company Can Be Victimized," for a depiction of the various internal and external sources of fraud.

1.1.4 The Causes of White Collar Crime

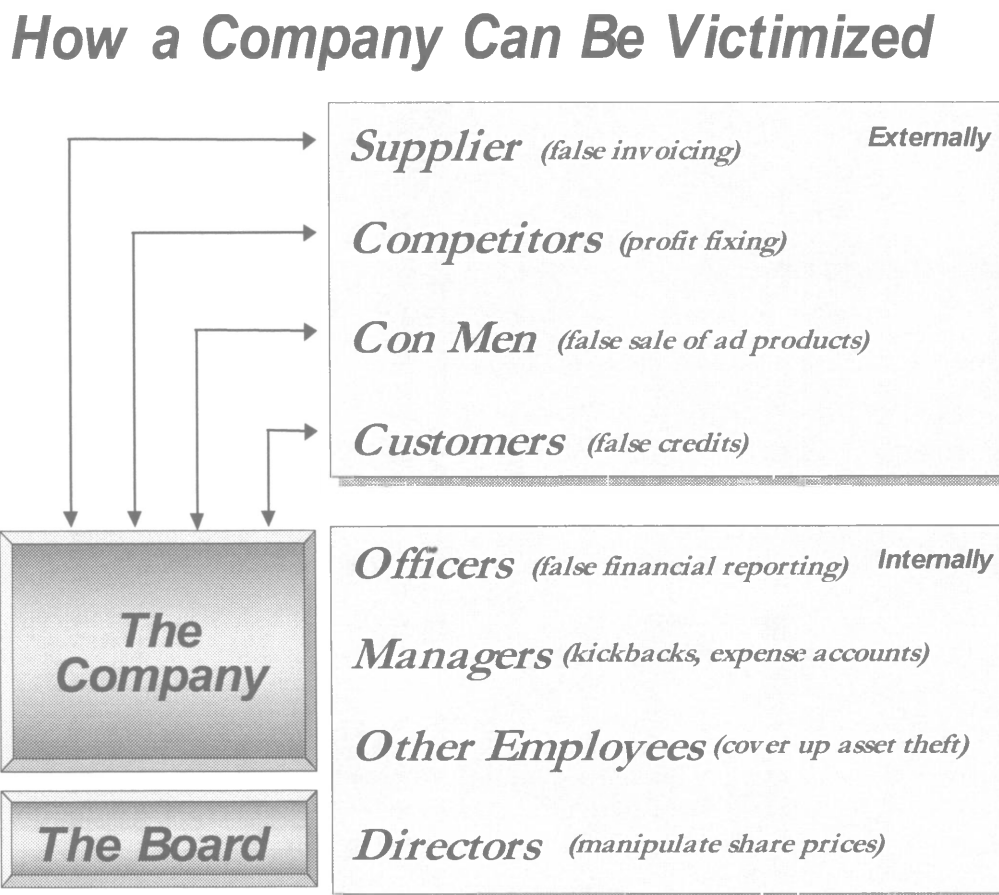
The theory of *differential association* is undoubtedly the best known among all explanations offered to account for crime. Although it applies to all forms of crime—not just white collar crime—it is nevertheless useful for the purposes of this *Handbook*.

This theory first appeared in 1939 in the third edition of Edwin H. Sutherland's *Principles of Criminology*. Later, Sutherland would make his best-known contribution to criminology by coining the phrase *white-collar crime* and writing a monograph on the subject.

Based on nine concepts or *points*, the theory of differential association begins by asserting that criminal behavior is learned. Expanding on that assertion, Sutherland specifies as a second point that criminal behavior is learned in interaction with other people in a process of communication. If individuals acquiring criminal habits or propensities were exposed to situations, circumstances, and interactions totally of a criminal nature, it would be relatively easy to comprehend how this process of communication operates. In view of the enormous variation in standards and personalities to which any individual in our society is exposed, it becomes exceedingly difficult to discern the elements that induce criminal behavior without some additional principles.

Sutherland's third point is that criminal behavior is acquired through participation within intimate personal groups. This suggests that the roots of crime are in the socializing experiences of the individual. Unfortunately, the process of socialization is far from adequately understood. Sutherland's fourth point indicates that the criminal learning

Figure 1-2. How a Company Can Be Victimized



process includes not only techniques of committing crime but also the shaping of motives, drives, rationalizations, and attitudes. Crime techniques often can involve a high degree of skill. For example, picking pockets (and not getting caught) demands considerable adroitness.

Fifth, Sutherland stipulates that legal codes define the specific direction of motives and drives as favorable or unfavorable.

Sixth, Sutherland establishes the principle of *differential association*. According to this postulate, a person becomes a criminal because of an excess of definitions favorable to violation of the law over definitions unfavorable to violation of the law. Sutherland states in his seventh point that differential association may vary in frequency, duration, priority, and intensity. But he does not suggest which of these elements is apt to be more important than the others.

Sutherland's eighth point is that learning criminal and delinquent behavior involves all the mechanisms that are involved in any other learning. As his next to last proposition, Sutherland stresses that learning differs from pure imitation.

The last point is a worthwhile reminder that while criminal behavior is an expression of general needs and values, it is not explained by these general needs and values because noncriminal behavior is an expression of the same needs and values. This means that the generalizations sometimes employed to account for crime—that people steal because they crave “esteem” or are “greedy” or kill because they are “unhappy”—have little scientific merit.

In other words, much of the same needs and values motivate criminals and noncriminals alike. People become or do not become criminals on the basis of their unique responses to common drives for prestige, happiness, success, power, wealth, and other human aspirations. One person with a pressing need for money may take an extra weekend job pumping gas, or try to borrow from a friend. Another person, feeling the same need, may hold up a fast food outlet.

1.1.5 Understanding the Risk

Of the two available ways to combat fraud—prevention and detection—a prevention strategy is obviously the preferred approach. Such a strategy can be either general or specific in its objective. General prevention techniques for risk management involve two main elements:

1. Understanding the risk
2. Guarding against the threat

Fraud Versus Theft

Resolved: Fraud is not the same as theft.

In a debate, most people would choose to defend the above statement. They might win by arguing that:

- Theft is like robbing a bank; fraud is like cooking the books to create the impression of improvement in the financial results of the enterprise.

- People committing theft do so at night, wearing masks; people committing fraud do so during the day, wearing suits.
- Theft is direct; fraud is indirect.
- Theft is what lower-class criminals commit; fraud is what upper-class criminals commit.

Few people, if any, however, will point out what is perhaps the most important difference between fraud and theft: The risk of fraud is much greater.

With an increasingly high media profile given to crime, particularly in large cities, most people are acutely aware of the need to protect themselves against crime's overt forms. In a bad neighborhood, for example, you would not leave the keys in your car or the doors unlocked. In fact you probably would not want to be there at all. In this case the risk of theft, a more overt and direct form of criminal act than fraud, is easy to assess and deal with.

Now consider a different scenario. If you were to leave your wallet briefly on your desk at work, you would also be exposing yourself to a risk. However, assuming that access to your workplace is restricted to other employees, in all likelihood, you would consider this risk very small. Presumably, the people you work with are not criminals and would never pick up your wallet in a direct act of theft. The risk of being detected, as perceived by a perpetrator, would be relatively high. You would certainly know that your wallet had been stolen and a thorough investigation would ensue, possibly implicating a coworker.

Herein lies the first of two pillars on which the greater threat of fraud is built. One pillar is based on the premise that most people believe that those who are relatively close to them—their friends and coworkers—are basically honest. Potential victims may rationalize about those around them: "They would never steal. As long as we lock the doors at night to keep out the 'real crooks,' we'll be safe."

The other pillar is based on the perception that fraud is in some sense an indirect form of theft. Although a criminal act, people who perpetrate fraud will in many cases rationalize their behavior, believing that because it's indirect, it's victimless. Alternatively, the perpetrator may rationalize that the victim deserves it, or where the amount involved in the fraud is low in relation to the total assets available, that the victim can afford it and/or won't even miss it. And so the second pillar is formed from the rationalizations of most fraudsters—the denial that the fraud is morally wrong: "No one will be hurt by this. The company won't even miss it. Besides, they deserve it for the lousy way they treat me."

These two pillars—low perception of the threat of fraud by potential victims, and a high degree of rationalization by potential perpetrators—combine to make fraud a much more insidious threat than ordinary theft. A further illustration of this greater risk: according to a report in a 1999 Federal Bureau of Investigation (FBI) *Law Enforcement Bulletin*, check fraud in 1994 was estimated to have an impact on financial institutions, private business, and the public that ranged from \$815 million up to \$10 billion. Further, according to bank executives, check fraud is the major crime problem facing the financial community. The enormity of the fraud problem is illustrated by another FBI report that indicated that about \$60 billion in mortgage loans processed annually involved some degree of fraud, and that in 1996, 35 percent of the \$3.3 billion of reported losses in the financial institution fraud criminal referrals the FBI received involved some type of loan fraud or false statement.

Generic Versus Individual Risk Factors

A large number of factors can determine the risk of fraud. This *Handbook* contains an approach—a system of categorization that facilitates the understanding of fraud risk and the development of an appropriate strategy to manage it.

The literature is filled with many different systems of categorizing fraud risk. The system developed for this *Handbook* splits the risk factors into two groups:

1. Generic
2. Individual

Generic risk factors remain relatively constant in their impact on any subject individual or group of individuals. They are largely within the control of the organization or entity that is protecting itself, and largely outside the control of potential perpetrators. Because these risk factors apply in the same way to any employee, they can be set and manipulated by an organization without considering individual differences among employees. Employee turnover has virtually no effect on these risk factors. For example, if there is no dollar limit on checks that employees in the accounting department can issue, this risk would exist no matter who is employed in the accounting department.

Individual risk factors change from person to person and can even change for the same individual over time. They are only partially within the control of the organization or entity that is protecting itself, and this control is more difficult to exercise because it applies to each individual separately. Whenever turnover occurs, the individual risk factors change and must be managed. Even worse, whenever an individual's personality, state of mind, circumstance, or motivation changes—which, after all, is a constant process—the associated risk factors may also change.

See Sections 1.2.1, “Generic Risk Factors,” and 1.2.2, “Individual Risk Factors,” for a more detailed discussion of generic and individual risk factors.

1.1.6 Guarding Against the Threat

On understanding the risk of fraud, you must develop an appropriate strategy and implement policies to guard against the threat. The main elements of this process are:

1. Choosing acceptable risk levels
2. Developing and implementing internal controls
3. Promoting an ethical environment
4. Arranging appropriate risk financing (insurance)
5. Ensuring adequate computer security

Choosing Acceptable Risk Levels

The risk of fraud can never be completely eliminated. Even if this were possible, it would probably not be desirable because of prohibitive costs and extremely tight controls that would stifle creativity and make employee morale suffer. The first step in a fraud-prevention strategy is to determine the acceptable level of risk.

Choosing acceptable risk levels intertwines with assessing the various risk factors. For example, one of the generic risk factors is the *opportunity risk* available to potential perpetrators. Assessing this opportunity risk enables you to make other decisions, such as: “Do we need to lower this risk, and if so, by how much?”

Developing and Implementing Internal Controls

Internal controls—consisting of basic controls, supervisory controls, and audit—represent the cornerstone of any fraud prevention strategy.

To ensure complete and accurate reporting, an internal control system must be designed and implemented *regardless* of the risk of fraud. However, a system should never *disregard* the risk of fraud; such disregard would amount to a virtual invitation to potential perpetrators.

See Section 1.3, Internal Controls and “Fraud-Proofing,” for a detailed discussion of internal controls.

Promoting an Ethical Environment

Promoting an ethical environment is another key element in a prevention strategy. In particular, implementing a formal code of ethics and business conduct helps set the tone for all employees within an organization. See Chapter 2, “Promoting an Ethical Environment,” for further discussion.

Arranging Appropriate Insurance

Recognizing that there will always be some risk of fraud, organizations must finance this risk either externally and explicitly (fidelity insurance) or internally and implicitly (self-insurance). See Chapter 3, “Risk Financing and Fidelity Insurance,” for further discussion.

Ensuring Adequate Computer Security

Computers and information technology play an increasingly important role in business and society in general. The pervasive nature of these technologies demands that adequate computer security be an integral part of any prevention strategy. Although computer security may be considered a subset of internal control, it is still an important aspect. See Chapter 4, “Computer Security and System Recovery,” for details.

1.2 FRAUD RISK FACTORS

Several factors contribute to the risk of fraud. Organizations use various systems for categorizing these factors; however, under most systems, the elements that combine to determine fraud risk are largely the same.

For example, one classification system is known as the GONE theory, an acronym for *greed*, *opportunity*, *need*, and *exposure*. Under this system, the greed and need factors relate largely to the individual (that is, the potential perpetrator), while the opportunity and exposure factors relate largely to the organization (that is, the potential victim). The four elements of the GONE theory interact to determine the level of fraud risk, and no one factor is universally more important than another. Each of the factors is unfavorable, to some extent, in virtually all situations. However, an organization that allows a sufficiently unfavorable or an out-of-balance combination of all four factors may face serious troubles. As one fraud investigator observed, “You can consider your money GONE.”

SAS No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 316), used a fraud “triangle” concept to categorize fraud. That document cited (1) incentives/pressures, (2) opportunities and (3) attitudes/rationalizations

as a framework for understanding fraud and its environment. Appendices to that auditing standard provided examples of fraud risk factors under each of these headings and a useful Exhibit directed to companies: “Management Antifraud Programs and Controls.”

In this *Handbook* we use a slightly different system that groups the risk factors into generic or individual, as previously defined. However, as described below, many of the same elements of the GONE theory or fraud triangle apply under this system as well.

1.2.1 Generic Risk Factors

Generic risk factors—those largely under the control of the organization or entity that is protecting itself—include:

- The opportunity given to potential perpetrators
- The likelihood of discovering a fraud that was committed
- The nature and extent of the punishment a perpetrator will receive once the fraud is uncovered and the perpetrator is caught

Note that the first factor corresponds to the *O* or opportunity in the GONE theory, while the second and third factors correspond to the *E* or exposure risk element. The exposure risk under the GONE theory is a product of two generic factors, which are the likelihood of getting caught and the subsequent consequences.

A brief description of each generic risk factor follows.

Opportunity to Commit Fraud

The opportunity to commit fraud refers primarily to allowing a potential perpetrator access to the assets of the organization, the accounting system or the object of the fraud. No organization can completely eliminate opportunity; experts consider such attempts uneconomical and counterproductive. As long as organizations have assets of value and these assets flow, are traded, or come under the control of others—such as employees, customers, and suppliers—the opportunity to commit fraud will always exist.

For organizations the challenge in fraud prevention is ensuring that the opportunity risk level is minimal under the circumstances, that is:

1. Assign, either explicitly or implicitly, to each employee an appropriate maximum opportunity level. For example, limit a junior clerk’s opportunity level to certain smaller fixed assets not bolted down in the office. Allow a more senior clerk’s maximum opportunity level to include an additional \$500 petty cash fund, or the day’s cash receipts. Allow a senior executive an additional \$5,000 check-signing limit. Consider similar limits regarding level of access to the accounting system.
2. Prohibit catastrophic opportunity levels. The definition of a catastrophic level depends on the circumstances—in particular, the size of the organization. For example, a small business with \$50,000 in cash should probably not allow anyone but its owner(s) access to the full amount.

Likelihood of Discovery

If an opportunity to commit fraud exists, making the chances of discovery high reduces the risk. In fact, even the *perception* that the chances of discovery are high can act as a deterrent. Of course, if a fraud does occur, *discovery* may result in *recovery* of some of the lost assets.

The likelihood of discovery stems primarily from the system of internal controls. Although these controls can never be so tight as to preclude any fraud from taking place, ideally they should be sufficient to prevent most material frauds from going undetected for any length of time.

Another factor that could increase the chance of discovery is encouraging employees to take an active role in reporting suspected fraud activities. Publicizing the negative impact of fraud on the stock price, employer profitability, and employee profit-sharing or retirement benefits has worked to stimulate employee efforts to curtail fraud.

See Section 1.3 for a closer look at internal controls.

Nature and Extent of Punishment

Discovery of a fraud is, in itself, insufficient to act as a deterrent against future fraud.

Organizations must put in place some adverse consequences for potential perpetrators, who, most importantly, must understand these adverse consequences.

Although research has not provided proof, conventional wisdom holds that the nature and extent of punishment can be a deterrent.

Organizations or entities wishing to protect themselves from fraud should have clear policies regarding the nature and extent of the consequences of getting caught; for example:

- Anyone who commits a fraud will be dismissed.
- All frauds will be reported to the authorities, and charges will be laid.

1.2.2 Individual Risk Factors

Individual risk factors—those that vary from employee to employee largely outside the control of the organization or entity that is protecting itself—fall into two categories:

1. Moral character
2. Motivation

Moral character corresponds to the *G* or greed factor in the GONE theory, while motivation is equivalent to the *N* or need factor. Each of these categories is described below.

Moral Character (Greed Factor)

Greed represents broad concepts, such as ethics and moral character, or the lack thereof. Moreover *greed* and *ethics* essentially relate to the internal or personality attributes of an individual, as do *character*, *integrity*, *honesty*, and the like. You cannot know whether an individual possesses these attributes without the ability to read that individual's mind. Even if this were possible, personal interpretation would still come into play.

Social values also have an impact on moral character. Many sociologists lamented a trend in Western societies during the 1980s, namely the pursuit of wealth as an overriding objective. The *Me Generation* and the *Decade of Greed* were phrases coined in connection with this trend, which was perhaps best epitomized by the memorable speech made by Michael Douglas when he played the character of Gordon Gekko in the 1987 movie, *Wall Street*: “Greed is right. Greed is good. . . .”

In fact, Gordon Gekko’s philosophy may hold some element of truth. A certain amount of greed, tough-mindedness, and competitive instinct could greatly enhance the chances of success for an organization or an individual in a free enterprise society. Regardless of one’s own value judgment, there is no doubt that these attributes do exist in society. This poses a problem, however. Greed may not necessarily preclude the existence of ethics and good moral character, but, if left unchecked or promoted to a great extent, it can have an adverse impact *vis-à-vis* the risk of fraud. This leads to the essential question at issue here: What can or should an organization do to minimize the risk of fraud posed by greed and other negative attributes? Consider the following:

1. *Corporate mission statement.* Set the goals of an organization in a corporate mission statement and communicate it to all managers and other employees. The primary goal of most businesses is to maximize profits, presumably over the long term in order to survive. Other objectives might include maintaining either a high market share, leadership in an industry, or both. However, businesses must pursue these goals in a manner consistent with good corporate citizenship and standing in the community. This emphasis on corporate responsibility sets the tone for management and employees, and encourages personal responsibility. Conversely, business should discourage irresponsible actions—and by extension, fraud.
2. *Written codes of business conduct.* “Good moral character” means different things to different people. An organization must define this term and relate it to particular types of behavior. For example, does your organization consider it moral and ethical for its employees to accept gifts from customers and, if so, is there a specified value or limit? A written code of ethics and business conduct can help translate the relative concepts of greed, ethics, and morality into more specific behaviors that are either acceptable or unacceptable.
3. *Management style and role models.* Management must set the right example for employees by acting responsibly and living up to the spirit of the corporate mission statement and code of business conduct. Moreover, management must clearly and visibly appear to do so in its dealings and communications with employees. Policy statements mean nothing if they are undermined by management’s actions. In fact, such a situation may be worse than having no policy at all because management’s failure to adhere to its own guidelines would foster a kind of cynicism and “rules are made to be broken” philosophy that might potentially encourage fraud and commercial crime.
4. *Hiring practices.* Regardless of corporate mission statements, codes of business conduct, and good role models, moral character ultimately depends on the individual employee. To the extent possible, set hiring practices that weed out prospects with low moral character. See chapter 3 for further discussion.

Motivation (Need Factor)

Why do people commit fraud? There is obviously no single, specific answer. People commit fraud for a variety of reasons.

Probably the most common group of fraud motivations relates to economic need. For example, the perpetrator may be experiencing an actual or perceived cash emergency; there is a mortgage to pay, drugs to purchase to satisfy an addiction, or gambling losses to win back. Alternatively, there may be no emergency but simply an unchecked desire for the good life, meaning the expenses of upscale restaurants, clothes, furs, jewelry, vacations, cars, homes, and summer cottages.

In addition, there are several motivations for managers to commit financial statement fraud. For instance, managers could have bonuses or incentives tied to revenue or earnings-per-share figures. Also, managers who own a large portion of company stock may be motivated to falsify financial statements to meet earnings-per-share projections and maintain or raise the company's stock price.

Less frequently, there might be other reasons, such as disenchantment, revenge, or simply the perception that everyone else seems to do it. Even more rarely, the motives could be eccentric: a sense of challenge or thrill. Finally, the cause may be some form of psychological illness, such as compulsion, anxiety, paranoia, or outright psychosis.

What can be done about all of these complex motives, seemingly locked up in the Pandora's box of an employee's mind? Admittedly, the options are limited but they include:

1. *A favorable environment.* Creating the right environment can reduce the motivation among employees to commit fraud. In an unfavorable environment, morale suffers and feelings of disenchantment—even hate and the desire for revenge—may take hold. Try to promote the right environment by treating employees fairly, keeping communication lines open, and providing mechanisms for discussing and resolving grievances.
2. *Performance appraisal and reward systems.* Measure each employee's work fairly by implementing a performance appraisal and reward system.
3. *Employee assistance programs.* Many enlightened employers provide free counseling and other assistance to employees facing personal problems, for example, alcohol and drug abuse. From the point of view of fraud prevention, this approach is preferable to keeping these problems "bottled up." This approach helps prevent resentment that could ultimately lead to the commission of fraud.
4. *Employee testing and screening.* As part of their hiring practices and sometimes on a regular basis thereafter, some employers use testing and screening procedures to identify and weed out high-risk individuals, or form the basis for remedial action, or both. Procedures include psychological testing, drug testing, and even honesty testing in the form of lie detector tests where not prohibited by law. Highly controversial, these tests, in some instances, could cause more harm than good, for example, to employee morale, the organization's reputation among prospective employees, and so on. Nevertheless, in especially sensitive occupations or circumstances, employers might find this testing appropriate and even necessary.
5. *Common sense and a watchful eye.* Although motives are not observable, the result of certain motives often is. An employee with a drug or gambling problem may not be able

to keep it a secret. And beware the \$25,000-a-year bookkeeper who drives to work in a Mercedes or who, wary of getting caught, never takes a vacation.

Profiles of Fraud Perpetrators

Although external pressures do play a major role in whether or not an individual commits fraud, internal characteristics can affect a potential fraud perpetrator as well. Gwynn Nettler in his book, *Lying, Cheating and Stealing*, makes the following observations:

- People who have experienced failure are more likely to cheat.
- People who are disliked and who dislike themselves tend to be more deceitful.
- People who are impulsive, distractible, and unable to postpone gratification are more likely to engage in deceitful crimes.
- People who have a conscience (fear, apprehension, and punishment) are more resistant to the temptation to deceive.
- Intelligent people tend to be more honest than ignorant people.
- The easier it is to cheat and steal, the more people will do so.
- Individuals have different needs and therefore different levels at which they will be moved to lie, cheat, or steal.
- Lying, cheating, and stealing increase when people are under great pressure to achieve important objectives.
- The struggle to survive generates deceit.

The highly publicized cases in recent years of computer hackers committing high-tech crimes have resulted in a public perception that individuals who are highly knowledgeable about computers are more likely to commit fraud; however, there is no evidence to support this premise.

1.2.3 High Fraud-Low Fraud Environments

Employee fraud, theft, financial statement fraud, and embezzlement are more likely to occur in some organizations than others. The most vulnerable organizations are usually hampered by weak management and inadequate accounting and security controls. Solutions often proposed include:

1. Tight accounting and audit controls
2. Thorough screening of applicants for employment
3. Close supervision and monitoring of employee performance and behavior
4. Explicit rules against theft, financial statement fraud, embezzlement, sabotage, and information piracy

Other considerations also affect the likelihood of employee crime. See Table 1.1, “A Comparison of the Environments and Cultures of Organizations With High and Low Fraud Potential,” for a comparison of the environment and culture of organizations with high fraud potential and organizations with low fraud potential.

TABLE 1.1 A COMPARISON OF THE ENVIRONMENTS AND CULTURES OF ORGANIZATIONS WITH HIGH AND LOW FRAUD POTENTIAL

| Variable | High Fraud Potential | Low Fraud Potential |
|-----------------------------------|--|--|
| <i>Management style</i> | Autocratic | Participative |
| <i>Management orientation</i> | Low trust Power-driven | High trust Achievement-driven |
| <i>Distribution of authority</i> | Centralized, reserved by top management | Decentralized, dispersed to all levels, delegated |
| <i>Planning</i> | Centralized Short range | Decentralized Long range |
| <i>Performance</i> | Measured quantitatively and on a short-term basis | Measured both quantitatively and qualitatively and on a long-term basis |
| <i>Business focus</i> | Profit-focused | Customer-focused |
| <i>Management strategy</i> | Management by crisis | Management by objectives |
| <i>Reporting</i> | Reporting by routine | Reporting by exception |
| <i>Policies and rules</i> | Rigid and inflexible, strongly policed | Reasonable, fairly enforced |
| <i>Primary management concern</i> | Capital assets | Human, then capital and technological assets |
| <i>Reward system</i> | Punitive Penurious Politically administered | Generous Reinforcing Fairly administered |
| <i>Feedback on performance</i> | Critical Negative | Positive Stroking |
| <i>Interaction mode</i> | Issues and personal differences are skirted or repressed | Issues and personal differences are confronted and addressed openly |
| <i>Payoffs for good behavior</i> | Mainly monetary | Recognition, promotion, added responsibility, choice assignments, plus money |
| <i>Business ethics</i> | Ambivalent, rides the tide | Clearly defined and regularly followed |
| <i>Internal relationships</i> | Highly competitive, hostile | Friendly, competitive, supportive |
| <i>Values and beliefs</i> | Economic, political, self-centered | Social, spiritual, group-centered |
| <i>Success formula</i> | Works harder | Works smarter |

TABLE 1.1 (continued)

| Variable | High Fraud Potential | Low Fraud Potential |
|---|--|---|
| <i>Human resources</i> | Burnout High turnover Grievances | Not enough promotional opportunities for all the talent Low turnover Job satisfaction |
| <i>Company loyalty</i> | Low | High |
| <i>Major financial concern</i> | Cash-flow shortage | Opportunities for new investment |
| <i>Growth pattern</i> | Sporadic | Consistent |
| <i>Relationship with competitors</i> | Hostile | Professional |
| <i>Innovativeness</i> | Copy cat, reactive | Leader, proactive |
| <i>CEO characteristics</i> | Braggart, self-interested, driver, insensitive to people, feared, insecure, gambler, impulsive, tight-fisted, numbers-oriented, materialistic, profit-seeker, vain, bombastic, highly emotional, partial | Professional; decisive; fast-paced; respected by peers; secure risk-taker; thoughtful; generous with personal time and money; people- products- and market-oriented; builder-helper; self-confident; composed; calm; deliberate; fair; and know who and what he or she is, and where he or she is going |
| <i>Management structure, systems and controls</i> | Bureaucratic Regimented Inflexible Imposed controls Many-tiered structure, vertical Everything is documented, and there is a rule for everything. | Collegial Systematic Open to change Self-controlled Flat structure, horizontal Documentation is adequate but not burdensome, and some discretion is afforded. |
| <i>Internal communication</i> | Formal, written, stiff, pompous, ambiguous | Informal, oral, clear, friendly, open, candid |
| <i>Peer relationships</i> | Hostile, aggressive, rivalrous | Cooperative, friendly, trusting |

1.3 INTERNAL CONTROLS AND “FRAUD-PROOFING”

Developing an understanding of the various factors that contribute to the risk of fraud is only the first step in a fraud prevention strategy. Following this, it is necessary to implement policies that will help to reduce the threat.

Some of the measures that can guard against the threat of fraud were explained previously in this chapter. Consider what is perhaps the main, and certainly the most common, prevention tool, namely, a good system of internal controls.

1.3.1 Defining Internal Control Objectives

Fraud-proofing is a term that can be used to describe an effective system of internal controls. However, this term is somewhat misleading because no internal control system can completely eliminate the risk of fraud. What fraud-proofing should do, in theory, is reduce the risk of fraud to an acceptable level. If you have suffered from a fraud attack, consider interviewing the fraudster after the case is closed. Many fraudsters have a bit of braggadocio in them and, as a result, are only too willing to let you in on the very holes in your control system they exploited.

The risk of fraud is not the only factor in defining internal control objectives. For example, management information and reporting requirements are important considerations as well. However, the acceptable levels of risk and opportunity, as defined in Section 1.1.6, “Guarding Against the Threat,” should also be considered. This means effectively combining the three levels of internal control to limit the risk of fraud to acceptable levels. See the discussion that follows in Section 1.3.2, “Basic Controls,” Section 1.3.3, “Supervision,” and Section 1.3.4, “Audit.”

1.3.2 Basic Controls

A variety of basic controls exist in a typical system of internal controls. The most relevant basic controls are grouped into three categories:

1. Physical access
2. Job descriptions
3. Accounting reconciliations and analyses

Physical Access

Most people acknowledge the need to control physical access to valuable assets, including intangible assets such as information. Measures to control physical access include the obvious practice of locking doors, desks, and file cabinets so that unauthorized personnel, either within or outside the organization, cannot gain access. Other measures include employee IDs and passwords, computerized security systems (for example, access cards that record time of entry and exit), and electronic surveillance systems, which should include every new innovation, such as biometrics—including, for example, iris scans and voice recognition—that the business can afford.

As a general rule, organizations should restrict physical access to those who require it to perform their job function. Of course, controlling physical access in this way will not

completely reduce the risk of fraud. However, it will help to reduce the risk in the following ways:

1. Many frauds require that the perpetrator come into physical contact with either the asset being misappropriated, or the related asset records, in order to conceal the fraud. Reducing physical access reduces opportunity.
2. Physical access controls are often the most visible to potential perpetrators. Strong controls in this area send a powerful deterrent message vis-à-vis the other controls in the system. Conversely, loose physical controls invite challenge.
3. Access controls that do not prevent fraud often assist in the fraud investigation process (for example, determining what actually happened and narrowing down suspects).

Carefully screening who had access to cash receipts would have saved one U.S. County Clerk much grief. According to a newspaper report, a temporary employee was stationed at the front desk to handle passport applications, including collecting the necessary fees. The temp properly recorded and submitted for processing those applications paid for by check or money order. She pocketed any cash received and destroyed all evidence of the cash applications so that there was no record of the transaction. Not paying attention to controlling physical access led to several thousands of dollars in losses.

Job Descriptions

Formal, specific job descriptions are a very effective fraud prevention tool. These descriptions should spell out exactly what is expected of each employee. Generally, employees should not perform duties outside their job description. Those who do represent a significant red flag.

Create job descriptions that reflect the important principle of division of duties. For example, employees with physical control over an asset should not also keep the records relating to that asset (this will only make it easier for them to cover up the fraud). Segregate all other especially sensitive duties—for example, purchasing and check signing.

The need for job descriptions goes beyond the widely recognized concept of segregating duties, although it is certainly one of the important consequences of job descriptions. Some cases may result in an entirely appropriate duplication of duties, for example, double signing checks. Specify in the job description that all employees *must* take annual vacations (another well-known fraud prevention tool, because an employer is more likely to discover an ongoing fraud scheme when the perpetrators are removed from the scene).

Thus, it is apparent that employers must approach the process of formulating job descriptions for their employees in an integrated fashion. From an internal-control and fraud-prevention perspective, different tasks performed by different individuals may be interrelated; therefore, an appropriate job description for one employee will often depend on the job descriptions of others, and vice versa.

Employers often ignore or underestimate the need for formal job descriptions, writing them off as “more useless paper.” At other times, employers create job descriptions but then ignore them. This attitude invites trouble. As one leading fraud investigator put it, “When people begin to do things outside their job description, you have reason to be concerned. If it goes unrewarded, they begin to develop a justification to steal. It’s very important that job descriptions are clear, agreed upon, and adhered to.”

Accounting Reconciliations and Analyses

After access controls and job descriptions, accounting reconciliations and analyses are the third most important group of basic controls. An essential ingredient of a successful fraud is successful concealment. Regular, appropriately performed accounting reconciliations and analyses often make such concealment difficult or impossible.

Perform accounting reconciliations regularly (for example, monthly basis) including:

- Bank reconciliations, for all accounts
- Accounts receivable reconciliations (both month to month and general ledger to subledger)
- Accounts payable reconciliations (again, both month to month and general ledger to subledger)

The exact nature of the accounting analyses performed depends on the nature of the organization's operations. Analyses relevant for most organizations include:

- Variance analysis of general ledger accounts (budget to actual, current year versus prior year, and so on)
- Vertical analysis of profit and loss accounts (that is, the calculation of expenses as a percentage of sales, and comparison of these percentages with historical standards, or budgets, or both)
- Detailed sales and major expense analyses (for example, by product line or territory)

Of course, organizations often undertake accounting reconciliations and analyses with other purposes in mind—for example, to make management decisions or to ensure the accuracy of the accounting records, or both. Nevertheless, this process also can highlight discrepancies that point to fraud.

1.3.3 Supervision

Supervision represents the second level of internal control. From a fraud prevention perspective, strong supervision is vital—especially in small businesses that may have difficulty achieving segregation of duties.

Active supervision differs significantly from supervisory or management override, in which a manager or supervisor actually takes charge of or alters the work of a subordinate. In fact, override itself is a red flag—that is, it suggests that the manager or supervisor may be engaged in fraud or the concealment of one. Ideally, a supervisor or manager should allow basic controls to operate as they were intended, rather than to be circumvented by those at higher levels.

As a fraud prevention mechanism, good supervision consists of:

1. Fraud awareness
2. Approval, review, double-checking, and redoing

Fraud Awareness

Fraud prevention specialists constantly emphasize the need for “fraud awareness,” to the point that the term has almost become a cliché. However, such awareness is perhaps the

key prerequisite in building any effective fraud prevention strategy, and is especially important at the supervisory level.

Specifically, supervisors must be alert to the *possibility* of fraud whenever an unusual or exceptional situation occurs, such as complaints from suppliers or customers, discrepancies that don't make sense, or accounting reconciliations that don't balance. If a manager's mind is closed to the possibility of fraud during an unusual or exceptional situation, the risk of the fraud continuing unabated greatly increases.

Several businesses have had positive results in raising employees' awareness by publishing regular internal newsletters. In addition to reporting actual fraudulent activities, the newsletters relate the impact of the fraud on both the employees and the bottom line.

Approval, Review, Double-checking, and Redoing

In addition to awareness, fraud prevention demands that supervisors actually supervise. This means going beyond the typical approval function, such as initialing invoices or performing other duties of supervisors and managers. A more thorough review, double-checking employees' work, and redoing some tasks, may be necessary and should be approached diligently. For example, assign supervisors the responsibility of double-checking important procedures such as the monthly bank reconciliation—that is, comparing the numbers on the bank reconciliations to those on the bank statements and in the general ledger, making certain those numbers total correctly, test-checking outstanding items at the very least, and so on. To simply initial bank reconciliations in a habitual or reflex-like manner without really reviewing and actually redoing them invites fraud.

For example, the owner of a busy downtown restaurant used the following system of internal control for sales. Employees entered all prenumbered customer bills into the cash register, and at least once each day the hostess/bookkeeper batched the customer bills, listed them on a deposit sheet, and made the related bank deposit. The owner then matched the totals on the deposit sheet with the amounts shown in the stamped deposit book, and believed this to be adequate supervision.

The owner's supervision of the bookkeeper, however, was inadequate especially because she was responsible for handling the cash (the bank deposit) and related records (customer bills, cash register tapes, deposit sheets). In fact, over a three-month period, the bookkeeper skimmed a portion of each day's cash receipts by omitting some of the cash sales bills and pocketing the corresponding amounts. The owner might have uncovered the fraud by using any one of the following methods:

1. *Segregating duties.* The owner rejected this method because he trusted the bookkeeper and did not want to incur the cost of an additional employee.
2. *Accounting for all prenumbered bills.* The owner opted not to use prenumbered bills because it was too time-consuming. The bookkeeper intentionally did not list the bills in numbered order on the deposit sheet and prenumbered books were issued out of sequence to waiters and waitresses.
3. *Matching daily cash register tapes to the daily cash deposit.* The owner rejected this simplest and most appropriate method, not wanting to check his employee's work in this way because the tapes were a messy "dog's breakfast" kept in a shoebox by the bookkeeper. The disorderly recordkeeping was entirely by design, of course, to cover up the fraud.

The owner eventually uncovered the fraud when the bookkeeper became too greedy and withheld a bit too much from what the owner knew was an especially good cash sales day, which raised his suspicions and led to an investigation.

This example illustrates the necessity of supervision. Often, it is the primary defense against ongoing frauds such as financial statement fraud, the skimming of cash, or the lapping of accounts receivable. The maximum opportunity level for the bookkeeper in the previous example should have been the outright theft of the day's cash receipts—typically less than half of a day's total receipts of about \$10,000. However, inadequate supervision allowed a smaller amount of cash—about \$700 a day—to be stolen over a period of three months, which amounted to a total loss of over \$60,000.

1.3.4 Audit

From a fraud-prevention perspective, audit represents the third level of an organization's internal control system.

Internal Audit

Internal auditors work for the organization and perform the kinds of work defined by senior management. In this sense, internal auditors are an extension of senior management—they have the same concerns and deal with the same issues described throughout this chapter. Therefore, their work might include fraud detection, or developing fraud prevention mechanisms, or both.

The duties of internal auditors include the analysis of accounting policies and procedures for potential risk areas. The internal audit department submits recommendations to the controller to minimize the risk of financial statement fraud or the misappropriation of assets by accounting personnel. These recommendations might include increased segregation of duties, or modification of journal entry procedures.

The training programs and available literature for internal auditors—as provided by the Institute of Internal Auditors (IIA)—pay specific attention to the issue of fraud prevention and detection. Historically, the perspective of internal auditors differs from that of the external auditors, which is described below.

External Audit

External auditors are independent of the organization. They report on financial statements and perform other independent reviews. The restricted role of the external auditor has evolved over time. During the late 1800s and into the early 1900s, auditors actively looked for fraud—to be a kind of “bloodhound.” Court rulings gradually redefined their role to that of a “watchdog.”

This watchdog metaphor has persisted throughout most of the twentieth century. In particular, the concept of materiality has played an important part in the accounting profession's view of fraud, which is, specifically, that an auditor's procedures cannot be expected to detect immaterial frauds. No audit can be expected to give absolute assurances in this area, since Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 316), requires that an auditor obtain *reasonable* assurance that there is no material misstatement as a result of

fraud.² If a fraud is material enough to affect the financial statements of an organization—and an auditor’s opinion on those financial statements—then the auditor’s procedures should be reasonably designed to uncover it. However, there is certainly no guarantee of detection. For example, even when the auditor’s procedures are sound, the perpetrator(s) may go to great lengths to deceive the auditor and hide the accounting fraud.

In recent years, the public’s expectations have reopened to some extent the bloodhound-watchdog debate primarily because of the perception that auditors should bear responsibility for detecting significant frauds even when immaterial to the total worth of an organization. In a 1998 speech by then Securities and Exchange Commission (SEC) Chairman Arthur Levitt, the issue of immateriality in contemporary financial statements was broached: “Some companies misuse the concept of materiality. They intentionally record errors within a defined percentage ceiling. . . . When either management or the outside auditors are questioned about these clear violations of GAAP [generally accepted accounting principles], they answer sheepishly, ‘It doesn’t matter. It’s immaterial.’ ” This is an example of the attempts to increase the responsibility of both management and external auditors in the detection of fraud.

1.4 DETECTING AND PREVENTING FRAUD IN BOOKS OF ACCOUNT

1.4.1 The Auditor’s Duty to Detect Fraud

Accountants and auditors have had to contend with dishonest practices in accounting records since commercial activities were first recorded using the double-entry system. Since that time, there has developed a division of responsibility between accountants and auditors. In general, the accountants are responsible for the preparation of the financial statements under the double-entry system. The auditor has a duty to report whether the results of operations and balance sheets reflected in those financial statements have been prepared in accordance with GAAP.

In addition to the auditor’s duty to determine whether the financial statements have been prepared in accordance with GAAP, historically auditors have had a corollary responsibility to determine whether any material entries were false (that is, fraudulent). But there has been much debate about whether the latter was the peculiar province of the auditor or of management. In general, management is primarily responsible for detecting fraud in the accounting records.

According to SAS No. 99, the auditor is responsible for obtaining reasonable assurance that there is no material misstatement of the financial statements due to fraud. Federal courts seem to hold auditors to a higher duty of professional care than do state courts. But even state courts tend to impose a duty to detect fraud under some circumstances. In fact, a large number of professional malpractice suits brought against outside auditors in state courts involve allegations of undetected embezzlement or failure to detect materially fraudulent financial reporting.

² In the language of auditing standards, “reasonable” is intended to mean a high but not absolute level of assurance. This was clarified by SAS No. 104, “Amendment to Statement of Auditing Standards No. 1, Codification of Auditing Standards and Procedures.”

Recent events regarding very large public companies in the United States and elsewhere have heightened the sensitivity of the investing public to fraudulent financial reporting. It is safe to assume that the public has an expectation that auditors should consider the detection of material financial reporting fraud as an important part of their overall responsibility.

1.4.2 Fraud and Statement on Auditing Standards No. 99

SAS No. 99 carries the same title as its predecessor SAS No. 82 (AICPA, *Professional Standards*, vol. 1, AU secs. 110, 230, 312, and 316), but is clearly more far-reaching and more performance directing. The new provisions in SAS No. 99 include sections dealing with: brainstorming the risks of fraud while exercising increased professional skepticism; discussions with management and others as to whether they are aware of fraud; the use of unpredictable audit tests; and responding to management override of controls by requiring on every audit certain procedures responsive to detecting management override. The standard also used the term “should” often throughout the SAS, making clear that many of the recommended procedures were not just for consideration. The SAS also directed auditor attention to revenue recognition, a constant source of reported frauds and misstatements, noting that improper revenue recognition should ordinarily be “presumed” to be a fraud risk. The new auditing standard was effective for audits of financial statements for periods beginning on or after December 15, 2002.

Consideration of Fraud in a Financial Statement Audit

Fraud detection is not the primary objective of a financial statement audit. Yet the auditors' responsibility for detecting fraud is increasingly controversial. Earlier standards and writings addressing fraud tried unsuccessfully to imply that collusive fraud was somehow not within the scope of an audit, as it is difficult to detect. This line of reasoning withered away under public pressure and litigation until today, the auditor seeks to perform an audit with a low risk of the financial statement containing material misstatement, whether due to fraud or misstatement. With the release of SAS No. 99 in October 2002, the auditor now has more in-depth guidance to assist him and more is expected of the auditor in his role of detecting financial statement fraud. However, as a result of the *expectation gap*, the controversy still exists.

The expectation gap is the difference between what the public expects auditors to *do* and what auditors *in fact, do*. In other words, the public remains ignorant of the extent of the auditors' responsibilities. This is contrasted with the limitations of what auditors can reasonably expect to achieve. The general public and certain media, regardless of the efforts by the AICPA and other professional groups, still lack a true understanding of the role of the auditor.

Auditors should be fully aware of their responsibilities under the AICPA's SAS No. 99.

As stated in SAS No. 99, the auditor should consider the risk that the financial statements are materially misstated due either to unintentional error or fraud. Accordingly, the auditor must specifically consider factors that bear on the likelihood of fraud. The level of risk assessed may affect engagement staffing, extent of supervision, overall strategy, and the degree of professional skepticism applied. In addition, as stated above, SAS No. 99 includes additional procedures to be performed by the auditor in their role of detecting financial statement fraud.

Auditors' Responsibility

SAS No. 99 states, in part, "If the auditor believes that misstatements are or may be the result of fraud, but the effect of the misstatements is not material to the financial statements, the auditor nevertheless should evaluate the implications, especially those dealing with the organizational position of the person(s) involved." With this in mind, the crux of the auditor's responsibility in conducting a financial statement audit, as it relates to fraud, is to determine whether the financial statements are free from material misstatement. To achieve this, the following steps should be followed (bearing in mind the items noted above):

1. Assess the risk of material misstatement of the financial statements due to fraud and consider that assessment in designing audit procedures.
2. Inquire of management about its understanding of the risk of fraud and its knowledge of frauds perpetrated on or within the organization.
3. Plan and perform the audit to achieve reasonable assurance of detecting material misstatement of the financial statements due to fraud.
4. Consider whether misstatements detected during the audit are the result of fraud and, if so, evaluate the implications and communicate the matter to appropriate client personnel.
5. Document the facts that evidence the auditor's assessment of the risk of fraud and the auditor's response to the risks identified.

For a more detailed discussion of these steps, see SAS No. 99 attached on the Fraud Prevention Checklists CD-ROM accompanying this volume.

Types of Fraud

The misstatements most relevant to an audit of financial statements originate from two types of fraud:

1. *Fraudulent financial reporting.* The client intentionally misstates the financial statements through phony accounting records or documents, the misrepresentation or omission of significant information, or the misapplication of accounting principles. Fraudulent management usually directs or performs these activities. In most cases, there will be collusion between members of management and possibly third parties.
2. *Misappropriation of assets.* Client personnel steal entity assets and conceal the theft through misstatement of financial records. Fraudulent employees usually perform these activities.

The auditor has no responsibility for detection of misstatements, whether caused by error or fraud, that are not material to the financial statements. For example, the misappropriation of assets often is not material to the financial statements. However, the client might incorrectly expect that the auditor should detect all cases of fraud, whether or not the financial statements are materially misstated.

1.4.3 Fraud Auditing Versus Financial Statement Auditing

Financial statement audits are usually conducted in the context of an annual recurring function (a process which, to a certain extent, assumes a level of stability in the enterprise being audited). On the other hand, fraud audits are usually only commenced when there is

a concern that something very unusual has occurred. For example, allegations of fraud have been made, a whistleblower has come forward, accounting entries appear to be unsupported, or revenue recognition appears to have been accelerated.

Financial statement auditing is a methodology for evaluating the level of accuracy, timeliness and completeness of the recordings of business transactions. However, auditors do not review all transactions. Auditors use sampling and confirmation techniques to test accuracy, timeliness, and completeness. The purpose of testing is to determine whether transaction data are free of material error and to confirm that financial statements accordingly are free of material misstatement.

In 2007, new auditing standards will require auditors of private companies to consider internal controls more closely than past practice. While testing of controls is only required when the auditor's strategy is to rely on controls, SAS No. 109, "Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement," and No. 110, "Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained," clarify that understanding controls should consist of evaluating the design of the control procedures (including all five components of the COSO framework and IT controls) and examining evidence of their implementation (i.e., the control has been placed in operation). Auditors will not be able to "default" to high control risk and simply perform substantive tests. The COSO framework is considered an appropriate template for assessing the effectiveness of controls. These more specific requirements regarding controls may indeed provide more information for auditors on fraud risks and control deficiencies to enable more detections of fraud and misstatement.

Fraud auditing, while borrowing many techniques from financial statement auditing, is more a mind-set than a methodology. It relies on creativity (right-brain thinking) as much as it does on reasoning (left-brain thinking). It requires that the fraud auditor think, but not act, like a fraudster by considering the following:

- Where are the weakest links in the internal controls?
- How can the controls be circumvented and what financial statement elements are most at risk?
- How would a fraudster create support for false entries?
- What would be a motivator for management to commit fraud?
- How would management rationalize the fraud?

The more fraud auditors can learn to think like fraudsters, the more effective their efforts will be in detecting fraud.

Financial statement and fraud auditing also differ in the degree of concern for evidence of material error or misstatement. Although the materiality rule in financial statement auditing has its place partially in a cost-benefit context, materiality is not a guiding principle in fraud auditing. The amount of a visible fraud may be small, but frauds in books of account can be like icebergs—the biggest part is below the surface. Discovering even small discrepancies can reveal large issues. Are all frauds in the accounting records discovered on the basis of undetected discrepancies? No. Many frauds surface on the basis of allegations or complaints by coworkers, coconspirators, customers, competitors, suppliers, or prospective suppliers.

Fraud auditors often have a considerable advantage over financial statement auditors in digging out the root nature and amounts of fraud—fraud auditors almost always are working in environments where it is known that fraud exists. Discovery of a fraud in a financial statement audit is a relatively rare event, despite the impressions one might get from reading the newspapers. It is not uncommon for general auditors to examine the statements of dozens of clients over decades, and still not see or discover a fraud. The role of the fraud auditor is sometimes likened to that of a pathologist, where the end result is known, and the task is seeking the reason and source. The role of the financial statement auditor is similarly likened to that of a general practitioner of preventive medicine, where sometimes the signals about the patient's health are just not observable.

1.4.4 Fraud Auditors Versus Financial Statement Auditors

Skills of fraud auditors include:

- Reconstructing financial transactions through third-party sources
- Gathering and preserving accounting evidence for trial
- Testifying as expert witnesses
- Calculating net worth and living expenses
- Inspecting documents for authenticity, alteration, forgery, and counterfeiting
- Documenting a fraud case for criminal, civil, and insurance claim purposes
- Designing fraud scenarios, that is, imagining what a fraudster might think and do in situations in which internal controls are loose or not enforced and the fraudster has certain powers and authority over assets and accounting records

What distinguishes fraud auditors from financial statement auditors? In most respects, they are the same. Fraud auditors must make order out of what looks like chaos in books and records. Many of the supporting documents the fraud auditor must access for confirmation lie in the hands of third parties who might be reluctant to assist in the audit effort. Fraud auditors are usually retained after an alleged fraud is discovered or allegations have been made and are given the tasks of finding any additional fraud and validating or refuting the allegations of fraud.

1.4.5 The Risk of Fraud

Some organizations suffer more fraud than others. What increases the risk or exposure to loss from fraud in any organization? The answer depends on a number of factors. The incidence of fraud in the accounting records is distributed unevenly. Some industries, some companies, some occupations, and some individuals are higher risks than others.

High-risk industries are noted for intense rivalry, low profits, and unethical business practices. Some members of these industries are controlled by underworld figures and may enjoy sweetheart arrangements with corrupt labor unions. Disputes are often settled by bribes, or, when necessary, by force.

High-risk companies are noted for poor management, loose controls, loose cash, and loose business morality.

High-risk occupations provide easy access to cash and accounting records, and are often characterized by low pay, long hours, and job-related stress.

High-risk individuals are financially overburdened people with low self-esteem, addictive personalities (prone to gambling, substance abuse, and high living); are poor managers of their financial resources; have worked their way into positions of trust; and rationalize their thefts as “borrowing” or getting even for imagined exploitation. Such people often work long hours at their own discretion, and take no vacations for fear their defalcations might be discovered while they are away. A growing number of these thieves also keep elaborate records of their thefts. The records usually contain dates, amounts, and details of the conditions in their lives at the time the cash or property was taken. It is believed that such scrupulous bookkeeping is a defensive ploy. If they get caught, they think they can make a credible defense of their intention to return the money or property. This defense may cast doubt on one element of proof needed to convict, that is, the intent to permanently deprive the owners of their property. The same characteristics that make highly motivated entrepreneurs successful can also fuel greed and misdeeds and blur the line between the business and the entrepreneur, such that intervention in the financial reporting aspects of the business does not seem inappropriate. Smaller businesses with active management oversight face both a potential blessing: better monitoring; and a potential curse: management override of controls.

People commit crimes for a number of reasons. The main motives are economic, egocentric, ideological, and psychotic. The economic motive (need or greed) is the most common one found for the crimes of fraud, theft, and embezzlement.

In large corporations, with promotional policies and compensation plans geared to short-term bottom-line results and little else, a form of competitive greed can set in at the profit-center management level. Even well-managed companies have become victims of their own compensation designs. Therefore, falsifications of unit profits, revenues, and expenses have become a greater problem in the U.S. corporate landscape.

1.5 A NEW ENVIRONMENT FOR FRAUD RISK DETECTION AND ENFORCEMENT

The issue of fraud in financial reporting has been on the radar screen for a significant period of time. Throughout the go-go stock market period of the 1990's, sporadic reports of fraudulent financial reporting and the enrichment of executives continued to emerge. Standards setters in the U.S. and Internationally were well aware of this dangerous issue, and with the urging and support of the research and conclusions of Panel on Audit Effectiveness of the Public Oversight Board, in conjunction with the International auditing standards group under IFAC, undertook projects to strengthen the auditing standards to address this threat to security markets and preserve the credibility of the profession. The Public Oversight Board was part of a self-regulatory structure of the profession to provide oversight to the peer review process and provide timely and relevant guidance to the auditing profession. It was dissolved in 2002 as the concept of what became the Public Company Accounting Oversight Board (PCAOB) was being formed.

Those efforts, which ultimately led to Statement of Auditing Standards No. 99, “Consideration of Fraud in a Financial Statement,” resulted in more focused guidance than

in any previous standard on the issue, and often used the word “should,” implying that suggested procedures were more than just considerations, but were generally required.

1.5.1 The Winds of Change

In the timeframe in which SAS No. 99 was being deliberated, huge public company fraud scandals were being played out in the news media on a daily basis. Corporate names such as Enron, Worldcom, and others, will forever signal a period when the fundamental structure on which our economic system is based was seen to be threatened. Such was the threat that Congress passed a law, The Sarbanes Oxley Act of 2002 (July 30, 2002, 107 P.L. 204, §1, 116 Stat. 745), to restore confidence in the securities markets and strengthen the financial statement reporting process.

1.5.2 The Sarbanes-Oxley Act of 2002

The Sarbanes Oxley Act had a number of sections that had a profound effect on the business environment from its enactment. Some of those most directly relevant to fraud and financial reporting are:

- Title 1 established the Public Company Accounting Oversight Board as an independent overseer/standard setter for accounting and auditing for “issuers” (public companies). The SEC would oversee and approve the rules promulgated by the PCAOB. The PCAOB adopted the AICPA auditing standards (through SAS 101) as of April 2003, and began to modify that literature with Standards issued by the PCAOB.
- Title 2 established new auditor independence requirements, including the prohibition of certain services, the requirement that management boards pre-approve certain non-audit services, and established guidelines for periodic auditor rotation.
- Title 3 outlined corporate responsibilities including Section 303 which requires quarterly certifications regarding controls from responsible officials.
- Title 4 outlined enhanced financial disclosures to be made, including the requirement for companies and their auditors to assess and report on the effectiveness of internal controls (Section 404).
- Title 7 addressed corporate and criminal fraud accountability with specific penalties for fraudulent acts.
- Title 8 addressed white-collar crime penalty enhancements.
- Title 11 was directed at Corporate Fraud and Accountability.

The net sum was a sweeping law attempting to detect fraud and dissuade individuals and organizations from participating in or permitting frauds that could threaten the viability of business reporting and capital financing.

Other countries (e.g., Canada, UK, Japan) have moved to study and adopt some or all of the provisions of SOX, adapted to their country’s laws and business practices. Thus, anti-fraud sentiment today is clearly not limited to the U.S.

1.5.3 PCAOB Auditing Standard No. 2 and the COSO Framework

In 2004, the SEC approved the implementation of Auditing Standard No. 2, “An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of

Financial Statements” (AS 2) in response to the requirements in section 404 of the Sarbanes-Oxley Act (SOX). That standard established auditor requirements for conducting such an audit and significantly increased required procedures and the extent of auditor’s work over the requirements in the AICPA’s Attestation report on internal controls (AT 501).

Both SOX and AS 2 led to the defacto establishment of an existing control framework as “the standard” for companies and auditors. In 1992 the Committee of Sponsoring Organizations (COSO) issued a multi-volume guide entitled “Internal Control—Integrated Framework.” This document grew out of the work of the National Commission on Fraudulent Financial Reporting (the Treadway Commission), a group formed to consider corrupt foreign practices and improper political campaign practices. Following recommendations from a 1987 report, the COSO was formed to create such a controls framework. The COSO Framework is discussed more fully in Chapter 10.

When the COSO Framework document was initially released, some companies voluntarily undertook assessments of their controls, and new attestation standards were developed to guide auditors in reporting to the public on internal controls. Interest then waned in undertaking this voluntary task, as companies concluded that the annual cost of such reporting was not providing a measurable benefit to the organization.

The COSO Framework was readily available when Congress was seeking guidance on the approach companies should take to strengthen and report on internal controls. While other comprehensive frameworks exist (COCO in Canada, Turnbull in the UK), the COSO Framework is today’s virtual standard for internal controls.

The COSO Framework had sat virtually untouched since its release in 1992. Guidance in the original document was less extensive on fraud than what had emerged in the literature and auditing standards since that time. Notable in the 1992 work is that there is little mention of the role of systems and IT in conjunction with controls and fraud. Additionally, there was no guidance specifically directed to smaller companies—not necessarily a focus of the original report, but certainly a concern if SOX was to apply to all public companies.

The first two years of reporting on Internal Controls under Section 404 occurred under this framework. Only “accelerated filers” (the largest companies) were required to report on internal controls in 2004 and 2005. Data from Audit Analytics used for an academic research study indicate that of 2,641 2004 opinions on internal control, 386 (14.6%) received adverse opinions because of material weakness, and preliminary data for 2005 indicates about half that rate of adverse opinion in the next period for the group of second-year filers. While that rate may seem low and encouraging, it does not reflect the massive amount of remediation undertaken during the period of examination to be able to reach the “effective controls” conclusion “as of” the ending balance sheet date reflected in the report. “Large, well controlled” entities received quite an overhaul along the road to a clean audit opinion on controls. An E&Y survey published in 2005 indicated that 25% of the largest companies remediated over 500 controls in their first year of implementation. These issues are important, as deficiencies and weaknesses in controls provide “opportunity” for fraud, one of the three essential elements identified in SAS No. 99 in the “fraud triangle.”

1.5.4 Issues for Smaller Entities and Private Companies

In July 2006, the COSO released a report entitled “Internal Control over Financial Reporting—Guidance for Smaller Public Companies” with welcome enhancements to the original guidance. While re-affirming that the basic principles of control are the same for smaller and larger entities, this document provides some simpler tools for analysis and some additional guidance on integrating fraud, systems, and IT considerations into the assessment of controls. This is in anticipation of the initially deferred smaller firms and Foreign Issuers (over 10,000 of them) having to report on internal controls beginning in 2007.

In 2007, a suite of new auditing standards (SAS No. 104 through SAS No. 111) will become effective for private companies. The significance of this event is that the new standards require the auditor to assess the design of internal controls and see that the controls have been implemented (but do not require the testing of controls unless that is part of the audit strategy). These standards, as has been true since SAS No. 55 and reflected in Codification section AU 319 are based on the COSO Framework. Under existing practice many auditors defaulted to “high” control risk, and performed a minimal assessment of controls for many entities, going on to rely mostly on substantive audit procedures as a basis for the opinion on the financial statements. This will no longer be permitted under the new standards. Auditors will assess the controls design and implementation and under SAS No. 112 (Communicating Internal Control Matters Identified in an Audit), effective in 2006, report identified material weaknesses and significant deficiencies to “those charged with governance.” It is anticipated that the additional focus on controls on all audits will reveal and report to management in a formal way more deficiencies than ever before. This standard will be effective for all audits conducted under AICPA standards, estimated to be more than 350,000 audits of private, non profit, and government entities.

Smaller businesses are not immune to fraud loss. The 2006 ACFE “Report to the Nation” indicates that the median fraud loss was \$190,000 to organizations with fewer than 100 employees.

Nonprofit entities and governments have also taken an active interest in the issue of reporting on internal controls and are providing input to the Auditing Standards Board on its revision of its Internal Control Reporting attestation standard (AT Section 501). An exposure draft of this revised standard was posted for comment, and is expected to be finalized in 2006. The devastating impact of alleged improprieties at the American Red Cross demonstrate how fraud or allegations of fraud can harm the mission or de-commission a nonprofit organization—even the largest ones.

Even among the “accelerated filer” group, smaller entities seemed to have a higher incidence of adverse reports. Most are expecting that the next tier of public companies trying to report on internal controls will have a more difficult time than the larger companies did due to:

- The lack of formality in the existing controls
- Less documentation of internal controls
- The lack of extensive internal audit resources
- The continuing lack of urgency in preparing for this reporting requirement

- The lack of financial resources to perform the assessment, hire expert assistance and pay additional professional fees for various legal and auditing services

While the close involvement of management with the business is sometimes cited as an asset in preventing misstatements and fraud, it can be a liability when management override is a risk.

What is clear is that we are at a crossroads in terms of the old and new order and the “war on error” (due to poor controls and fraud).

1.5.5 Post Sarbanes Implementation Effectiveness

It may indeed be too soon to evaluate the impact of the Sarbanes-Oxley legislation and other forces set in motion by that. Frauds continue to be found such as a fraud at Refco, recently discovered by the auditors Grant Thornton LLP. Enforcement actions and prosecutions of executives have had mixed success to date, but are prominent in the business news. As of September 2006, nearly 100 firms are embroiled in SEC and internal investigations and restatements due to backdating or spring-loading the dates of stock option awards. Now that stock options can result in compensation expense and are not just a disclosure item, seemingly broad and longstanding inappropriate corporate policies and practices are coming to light. Auditors are now expanding their procedures to cover such possible schemes in other businesses.

The bottom line may be that the forces at work today will result in the earlier detection of frauds as a result of auditing procedures, and serve as a deterrent to those tempted to massage the numbers or gain unfair advantage.

1.6 RISK MANAGEMENT CHECKLIST

Table 1.2, “Risk Management Checklist,” is designed to assist CPAs in assessing and managing the risk of fraud in their organizations and in those of their clients. Generally, all *no* answers require investigation and follow-up, the results of which should be documented. The final section entitled “Specific Risk Factors” generally requires investigation and follow-up for all *yes* answers. Use the “Ref” column to cross-reference any additional documentation to the appropriate working papers.

Companies also can use this checklist to self-assess their fraud awareness and fraud readiness. The Exhibit to SAS No 99 also provides a discussion of anti-fraud programs and controls from the company perspective.

The checklist is intended for general guidance and information only. Use of the checklist does not guarantee the prevention or detection of fraud and is not intended as a substitute for audit or similar procedures. Those with vital concerns about fraud prevention or who suspect fraud should seek the advice of a competent fraud practitioner.

TABLE 1.2 RISK MANAGEMENT CHECKLIST

| Risk Management Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-------|
| 1. Does the organization have an adequate level of fraud awareness, and are appropriate policies in place to minimize fraud risk, specifically: | | | | |
| a. Generic risk factors | | | | |
| ● Has the organization assigned each employee a maximum “opportunity level” to commit fraud, that is, has management asked itself the question, “What is the maximum amount this employee could defraud the organization, and does this represent an acceptable risk?” | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Has the organization set a catastrophic opportunity level; that is, has management asked itself the question, “Have we ensured that no single employee—or group of employees in collusion—can commit a fraud that would place the organization in imminent risk of survival?” | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Does the organization have a policy of immediately dismissing any employee who has committed fraud? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Does the organization have a policy of reporting all frauds to the authorities and pressing charges? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● For all frauds experienced by the organization in the past, has management evaluated the reasons that led to the fraud and taken corrective action? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| b. Individual risk factors | | | | |
| ● Does the organization have a corporate mission statement, which includes an objective of good citizenship or the maintenance of good standing in the community? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Does the organization have a written code of ethics and business conduct (see the checklist in Chapter 2 for details)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Does the organization conduct ethical and security training for new employees and periodic updates for existing employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Does management set the right example; that is, does it follow the organization’s mission statement, code of ethics and business conduct, and other policies of the organization; and is it clearly seen to be doing so by employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Does the organization’s culture avoid characteristics that promote unethical behavior, for example, high or even hostile competitiveness within the organization that might push employees to the point of burnout; pointless rigid or petty policies, or both; overcentralization of authority? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

(continued)

TABLE 1.2 (continued)

| Risk Management Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| <ul style="list-style-type: none"> ● Does the organization have a fraud hotline or other communication vehicle for reporting issues? Is the hotline number communicated or easily accessible to employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Has the organization communicated the Whistleblower Protections of the Sarbanes-Oxley Act or any other applicable government regulations to employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Do the organization's hiring policies, to the extent possible, seek out individuals of high moral character and weed out those of low moral character (see the checklist in Chapter 3)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Does the organization use screening and/or testing procedures for especially sensitive positions; for example, psychological tests, drug tests, or lie detector tests, or a combination of all three, where permitted by law? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Does the organization provide or encourage counseling, or both, for employees with personal problems, for example, alcohol and drug abuse? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Does the organization have fair policies in the area of employee relations and compensation, for example, salaries, fringe benefits, performance appraisal, promotions, severance pay; and do these policies compare favorably with those of competitors and promote an environment that minimizes disenchantment and other similar motives to commit fraud? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Does the organization have fair mechanisms in place for dealing with employee grievances? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Does the organization, as a feedback mechanism concerning employee relations' policies, conduct exit interviews with departing employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <p>c. Overall risk factors</p> | | | | |
| <ul style="list-style-type: none"> ● Does the organization exhibit an awareness of fraud and its possible manifestations, for example, signs of employee problems such as drug addiction, employees who are living beyond their means, etc.? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <p>2. Does the organization have an adequate system of internal controls, specifically:</p> | | | | |
| <p>a. Internal control</p> | | | | |
| <ul style="list-style-type: none"> ● Has the organization explicitly considered the need for fraud prevention in the design and maintenance of the system of internal controls? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

TABLE 1.2 (continued)

| Risk Management Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-------|
| b. Control over physical and logical access | | | | |
| ● Does the organization have a policy of locking doors, desks, and cabinets after hours and when unattended, especially in areas with valuable assets including files and records, for example, personnel and payroll, customer and vendor lists, corporate strategies, marketing plans, research? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Does the organization use IDs and passwords, for example, for computer files? Are these passwords changed periodically and de-activated on a timely basis when employees leave or are terminated? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Does the organization state and enforce a policy that restricts access to those requiring it for job performance, including a strict policy against employees allowing access to unauthorized personnel, for example, by loaning keys or sharing passwords? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Has the organization installed, for especially sensitive areas, the computerized security or electronic surveillance systems, or both? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Does the workplace <i>appear</i> to an impartial observer to have adequate access controls? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| c. Job descriptions | | | | |
| ● Does the organization have written, specific job descriptions? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Are job descriptions adhered to? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Does the organization have an organization chart that reflects and is consistent with the job descriptions of its employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Are incompatible duties segregated, for example, the handling of valuable assets—especially cash—and related records? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Does the organization properly segregate the purchasing functions, that is, ensuring that one individual cannot requisition goods or services, approve and make the related payment, and access accounts payable records? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Are especially sensitive duties duplicated, for example, the double-signing of checks over a specified amount? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Do job descriptions specify that employees must take annual vacations? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

(continued)

TABLE 1.2 (continued)

| Risk Management Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| <ul style="list-style-type: none"> ● Is the overall process of formulating job descriptions integrated with adequate consideration to the importance of fraud prevention? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Regular accounting reconciliations and analyses | | | | |
| <ul style="list-style-type: none"> ● Are all bank accounts reconciled? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Are all accounts receivable reconciled, for example, month to month, general ledger to subledger? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Are all accounts payable reconciled, for example, month to month, general ledger to subledger? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Has the organization performed a variance analysis of general ledger accounts, for example, budget to actual, current year versus prior year? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Has the organization performed a vertical analysis of profit and loss accounts, that is, as a percentage of sales against historical or budget standards, or both? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Has the organization performed an analysis of detailed sales and major expenses, for example, by product line or geographic territory? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Supervision | | | | |
| <ul style="list-style-type: none"> ● Do supervisors and managers have adequate fraud awareness, that is, are they alert to the <i>possibility</i> of fraud whenever an unusual or exceptional situation occurs, such as supplier or customer complaints about their accounts? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Do supervisors and managers diligently review their subordinates' work, for example, accounting reconciliations, and redo the work when appropriate? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Does close supervision adequately compensate against the increased risk of fraud in smaller businesses or where an inability to divide duties exists. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Is supervisory or management override prohibited and are others within the firm alert to the fraud risks associated with management override? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Audit | | | | |
| <ul style="list-style-type: none"> ● Is there an internal audit function? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Does the internal audit function perform regular checks to ensure that fraud prevention mechanisms are in place and operating as intended? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Are external audits performed on a regular basis, for example, quarterly for larger businesses and public companies? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

TABLE 1.2 (continued)

| Risk Management Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| ● Are the timing demands of management on external auditors reasonable? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Do external auditors receive full cooperation from management with respect to their work in general and fraud matters in particular, for example, through the audit committee? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Has the organization specifically addressed the following fraud prevention issues: | | | | |
| a. Ethical Environment | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Risk Financing | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Computer Security | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| Specific Risk Factors | | | | |
| Fraudulent Financial Reporting | | | | |
| 1. Is the organization's financial stability or profitability threatened by economic, industry, or entity operating conditions? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. Is there excessive pressure on management or management incentives related to reaching earnings expectations or certain revenue benchmarks? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Are there significant balances in the financial statements which are based on subjective management estimates? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 4. Are there significant cash balances or significant transaction activity in overseas banks in tax havens such as the Cayman Islands or the Channel Islands? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 5. Does the entity have an overly complex organizational structure or a large number of complex subsidiaries? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 6. Does management consistently use materiality as a basis for justifying marginal or inappropriate accounting methods? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| Misappropriation of Assets | | | | |
| 1. Are there planned layoffs which have become known by employees throughout the company? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. Are the company's assets easily convertible and are they physically available to employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Is there insufficient segregation of duties related to check writing, wiring of funds, or cash? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 4. Are the controls over the accounting system or automated records inadequate? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 1.2 *(continued)*

| Risk Management Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| 5. Are audits of cash, inventories and other saleable or useable goods under employee oversight conducted periodically and unpredictably? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 6. Do certain employees exhibit a change in behavior to a disagreeable or discontent state? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |



CHAPTER 2:

Promoting an Ethical Environment

- 2.1 Ethics: A Framework 3
 - 2.1.1 Overview..... 3
 - 2.1.2 Ethics at Work 4
 - 2.1.3 Promoting an Ethical Environment..... 5
 - 2.1.4 Ethics and Information Technology.....12
- 2.2 Ethical Environment Checklist.....16

CHAPTER 2:

Promoting an Ethical Environment

2.1 ETHICS: A FRAMEWORK

An ethical environment is a key element in any effective prevention strategy. This chapter will acquaint you with the field of applied ethics, provide essential tools for promoting an ethical environment within an organization, and conclude with a diagnostic tool that you can use when evaluating an organization's current ethical status.

2.1.1 Overview

Ethics—derived from the Greek *ethos*, meaning character or custom—is a very broad term referring to principles or standards of human conduct. Ethics has been, and continues to be, one of the key concerns of all religions, schools of philosophy, sciences, liberal arts, professions, and political movements. Moses, Confucius, Plato, Aristotle, Kanto, and many others devoted a great deal of their recorded teachings to the subject of ethics. It is impossible to engage in any human endeavor, including business, without entering the field of ethics.

Applied Ethics

Applied ethics is the science devoted to the study of the “walk,” rather than the talk, of ethics. According to Lisa H. Newton, in her text *Doing Good and Avoiding Evil: Principles and Reasoning of Applied Ethics*, “Applied ethics, then, is the field that holds ethical theory accountable to practice and professional and business practice accountable to theory.” It’s where the rubber meets the road.

Personal Versus Organizational Ethics

Whose principles and standards should we adopt? There remains much confusion about this fundamental question. Some believe that ethics are a matter of personal choice. Therefore, any attempt to establish a code of ethics, or conduct, would result in a narrow flight of parochial fancy that would be so patently offensive to so many, it would render itself immediately irrelevant. Others believe that a kind of universal genetic code of ethics or conduct exists. This theory suggests that we are all born with an inherent sense of right and wrong. So, any artificial code of ethics is unnecessary and would be flawed in any way in which it conflicted with the natural code. Both groups believe it would be wrong for any organization to impose ethical standards on its members, employees, or other stakeholders. Nothing could be further from the truth.

It is an organization's right and duty to clearly communicate its values and expectations regarding the conduct of its affairs to all its stakeholders. Employees or members may freely choose to join, or not to join, any given organization. But, once individuals choose to join an organization, they assume a duty to respect the organization's values and abide by its code of conduct.

Ethics and the Law

When confronted about unethical behavior, many people will point out that their actions were not illegal. This would be roughly analogous to saying that because a person follows the rules of law, he or she would be an excellent judge. According to the *Professional Ethics for Certified Public Accountants* (a publication of the California Certified Public Accountants Foundation for Education and Research) "Laws and rules establish minimum standards of consensus impropriety; they do not define the criteria of ethical behavior."

2.1.2 Ethics at Work

In the Professions

Most, if not all, recognized professions have developed written codes of ethics, professional conduct, or both. They also have implemented means to assure that members of the profession abide by these codes. Violators are usually disciplined or expelled, sometimes in public proceedings, to demonstrate the profession's commitment to its code and willingness to effectively police itself.

Some would argue that the professions became interested in ethics for entirely selfish reasons. They see the rise of successful plaintiffs' litigation in the 1970s as a key motivator in the promulgation of professional codes of ethics and conduct. They also point out that, during the 1980s and 1990s, the federal government demonstrated an interest in playing an increased role, including the actual promulgation of codes of conduct, in the regulation of professions. The AICPA has written and rewritten its code of professional conduct many times during the past 100 years or so. In fact, according to *Professional Ethics for Certified Public Accountants*, a complete restatement of the code was made in 1973.

Whatever the motivation, professional codes of conduct have been effective. The reason is simple: if you do not abide by the ethics code of your profession (medical, legal, etc.) you may risk being expelled from your professional organization, thus losing the right to practice and earn a living. Coupling this reason with the profession's corporate interest in maintaining its standing and authority, and minimizing its own exposure to litigation and intrusion by regulatory agencies or others, demonstrates the steps taken by many professional organizations toward promoting an ethical environment.

But, how do we apply this model to businesses, including professional firms?

Business Ethics

Should business be concerned with ethics? The answer was not always a unanimous *yes*. Who hasn't heard the appropriated maxim: All is fair in love and business. You may recall Shakespeare's merchant and Dickens' Fagan as examples of at least the perception of business motives in western society. In this country, tales of the robber barons of the nineteenth century suggest that business ethics were not at the top of the enterprise success-factor list. That was then, but what about now? As recently as the 1970s, mainstream

economist Milton Friedman said that the only obligation of a business is to make a profit. This became dogma in American business schools in the 1970s and 1980s.

So, why should business be concerned with ethics today? One could argue that after November 1991—the effective date of the federal sentencing guidelines for organizations—business became concerned with ethics in order to guard against huge fines and penalties. But there are other, pragmatic reasons for business to be concerned with ethics:

Enlightened self-interest. According to the *Professional Ethics for Certified Public Accountants*, a business needs to avoid scandals, keep government off its back, protect itself from internal corruption, avoid fines and penalties, and keep its executives out of jail. Also, there is the value of a good corporate image, the internal cost of investigations and legal fees, the value of good employee morale, and the impact of wrongdoing on the share value of public companies to consider. In fact, ethics may have a great deal more to do with making a profit than Mr. Friedman imagined.

2.1.3 Promoting an Ethical Environment

The Tone at the Top

You've heard it before and it must be said again. The tone of upper management is most important in the field of ethics. Ethics will not suffer senior management's clever rationalization or thinly veiled hypocrisy. Fortunately, or unfortunately, ethics always comes down to a simple choice of right over wrong. Even the most learned defense of improper conduct in the executive suite would fail the ethics test. If the bosses aren't ready to walk the talk, the process simply will not work.

Senior management must be made aware of this essential element. Some will raise objections about the cost of an ethics program or its potential negative impact on revenue. Even today, the best way to communicate the value of an effective ethics program is to quantify the cost of not having an ethics program. Statistics and examples abound. According to an Association of Certified Fraud Examiners report, it was estimated that in 1996 U.S. organizations lost over \$400 billion to occupational fraud and abuse. But, to bring the point home, you need look no further than your favorite daily business journal. Virtually every issue contains stories of businesses and other organizations that have been victimized through fraud and paid dearly for it. Those businesses that allegedly "benefited" from the fraud end up losing the most.

The Current Situation

All ethics, like all politics, are local. Resist the temptation to run out and "buy" someone else's ethics program for your organization. An ethical environment flows from an ethics program that is tailored to the organization. If you try to develop a rule in advance for every situation, you will fail. If you try to fix things that are not broken, you will fail. Finally, if in the process of installing your new, super-deluxe, off-the-shelf ethics program, you communicate your distrust of employees and other stakeholders to them, they, in turn, will justify that distrust.

For all of these reasons, begin by analyzing your individual organization. Involve everyone in the process. Get their input. Develop a brief statement (mission statement) of the organization's core values and mission.

Perform a diagnostic to identify weak and strong areas of ethical conduct within the organization. You should consider using the Ethical Environmental Checklist at the end of this chapter, or you could use this checklist as a template to develop a diagnostic tool of your own. Once you compile the results of your diagnostic exercise, analyze the results, make any necessary decisions, and begin designing the program.

Designing the Ethics Program

The most important requirement when promoting an ethical environment is having a written code of ethics and business conduct. A written code helps to set the right ethical tone within an organization. Figure 2-1 is an example of a written mission statement.

Figure 2-1. A Written Mission Statement

Mission Statement

The Organization's mission is to provide the highest quality goods and services to its customers; to strive at all times for market leadership and in so doing, to benefit the Organization's shareholders and its employees.

The Organization is committed to a policy of fair dealing and integrity in the conduct of all aspects of its business. This commitment is based on a fundamental belief in law, honesty and fairness. The Organization expects its employees to share its commitment to high legal, ethical and moral standards.

This Code of Business Conduct is mandatory, and the Organization expects full compliance by all of its employees and by its subsidiaries under all circumstances. The Organization will monitor compliance, and any violation of the Code may result in disciplinary action that could include termination of employment.

Employees uncertain about the application of the Code should consult with their superior. Similarly any employee who becomes aware of, or suspects, a contravention of the Code, must promptly advise his or her superior, or report the matter directly to Human Resources, Internal Audit or the Law Department.

Figure 2-2 is an example of an organizational code of conduct, which includes definitions of what is considered unacceptable, and the consequences of any breaches thereof. Note that figure 2-2 is only an example. The specific content and areas addressed in your mission statement and code should flow from your own analysis of your organization.

Figure 2-2. An Organizational Code of Conduct

Organizational Code of Conduct

The Organization and its employees must, at all times, comply with all applicable laws and regulations. The Organization will not condone the activities of employees who achieve results through violation of the law or unethical business dealings. This includes any payments for illegal acts, indirect contributions, rebates and bribery. The Organization does not permit any activity that fails to stand the closest possible public scrutiny.

All business conduct should be well above the minimum standards required by law. Accordingly, employees must ensure that their actions cannot be interpreted as being, in any way, in contravention of the laws and regulations governing the Organization's worldwide operations.

Employees uncertain about the application or interpretation of any legal requirements should refer the matter to their superior, who, if necessary, should seek the advice of the Law Department.

General Employee Conduct

The Organization expects its employees to conduct themselves in a businesslike manner. Drinking, gambling, fighting, swearing and similar unprofessional activities are strictly prohibited while on the job.

Employees must not engage in sexual harassment, or conduct themselves in a way that could be construed as such, for example, by using inappropriate language, keeping or posting inappropriate materials in their work area, or accessing inappropriate materials on their computer.

Conflicts of Interest

The Organization expects that employees will perform their duties conscientiously, honestly and in accordance with the best interests of the Organization. Employees must not use their position or the knowledge gained as a result of their position for private or personal advantage. Regardless of the circumstances, if employees sense that a course of action they have pursued, are presently pursuing or are contemplating pursuing may involve them in a conflict of interest with their employer, they should immediately communicate all the facts to their superior.

Outside Activities, Employment and Directorships

All employees share a serious responsibility for an Organization's good public relations, especially at the community level. Their readiness to help with religious, charitable, educational and civic activities brings credit to the Organization and is encouraged. Employees must, however, avoid acquiring any business interest or participating in any other activity outside the Organization that would, or would appear to—

(continued)

Figure 2-2. (continued)

- Create an excessive demand upon their time and attention, thus depriving the Organization of their best efforts on the job.
- Create a conflict of interest—an obligation, interest or distraction—that may interfere with the independent exercise of judgment in the Organization's best interest.

Relationships with Clients and Suppliers

Employees should avoid investing in or acquiring a financial interest for their own accounts in any business organization that has a contractual relationship with the Organization, or that provides goods or services, or both to the Organization, if such investment or interest could influence or create the impression of influencing their decisions in the performance of their duties on behalf of the Organization.

Gifts, Entertainment and Favors

Employees must not accept entertainment, gifts, or personal favors that could, in any way, influence, or appear to influence, business decisions in favor of any person or organization with whom or with which the Organization has, or is likely to have, business dealings. Similarly, employees must not accept any other preferential treatment under these circumstances because their position with the Organization might be inclined to, or be perceived to, place them under obligation.

Kickbacks and Secret Commissions

Regarding the Organization's business activities, employees may not receive payment or compensation of any kind, except as authorized under the Organization's remuneration policies. In particular, the Organization strictly prohibits the acceptance of kickbacks and secret commissions from suppliers or others. Any breach of this rule will result in immediate termination and prosecution to the fullest extent of the law.

Organization Funds and Other Assets

Employees who have access to Organization funds in any form must follow the prescribed procedures for recording, handling and protecting money as detailed in the Organization's instructional manuals or other explanatory materials, or both. The Organization imposes strict standards to prevent fraud and dishonesty. If employees become aware of any evidence of fraud and dishonesty, they should immediately advise their superior or the Law Department so that the Organization can promptly investigate further.

When an employee's position requires spending Organization funds or incurring any reimbursable personal expenses, that individual must use good judgment on the Organization's behalf to ensure that good value is received for every expenditure.

Organization funds and all other assets of the Organization are for Organization purposes only and not for personal benefit. This includes the personal use of organizational assets such as computers.

Figure 2-2. (continued)

Organization Records and Communications

Accurate and reliable records of many kinds are necessary to meet the Organization's legal and financial obligations and to manage the affairs of the Organization. The Organization's books and records must reflect in an accurate and timely manner all business transactions. The employees responsible for accounting and record-keeping must fully disclose and record all assets, liabilities, or both, and must exercise diligence in enforcing these requirements.

Employees must not make or engage in any false record or communication of any kind, whether internal or external, including but not limited to—

- False expense, attendance, production, financial or similar reports and statements
- False advertising, deceptive marketing practices, or other misleading representations

Dealing With Outside People and Organizations

Employees must take care to separate their personal roles from their Organization positions when communicating on matters not involving Organization business. Employees must not use organization identification, stationery, supplies and equipment for personal or political matters.

When communicating publicly on matters that involve Organization business, employees must not presume to speak for the Organization on any topic, unless they are certain that the views they express are those of the Organization, and it is the Organization's desire that such views be publicly disseminated.

When dealing with anyone outside the Organization, including public officials, employees must take care not to compromise the integrity or damage the reputation of either the Organization, or any outside individual, business, or government body.

Prompt Communications

In all matters relevant to customers, suppliers, government authorities, the public and others in the Organization, all employees must make every effort to achieve complete, accurate and timely communications—responding promptly and courteously to all proper requests for information and to all complaints.

Privacy and Confidentiality

When handling financial and personal information about customers or others with whom the Organization has dealings, observe the following principles:

1. Collect, use, and retain only the personal information necessary for the Organization's business. Whenever possible, obtain any relevant information directly from the person concerned. Use only reputable and reliable sources to supplement this information.

(continued)

Figure 2-2. (continued)

2. Retain information only for as long as necessary or as required by law. Protect the physical security of this information.
3. Limit internal access to personal information to those with a legitimate business reason for seeking that information. Only use personal information for the purposes for which it was originally obtained. Obtain the consent of the person concerned before externally disclosing any personal information, unless legal process or contractual obligation provides otherwise.

When designing your program, implementation strategy and training, remember the following bit of wisdom:

Give a person a fish and he or she will be able to eat today. Teach a person to fish and he or she will be able to eat for a lifetime.

If you try to create a rule for every ethical dilemma, your people will focus on how to fit their decisions to the rules. On this premise, if there is no rule, there is no problem. If you train your people to make ethical decisions for themselves, however, they will focus on doing just that.

Training and Communication

After writing your organization's code of ethics and business conduct, ask everyone to read it and have them confirm in writing that they have done so and understood the content. Keep a record of this acknowledgment.

You should consider seminar training for all employees and agents. The training doesn't have to be long and complicated. Use the KISS (Keep It Simple Stupid) method to develop your ethics curriculum. Instead of giving them rules, give them tools. These tools can be as simple as a list of broad principles to follow and questions to ask when making decisions.

In *Policies and Persons: A Case Book in Business Ethics*, John B. Mathews and coauthors suggest the following tools.

1. Avoid harming others.
2. Prevent harm to others.
3. Respect the rights of others.
4. Do not lie or cheat.
5. Keep promises and contracts.
6. Obey the law.
7. Help those in need.
8. Be fair.

So, when a considered action may raise serious ethical questions, try applying the generalized criteria. For example, you can use the guidelines above and ask yourself the following specific questions.

1. Does the considered action violate any of the following?:
 - A criminal law
 - A civil law
 - A company policy
 - A professional code
 - An industry code
 - My personal values
2. Is the action fair, just, and equitable to all parties?
3. Does the action serve the common good and the public's interest?
4. Does it provide the greatest good for the greatest number?
5. Does it do the least harm to the greatest number?
6. Does it cost more than its social benefits?
7. Would you like it if it were done to you (known as "The Golden Rule")?
8. Would an ethical role model (for example, your parent, priest, or minister) approve of this act?

Enforcement

As discussed in chapter 1, an effective prevention strategy demands there be some adverse consequences when an employee is caught committing fraud (for example, dismissal of the employee and the pressing of charges). Similarly, there also must be some adverse consequences—commensurate with the severity of the breach—when an employee contravenes an organization's stated policies, and in particular its code of ethics and business conduct. For severe breaches, or for repeat offenders, dismissal may be an appropriate consequence and the organization's policies should so state.

To ensure that all employees are aware of their responsibilities, organizations should require that the staff sign an annual declaration stating they are aware of the company's code of ethics and business conduct policies, and confirming they have complied in the past and will continue to do so.

Employee Hiring and Employee Relations

Ultimately, the employees, not the organization's policies, create a good ethical climate. Employee hiring practices and employee relations are therefore important fraud prevention variables. The Ethical Environment Checklist (at the end of this chapter) provides a fairly comprehensive list of the factors to consider.

Generally, organizations face a balancing act. On the one hand, they must minimize the risk of fraud and be cost-effective in employee remuneration. On the other hand, they must promote an open environment in which employee morale and creativity flourish, while employees feel rewarded for their efforts. Tipping the scale too far to one side or the other can lead to problems, or reduce the competitiveness of an organization, or both. Organizations can achieve success at a point somewhere in between and only through the good judgment of management.

2.1.4 Ethics and Information Technology

The ever-accelerating information revolution—particularly during the latter half of the twentieth century—has raised special ethical issues. In particular, makers, distributors, owners, managers, and users of information resources have ethical responsibilities for the products and services that they create, own, sell, manage, and use. The ethical issues raised by information technology include the following:

- Privacy
- Piracy
- Safety and health
- Data security
- Data integrity
- Competence
- Honesty
- Loyalty
- Fairness

Privacy

A myriad of both private and public-sector organizations collect data for a wide variety of purposes. The U.S. government alone has gathered and stored four billion records on individuals. The development of database management software for personal computers has extended these capabilities to anyone with a few hundred dollars. Although databases have grown explosively, controls over access and disclosure of confidential data have not kept pace. Unauthorized access to databases and disclosure of confidential information contained therein are commonplace.

There are legal constraints on the improper collection and dissemination of personal data in the United States and Canada, embodied in their respective Constitutions, Supreme Court decisions, tort law, and in federal and state privacy and consumer rights enactment. However, these laws and rulings are not sufficiently clear to reach consensus. For example, on the question of access to personal history databases versus an individual's right of privacy, an ethicist might ask the following.

- Who is collecting the data?
- For what use are the data being collected?
- How, to whom, and for what purpose will the data be disseminated?
- How well protected is that data against unauthorized access and disclosure?
- How accurate, complete, and timely are the data?
- What degrees of confidentiality should be accorded to such disparate data as medical, psychiatric, credit, employment, school and criminal records?

If medical records were considered the most confidential of the lot, the ethical standard for the care accorded such data would be higher; that is, medical records should be gathered, stored, and disseminated with great care and caution.

Piracy

Software piracy signifies that the creative work of another has been used or duplicated without permission or payment of royalty, or both. The definition assumes that the software's creator has complied adequately with the legal requirements of the federal copyright law. Therefore, the software pirate commits an act of infringement and may be civilly sued for damages, criminally prosecuted, or both.

Software piracy is probably the most common breach of ethics in the field of information technology. For each software program sold, developers claim that another two to five copies are bootlegged. The lost royalties of developers are staggering. Some thieves rationalize that software prices are too high and that the developers are large and will not miss the lost royalties. In reality, the software industry has become increasingly competitive and losses to piracy can have a serious impact on a company's viability. Moreover, even the largest and most profitable developers have a right to seek a fair price and return for their development efforts, the costs incurred and the risks taken.

Safety and Health

The widespread use of computers in today's information-driven economy has contributed to and in some instances created, unique safety issues that can be divided into the following two distinct categories:

1. Accidents resulting from the use of computer-controlled systems
2. Occupational health and safety problems for users caused by long-term or improper use of computers, or both

Computer-controlled systems safety issues—The accelerated pace of technological change in this century has resulted in an exponential increase in new industries with many innovative products and processes. Dangerous substances and sensitive information are being handled on an unparalleled scale. New systems are being built—using computers to control them—that have the capacity to cause extensive destruction of life and the environment. A single accident could be catastrophic. Computers now control most safety-critical devices and they often replace traditional hardware safety interlocks and protection systems. Even when hardware protection devices are retained, software is often used to control them. Because of the explosive increase in the use of, and reliance on computers, methods to ensure the safety of computer-controlled systems have not always kept pace with the development of these very systems. Ethicists recognize there is a serious danger of overreliance on the accuracy of computer outputs and databases. The nonoccurrence of particular types of accidents in the past is no guarantee that they will not take place in the future. Software and hardware developers and information technology professionals alike must recognize their moral and ethical responsibilities. We can't wait to learn from experience, but must attempt to anticipate and prevent accidents before they occur.

Computer-related safety and health issues—Today's computer operators, particularly heavy users, may develop problems caused by the repetitive motions used daily in operating their machines. The most common problem is repetitive stress injury (RSI), in which workers experience moderate to severe pain in the muscles and joints of the hands, wrists, arms, shoulders, neck and back. RSI can be caused by carpal tunnel syndrome (CTS), irritation of the nerves leading to the fingers due to the prolonged use of a keyboard while the body is in an unnatural or strained position. RSI can be completely incapacitating, sometimes

requiring surgery if not treated early. According to Patrick G. McKeown in his text, *Living With Computers*, these injuries are epidemic in computer-related jobs; RSI constitutes more than 60 percent of work injuries and costs employers \$20 billion annually. Other health-related problems involve radiation emissions from the monitor and eyestrain from watching the screen for long periods of time without proper lighting or screen glare protection, as well as noise-induced problems caused by the pervasive low-level noise in today's computer environment.

Because of the enormous costs resulting from worker's health and safety issues, many organizations are opting for ergonomically designed work environments. Ergonomics, or human factor engineering, is the science of designing equipment for the workplace to keep employees safe and healthy while they work, which usually results in fewer physical complaints, higher employee morale and increased productivity. An ergonomically designed work area considers the following factors:

- The height and position of the monitor
- The height and angle of the keyboard
- A fully adjustable chair that provides lower back and adjustable arm support and height adjustment capabilities
- A keyboard that allows users to work with their hands in a natural position
- A mouse designed for either a left- or right-handed user with wrist support
- An anti-glare monitor screen
- Noise reduction measures
- Proper indirect and task lighting
- Adequate ventilation

In addition, employers should emphasize the proper use of equipment, encourage regular breaks, and provide stress reduction training for employees to further minimize the risk factors related to RSI and related injuries. In an ethical environment management is sensitive to the well-being of regular employees and applies the same principles to part-time workers and support staff.

Data Security

The protection of personal information from unauthorized access, disclosure, and duplication obligates a database owner to—

- Formulate and enforce standards for the proper use of the data.
- Communicate to, educate, and train users about their responsibility for protecting such information.
- Plan for likely contingencies.
- Establish adequate security controls.
- Monitor control exceptions.

Data Integrity

An incorrectly entered arrest report, credit report, insurance rejection, debt default, or lab test can cause great emotional and financial damage. Yet the error rates of databases with such sensitive information are often higher than the standards of quality set by the original designers of these systems. Accuracy, timeliness, completeness, and relevance are what give information its value. In particular, creators of personal history databases have a special obligation to compile and process such data accurately and to protect it from the prying eyes of snoops, browsers, and hackers.

Today people can collect, process and disseminate information at a high speed. If information is irrelevant to the needs of users or is flawed in logic, assumptions or conclusions, relying on such specious data can cause catastrophic damage. Therefore, quality begins with clear objectives, exacting designs, flawless development and proper training of users. People and organizations involved in software development and database design are obliged to make products that are fit for their intended uses and have no fundamental defects.

Competence

The field of information technology is notable for its fast growth and complexity, and the sweeping social, economic, and political changes it has wrought. At times, change seems overwhelming. Skills and products become obsolete overnight. Companies must invest large sums of money in research and product development.

In the race to get new products out of the labs and into the market, people often compromise quality, safety and security. New products might contain design flaws, software errors, bugs and glitches, and other impediments to proper functioning. These impediments can be costly to uninformed and unsophisticated users. Makers and providers of information technology products—both hardware and software—must take great care and caution in their work to avoid damage or interruption of service to their users. Providers of information technology should seek the most competent people available for sensitive design and product development projects. They should also create an ethical climate in their firms and foster responsible behavior among all employees.

Honesty

Makers, sellers, dealers, distributors, and installers of information technology products—like all other business people—must be honest in their dealings with one another. All parties should use truthful representations, nondeceptive advertising, and accurate labeling, as well as fulfill contract requirements.

Loyalty

The information technology industry is large, complex, fast changing, and highly competitive. Some information products—such as chips and PCs—have become commodities. The relationship between buyers and sellers is changing from one in which mutual trust, confidence, and faith give way to arms-length transactions. Sellers attract buyers on the basis of price alone. The service-after-sale element is forgotten.

These same industry dynamics have also changed the relationship between employers and employees. Loyalty is supposed to be a two-way street. In today's competitive environment, some high-tech, high-talent employees are loyal only to their paychecks thereby blurring obligations between employers and employees, sellers and buyers, and manufacturers and suppliers.

Fairness

Normally people conduct business on the basis of mutual faith and trust. You cannot, however, provide for all contingencies in a formal contract. The writing and execution of a detailed contract would take too long, thus frustrating the objectives of both parties.

Assuming business ethics are a matter of mutual rights and obligations of the transacting parties implies that fairness is the rule by which we measure whether a transaction is right or wrong. In theory, both parties have equal bargaining power in a commercial transaction. Therefore, ethics should leave the parties to their own negotiations. Often in the information industry, both parties are not of equal size, competence, skill, knowledge or experience. In these circumstances, fairness may mean that the more powerful of the two has an added measure of obligation. The English common law treated buyers and sellers as equally competent to transact business. Yet in the modern era the notion of *caveat emptor* (let the buyer beware) has been diluted. Sellers with superior knowledge, skills, and resources must be most forthcoming. Fairness may no longer be a 50-50 proposition. Fairness depends on the relationship between the parties, their relative power positions, and the context of the business transaction.

2.2 ETHICAL ENVIRONMENT CHECKLIST

CPAs can use table 2.1, Ethical Environment Checklist to help promote an ethical environment in their organizations and in those of their clients. *No* answers may require investigation and follow-up, the results of which should be documented. Use the *Ref* column to cross-reference the checklist to appropriate work papers.

Some sections in this comprehensive checklist may not be applicable or appropriate in certain instances. For example, most organizations will not conduct the entire employee screening procedures described in section 4 of the checklist. This checklist is intended for general guidance and information only. Use of this checklist does not guarantee the prevention of fraud. If fraud prevention is an especially vital concern or if fraud is suspected, consider seeking the advice of a knowledgeable fraud practitioner.

TABLE 2.1 ETHICAL ENVIRONMENT CHECKLIST

| Ethical Environment Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|-----|
| 1. Organizational Approach to Ethics | | | | |
| a. Does the organization have a Mission Statement that emphasizes respect for the law, ethics, and ethical conduct? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Does the organization have a written and enforced Code of Ethics? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. If the organization or its employees are subject to outside ethical standards and rules (e.g., industry or professional), does the organization's code refer to and emphasize their importance? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Does the organization have— | | | | |
| • Internal auditors? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Electronic data processing (EDP) auditors? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • At least one Data-Security Officer or Administrator? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • A Corporate-Security or Loss-Prevention Unit? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • An investigative staff? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Does the organization, as a matter of written policy, refer incidents of employee crimes on the job to police or prosecutorial authorities? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. If the organization has experienced fraud in the past five years, has management established the causes and taken remedial action for any of the following: | | | | |
| • A substantial inventory shortage corporate-wide | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • A substantial inventory shortage in a major operating division | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • A major embezzlement involving a loss of more than \$10,000 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • A successful penetration of the main office computers by outsiders | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • An accounts payable, accounts receivable, payroll, or benefit claim fraud of any amount | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • A commercial bribery of purchasing or other personnel | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. Situational Approach to Ethics | | | | |
| a. Are ethical considerations a critical element in corporate policies, tactics, and decision-making? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Is there a specific framework—especially for important and difficult corporate decisions or actions—for addressing the ethical element, such as a series of questions like those set out in item 2c (below)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 2.1 (continued)

| Ethical Environment Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| ● Engaging in false advertising and deceptive marketing practices | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Disclosing company trade secrets to unauthorized persons | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Fixing prices with competitors | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Gambling on the job | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Abusing drugs or alcohol, or both | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Fighting on the job | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Stealing company property, including personal use of company property (for example, computer time) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Destroying company property | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Falsifying time or attendance reports | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Falsifying production reports | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Falsifying personal data on a job application | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Falsifying or forging accounting records | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Destroying accounting records | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Falsifying expense accounts | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Allowing unauthorized persons access to confidential records (for example, payroll and personnel records, customer and vendor lists, research results, product and marketing plans) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Allowing unauthorized persons access to company buildings or critical work areas | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Loaning company building access identification cards, badges or door keys to unauthorized persons | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Disclosing computer log-on codes or passwords to unauthorized persons | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Allowing unauthorized persons use of computer terminals | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 4. Ethics and Human Resources | | | | |
| a. To the extent necessary, when considering an applicant and depending on the importance and sensitivity of the position, does the organization perform reference checks, background inquiries or investigations, or any combination thereof, to confirm the applicant's— | | | | |
| ● Identity | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Educational achievements | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 2.1 (continued)

| Ethical Environment Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| • Credit standing | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Satisfactory past employment history | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Absence of criminal convictions (including name or fingerprint checks, or both) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Reputation | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Character | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Especially for very sensitive positions (for example, those affecting public safety, the custodianship of large amounts of cash or securities, the secrecy of important information), and to the extent allowed by law, does the organization administer any of the following to employees and prospective employees: | | | | |
| • Polygraphs | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Paper and pencil honesty tests | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Voice stress analyses | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Handwriting analyses | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Intelligence tests | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Psychological diagnostic tests | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Drug tests | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Does the organization conduct or provide (or both) any of the following: | | | | |
| • Security orientation training for new hires | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Ongoing security awareness training programs for all employees | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Written rules of employee conduct to all employees | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Annual, signed employee declarations acknowledging awareness of the company's code of conduct, and past and future adherence to it | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Hearings for employees charged with punishable offenses | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Employee representation at such hearings | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Does the organization use or provide any of the following: | | | | |
| • Job descriptions | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Organization charts | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Performance standards | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| • Performance appraisals | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

TABLE 2.1 (continued)

| Ethical Environment Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| <ul style="list-style-type: none"> ● Coaching and counseling of employees whose work is unsatisfactory | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Counseling of employees with drug abuse problems | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Technical training programs | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Human resource development programs | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Tuition reimbursement | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Time off for study | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Time off for family emergencies | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Employee involvement programs | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Job enlargement, enrichment or rotation programs | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Exit interviews for departing employees | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <p>e. Does the organization compare favorably or at least equally with other firms in its industry, or areas of operations, or both, with respect to any of the following:</p> | | | | |
| <ul style="list-style-type: none"> ● Salaries | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Fringe benefits | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Blue-collar turnover | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● White-collar turnover | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Absenteeism | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Employee firings | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Promotions from within the company | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Ability to recruit new employees | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Skills of its employees | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Educational level of employees | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Employee attitudes toward their work | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <ul style="list-style-type: none"> ● Employee loyalty | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <p>5. Ethics and Information Technology</p> | | | | |
| <p>a. Does the organization's code of conduct specifically address the importance of using information technology (especially computers) in an ethical manner?</p> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <p>b. Are the following specific ethical concerns relating to information technology adequately addressed in the organization's code of conduct and in its policies:</p> | | | | |

(continued)

TABLE 2.1 (continued)

| Ethical Environment Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| <ul style="list-style-type: none"> ● Privacy of information (for example, information related to employees, customers or clients) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Prohibition of software piracy | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Safety and health (for example, ergonomically sound computer workstations) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Quality standards for information technologies and the information they process (for example, accuracy, integrity, security) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Relationship of technology and human resources (for example, communication with employees concerning technological change, adequate training) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

CHAPTER 3:

Insurance Against Fraud

| | | |
|-------|---|----|
| 3.1 | Financing the Risk of Fraud..... | 3 |
| 3.2 | Fraud Insurance | 3 |
| 3.2.1 | Overview | 4 |
| 3.3 | Important Provisions in Commercial Crime Policies | 4 |
| 3.3.1 | Insuring Agreements | 5 |
| 3.3.2 | Policy Definitions | 6 |
| 3.3.3 | Policy Exclusions | 7 |
| 3.4 | Insured's Responsibilities in the Event of a Loss..... | 16 |
| 3.4.1 | Duties of the Insured | 16 |
| 3.4.2 | Handling the Discovery of Employee Dishonesty | 16 |
| 3.4.3 | A Course of Action..... | 17 |
| 3.4.4 | Notice of Loss..... | 18 |
| 3.4.5 | Supporting Documents..... | 18 |
| 3.5 | The Insurer | 21 |
| 3.5.1 | The Insurer's Investigation..... | 21 |
| 3.5.2 | Subrogation Rights and Duties..... | 22 |
| 3.5.3 | Response to a Claim Denial | 22 |
| 3.5.4 | Summary..... | 23 |
| 3.6 | Fraud Insurance Checklist | 23 |

CHAPTER 3:

Insurance Against Fraud

3.1 FINANCING THE RISK OF FRAUD

Every organization must identify its risks and implement a strategy that balances the cost of potential losses with the cost of an acceptable level of risk management. Although the risk of loss from fraud and other forms of dishonesty can be reduced, no amount of spending on prevention can eliminate it completely.

As with any area of risk, an organization can select an acceptable level of potential loss and finance it from its own resources by, in effect, self-insuring or through the purchase of appropriate insurance coverage. It would be imprudent not to consider purchasing insurance from a reputable insurance company, particularly in situations in which there is a significant risk of potential and possibly catastrophic loss. In reality, however, some organizations do not even consider, let alone acquire, the appropriate insurance because they do not know how to assess the risk and its financial impact correctly or they are simply unfamiliar with the nature of available insurance coverage.

Most individuals and businesses should never consider self-insurance, that is, waiting until a loss occurs and then absorbing the costs out of their own resources. This is particularly true where there is a risk of a catastrophic loss that may threaten the very survival of a business. In other areas of risk, it would be unthinkable to not obtain insurance against potential catastrophes such as life and disability insurance for breadwinners supporting families, fire insurance for homeowners, and liability insurance for professionals and automobile owners.

This chapter reviews the kinds of insurance coverage generally available against employee fraud and dishonesty. It also reviews some of the issues found in insurance policies, common exemptions, and some of the important duties of the insured. In addition, the chapter will provide a step-by-step guide to making a claim after the discovery of the dishonest act.

It must be stressed that an insurance policy is a contract. Insurance and legal advisers should be consulted to consider whether insurance is appropriate, the nature and extent of coverage required, and how any losses sustained should be handled.

3.2 FRAUD INSURANCE

Chapter 1, “Managing the Risk of Fraud,” of this *Handbook* provides a definition of fraud as *criminal deception intended to financially benefit the deceiver*. In that same chapter is a description of how a company may be victimized from outside by customers, suppliers, competitors or “con men,” and from inside by directors, officers, and employees (see Figure 1-2, How a Company Can be Victimized).

Basic coverage insures a business against losses suffered directly as a result of fraud or dishonesty committed by employees of the insured (as defined in the policy). It typically forms part of a crime or dishonesty policy that also covers losses due to theft, disappearance, or destruction of the insured's property.

Such coverage does not, however, protect against losses suffered as a result of the fraudulent and dishonest conduct by outside (nonemployed) directors or external parties when not in collusion with employees. Dishonest acts by outside directors may be covered under a separate director and officer policy although fraud against the insured or against a third party is not generally covered.

3.2.1 Overview

Insurance policies providing coverage against losses from employee fraud and dishonesty have many names including commercial crime, blanket bonds, and 3D policies (dishonesty, destruction, and disappearance). The desired coverage may be reflected in standard bond or policy language, as an extension of coverage or rider to existing insurance policies or in a manuscript format, that is, written for a specific company or set of circumstances.

Coverage and wordings may be specific to certain industries. For example, there are specific forms for financial institutions such as banks, brokerage houses, and insurance companies. For other industries, including manufacturing, health care, retailing, transportation, or service providers, dishonesty coverage is more generic. Regardless of the name used by a particular insurer, policies generally follow a similar format. This *Handbook* uses the term *commercial crime policy* when referring to coverage for employee fraud and dishonesty, unless otherwise noted.

When a company applies for a policy, the insurer will ask for information to be used in evaluating the risk and determining the premium. Although the type of details requested may vary from insurer to insurer, the information will always show how the applicant operates its business and the controls and procedures in place to prevent loss. If this information is false or erroneous or the insurer is not advised of changes such as discontinued or weakened controls, the ability to make a successful claim may be jeopardized. Therefore, the insurer must be informed of any changes that may affect assessment of the risk to be covered.

3.3 IMPORTANT PROVISIONS IN COMMERCIAL CRIME POLICIES

The principal components of a commercial crime policy are the Insuring Agreements. Their purpose is to describe and define the kinds of losses covered under the policy and make clear what needs to be demonstrated as proof of a valid claim, in addition to listing the various conditions and limitations. The first Insuring Agreement is typically for *Employee Dishonesty* or *Employee Theft*. The following types of losses, which do not reflect losses identifiable with or attributable to the conduct of employees of the insured, are also covered by Insuring Agreements:

1. Loss inside the premises
2. Loss outside the premises
3. Depositor forgery
4. Money order fraud and counterfeit paper

The conditions and limitations further defining the coverage include the following:

- Definitions
- Exclusions
- Duties of the insured

3.3.1 Insuring Agreements

Employee Dishonesty or Employee Theft

Although the wording of this agreement may vary among insurers, there are certain important common elements that should be noted:

- The indemnity is for loss of money, securities, and other property
- The loss must result *directly* from one or more acts of an employee of the insured
- The employee can be acting alone or in collusion
- Coverage continues even when individual employees cannot be identified.

The meaning of various terms used, such as *property* or *employee*, may be given specificity in the “Definitions” section of the policy. It is essential, therefore, to refer to and understand the definitions outlined in the terms of coverage to ensure that the policy meets the particular needs of the organization. Some of the more significant terms, as they are typically defined in a policy, are discussed later in this chapter.

Where the Insuring Agreement is for *Employee Dishonesty* (sometimes described as *Employee Fidelity*), coverage for loss resulting directly from employee fraud or dishonesty is further qualified by wording that refines the scope of possible losses covered. Some typical wording is shown in Figure 3-1, Dishonest or Fraudulent Acts.

Note the reference to the manifest intent to cause the loss and obtain a financial benefit. Unfortunately, the courts have shown no consensus in the interpretation of *manifest intent*. Some have found this term applicable only where the employee intends to gain a benefit at the expense of the insured; others have found a broader meaning and afford coverage if the employee acted with such disregard for the insured that the loss was a virtual certainty. In one case, a court ruled: “Such a person is deemed to intend the natural and probable consequences of his acts.”

It is important to note, in the wording of Figure 3-1, the restriction on the type of financial benefit that disallows claims in situations in which the employee receives the benefit because of his or her position in the company. Therefore, in a situation in which the benefit intended and obtained by the dishonest employee is, for example, a bonus, there would be no grounds for a claim under the policy.

Figure 3-1. Dishonest or Fraudulent Acts

DISHONEST OR FRAUDULENT ACTS

Dishonest or fraudulent acts are committed by an employee with the manifest intent to:

- (1) Cause the loss
- (2) Obtain financial benefit for the employee or any other person or organization intended by the employee (other than salaries, commissions, fees bonuses, promotions, awards, profit sharing, pensions or other employee benefits earned in the normal course of employment).

In a commercial crime policy in which the insuring agreement is for *Employee Theft*, coverage is for loss resulting directly from theft. The term *theft* may be defined as, for example, the unlawful taking of money, securities, or other property to the deprivation of the insured. There is no reference either to the intent of the person committing the theft or to their financial benefit. Although the word *fraud* is not used, the circumstances and resulting loss would be tantamount to fraud as defined in the policy.

Other Insuring Agreements

A typical commercial crime policy includes an insuring agreement against loss of money and securities by the theft, disappearance, or destruction within the insured's premises or any banking premises (usually referred to as *Loss Inside the Premises*) or outside the insured's premises while being conveyed by messenger or armored car company (usually referred to as *Loss Outside the Premises*).

A policy may also contain insuring agreements providing coverage against:

- *Money Order and Counterfeit Paper Currency.* Money order fraud and counterfeit paper are typically defined as loss due to the acceptance, in the normal course of business, of counterfeit currency, money orders, and so on.
- *Depositor Forgery.* Losses as a result of the insured having someone process forged checks, money orders, and so on, through its bank account.

A rider can provide additional coverage for risks not covered by a standard policy. Riders may provide coverage for losses from unauthorized electronic transfers, pension plan frauds, credit card forgeries, computer fraud, and the unauthorized use of telephone services. An insurance professional can ensure the rider provides the required supplementary protection.

3.3.2 Policy Definitions

Definition of words and descriptions adds specificity. In some policies, however, what is included by definition may be excluded in the "Exclusions" section. Therefore, "Definitions" should be read carefully and in conjunction with the "Exclusions" section.

Employee

One of the most important definitions is that of *employee*. The definition of employee limits the coverage. Make sure the definition gives the kind of coverage required in the case of loss.

In a typical policy, an employee is defined as any person who, while in the regular service of the insured and in the ordinary course of business, is compensated by way of salary, wages, or commission. A policy may also be written to include temporary staff under the definition of employee.

Some persons defined as employees may be excluded from coverage. For example, a paid outside director of the insured not retained in any other capacity may be expressly excluded from the definition under the policy. Further, the definition may also exclude such third parties as agents, brokers, consignees, or independent contractors.

3.3.3 Policy Exclusions

An insurer will write policies with its own list of exclusions. Commonly found exclusions are losses from:

- Acts committed by the insured (the owner) or a partner
- War and insurrection

Read carefully and understand the terms before purchasing the coverage and obtain competent advice when preparing a proof of loss. The following sections describe other examples of commonly found exclusions.

Indirect Losses

Commercial crime policies specifically exclude indirect and consequential losses such as lost income, lost business opportunities, or lost interest on stolen funds. Although the insurer's intent is to limit its obligations to direct losses only, court rulings have not consistently recognized this position. Discuss the relevant case law with legal counsel for any jurisdiction in question.

An indirect loss would also include investigative costs incurred in establishing the existence and amount of a direct loss. Separate coverage may be available from an insurance carrier to cover these costs; some write policies covering all or part of the costs of investigation, while others cover costs shared between the insurer and the insured. You should weigh the cost of this coverage in light of the potential cost of any investigation. A typical wording of an indirect loss exclusion is excerpted in Figure 3-2, Indirect Loss Policy Provision.

Figure 3-2. Indirect Loss Policy Provision

INDIRECT LOSS EXCLUSION

Indirect Loss: Loss that is an indirect result of any act or "occurrence" covered by this insurance including but not limited to, loss resulting from:

- (1) Your inability to realize income that you would have realized had there been no loss of, or loss from damage to, Covered Property
...
- (2) Payment of costs, fees or other expenses you incur in establishing either the existence or the amount of loss under this insurance.

Atlas Construction Case Study

Atlas Construction, Inc. had a long history in construction and commercial development and was widely regarded as one of the most reputable companies in the region because it completed all projects on time and within budget. Much of this reputation was attributable to the hands-on management style of project managers and the sophisticated accounting and management reporting system that could provide up-to-the-minute actual costs with a comparison to budget.

As part of risk-management, the operation was assessed annually for vulnerability to fraud and the effect of potential losses. In consultation with its insurance advisers, a standard commercial crime policy was in place, which provided annual coverage of \$500,000 with a \$5,000 deductible. There had been no claims made against the policy since its inception.

One day, an anonymous letter was received alleging that one of the project managers was colluding with a supplier to inflate invoices in order to receive kickbacks. A discrete investigation was undertaken to get to the heart of the problem without alerting or confronting the project manager.

Internal auditors together with external investigators and forensic accountants conducted a thorough review of bids for the supply of goods and services and the payment of supplier invoices. It soon became apparent that not only were certain suppliers' invoices, which were consistently 7 percent higher than agreed, approved for payment by the project manager, but also numerous suppliers were found to be connected to the project manager and his close family members. Strong evidence showed that some "suppliers" were merely shell companies supplying no goods or services; their only purpose was to receive the payments from Atlas. The project manager was confronted with the evidence and confessed to the scheme although he claimed to have spent all the proceeds of the fraud.

Atlas determined it had lost almost \$350,000 to the fraudulent suppliers. The police were notified and civil proceedings were initiated to recover. A claim against the insurance policy was made for \$422,000 representing the loss from fraudulent

suppliers plus \$72,000 in investigation costs (internal audit and external professionals) and legal costs. Atlas considered the \$72,000 to be directly attributable to the fraudulent and dishonest acts of its employee and would not have been incurred but for his conduct. This part of the claim was denied on the basis of the policy's explicit exclusion of such costs as indirect.

Inventory Losses

One of the most common types of business loss is inventory loss. A company comes to the end of a reporting cycle and compares the value of inventory reflected in the perpetual inventory records to the value of the physical inventory on hand, and notes a significant discrepancy for several product groups. The value of physical inventory on hand is far less than the accounting records indicate. Is the discrepancy the result of recording errors in the perpetual system, a flawed physical count, errors in the values applied to the physical inventory or, possibly, theft?

A claim citing the discrepancy as proof of employee theft and the loss suffered would be denied under a commercial crime policy. The coverage would be denied on the basis of the policy's "inventory loss exclusion" clause stating that an inventory loss, the existence of which is based solely on an inventory or profit-and-loss calculation, is excluded from coverage.

The inventory loss exclusion disallows claims for losses resulting from errors in the accounting records or improper physical inventory counts and pricing. A claim can only be successful if the evidence demonstrates there is no error or inaccuracy in the records and, in the absence of overt evidence of theft by employees or others, there is no plausible explanation for the discrepancy other than theft. It also excludes claims made where the discrepancy reflects inventory shrinkage occurring in the ordinary course of business. Such shrinkage may be the result of physical decline or reduction caused by evaporation, the disposal of damaged goods, promotional giveaways, and the distribution of samples to prospective customers.

There may indeed be suggestive evidence of inventory theft by employees. For example, employees may have been seen loading inventory into their cars after work on a Friday. The perpetual records may even show the items to be in stock despite the fact they cannot be physically located. The volume and frequency of the thefts must now be investigated. One Friday-night theft does not create a significant discrepancy.

The first step to determining whether an actual inventory loss has occurred is to understand the company's accounting system as well as the internal control processes of the inventory cycle, the perpetual accounting system, and the physical inventory system.

The inventory cycle includes:

- Manufacturing or purchasing process
- Warehouse receiving process
- Sales order process
- Warehouse shipping process
- Perpetual inventory accounting system:
 - Purchase journal
 - Sales journal
- Reconciliation process with physical count
- Physical inventory system
- Count process
- Pricing process
- Adjustments (obsolescence, shrinkage, and sales cutoff)

Understanding the control processes permits investigation of their operation during the period of the alleged theft. This knowledge should identify exploitable weaknesses and help focus the detailed investigation. It may also identify changes introduced by a particular employee or group.

If the accounting records are to provide the proof needed to substantiate a theft claim, the investigation should start with the most recent accounting period in which the perpetual system and the physical count were in agreement. Care must be taken, however, to identify and explain any accounting adjustments or unusual entries made to reconcile the perpetual system to the physical count. A comparison of the inventory accounting activity between the base period and the period of the alleged theft should identify some red flags. Pay particular attention to any large or unusual adjustments to the inventory records. Investigate and understand these adjustments because fraudsters often hide their thefts temporarily with accounting adjustments.

Another step is to interview the personnel working at the different stages of the inventory cycle including those involved in accounting for purchases and sales, receipts and deliveries, and those physically handling the inventory in the warehouse or transport and delivery. A productive interview requires a thorough understanding of what *should* have occurred. The interviews may identify control overrides and/or control weaknesses exploited by the fraudster. Also inquire about new employees or employees who have recently left the company and interview them, if necessary. The discrepancy could be revealed by a new employee's activities or by a departed employee no longer able to conceal the theft.

If an employee theft is uncovered, the insured will be required to file a Proof of Loss that identifies:

- The thief (if known)
- The circumstances of the theft
- Period in which the theft took place
- The amount of stolen inventory
- The value of stolen inventory

As always, get advice from attorneys and insurance advisors when acquiring coverage or making a claim.

Inventory Loss Case Study

Jetro, Inc. has been a wholesaler of men's clothing in Pennsylvania for the last ten years. The company maintains an integrated perpetual inventory system tied to purchasing and deliveries and sales. Historically, Jetro has taken annual physical inventory counts on December 31, the last day of the fiscal year. In 2002, however, Jetro's internal accounting group requested a surprise count to be scheduled for March 31 and employees were notified just two days in advance.

The physical inventory count showed only \$6.4 million, while the perpetual inventory system identified \$6.5 million. After the internal auditors had doublechecked the numbers, they conducted an investigation to find the missing \$100,000.

Using their knowledge of the entire inventory cycle, the internal auditors reviewed the activity recorded in the December 31, 2001, perpetual-to-physical inventory working papers. They also interviewed various warehouse and accounting personnel as to possible reasons for the shortage.

Their investigation uncovered the following red flags:

- Three purchase orders for \$45,782, \$48,925, and \$49,818 were identified in December 2001 to three different companies that had not done business with Jetro for about two years. Internal audit found these amounts interesting since they were all just under the \$50,000 limit requiring management approval. Further review of the invoices showed all three companies had processed billing address changes to P.O. boxes in South Carolina.
- As of March 31, 2002, all three companies still had the over-90-day receivable balance outstanding.
- During an interview, a part-time weekend warehouse employee said that, on Saturdays, he always noticed about 15-to-20 garment boxes stacked in pick-up bay 1. He found this strange since only bays 4 through 8 were used for Saturday shipments. When he questioned his supervisor, he was told not to concern himself with that order. He continued to notice this pattern on subsequent Saturdays but never inquired about it again. When questioned further by internal audit, the employee recalled this had been going on since about October or November 2001.

- Upon further review of the March 31, 2002, physical count sheets, internal audit noted several handwritten adjustments to the count sheets. These adjustments increased the quantities on several brands of men's suits.

Internal control became increasingly suspicious of Walter Wilson, the Saturday warehouse supervisor, because of what they knew from the interview with the warehouse clerk and from the fact that it was Mr. Wilson who had adjusted the count sheets. Internal audit decided to do some background checking before they confronted Mr. Wilson.

An outside investigation agency uncovered the following:

- The owner of the P.O. boxes in South Carolina belonged to Jennifer Hickey. Ms. Hickey was also identified as Jennifer Wilson Hickey, Walter Wilson's married sister.
- It was discovered that Walter Wilson was the coowner of a small discount retail-clothing outlet in New Jersey.
- Upon inspection of the New Jersey clothing store, the investigative agency identified numerous matches of suits sold by Jetro.

Based on the results of the investigation, Jetro confronted Mr. Wilson. After his initial denial, Jetro began to unveil the evidence. In the end, Mr. Wilson admitted to stealing an unknown quantity of men's suits for sale in his store. He admitted to starting the theft in November 2001. He covered his 2001 theft with the three fictitious purchase orders and shipments. He estimated he stole another \$250,000 of men's suits in 2002. He was planning to leave Jetro before collection efforts commenced on the three fictitious December 2001 sales. In the meantime, the surprise inventory required him to adjust the March 31, 2002, physical counts to buy more time (and apparently steal more suits).

Now that Jetro had Mr. Wilson's confession, they needed to quantify the amount of loss for their insurance claim. A \$489,525 "Proof of Loss" was eventually filed. The breakdown and support follow:

- \$144,525 in 2001 representing the three fictitious invoices. Mr. Wilson utilized three former Jetro customer names because these customers were already approved to do business with Jetro. The billing address was changed to his sister's P.O. boxes to assure that the three companies would not receive the billings. With the fictitious shipments to the three customers, no significant discrepancies would be noted in the December 31, 2001, perpetual-to-physical reconciliation.
- \$345,000 in 2002 represents the theft in the first quarter. After reversing the March 31, 2002, handwritten count-sheet adjustments made by Mr. Wilson, the physical inventory totaled approximately \$6.1 million, not \$6.4 million. This now resulted in a \$400,000 discrepancy. Based on a reconciliation of purchase and sale information in 2002, the investigation identified a purchase value of \$345,000 in suits with no matching sales and no physical inventory of the suits. The reconciliation involved taking the perpetual inventory from December 31, 2001, adding in all purchases of a particular brand of men's suits (the merchandise Mr. Wilson was stealing) and subtracting all sales of the suits. This amount was then reconciled to the March 31, 2002, physical count to quantify the amount stolen.

The remaining \$55,000 (\$400,000 less \$345,000) does not relate to suit theft and thus was not included in the claim. Internal control has attributed the \$55,000 to shrinkage for the first quarter of 2002.

In conclusion, a surprise physical inventory count, an observant part-time warehouse clerk and some diligent investigation on behalf of internal audit resulted in Jetro stopping a potentially larger theft and a being able to present a well-supported "Proof of Loss."

Is this documentation enough to assure a full recovery? No claim payment can be guaranteed; however, every link between the employee and the claimed loss strengthens the insured's claim.

Figure 3-3. Standard Inventory Loss Exclusion

STANDARD INVENTORY LOSS EXCLUSION

Loss, or that part of any loss, the proof of which as to its existence or amount is dependent upon:

- (1) an inventory computation; or
- (2) a profit or loss computation.

Source: Employee Dishonesty Coverage Form (CR 00 01)

Loan Loss

Among the various commercial crime policies available from insurers, financial institution bonds are specifically for financial institutions such as commercial banks, savings associations, savings banks, credit unions, insurance companies, and securities brokers.

Lending institutions suffer losses if the borrower fails to repay the loan and the market value of the collateral is too impaired to permit full recovery of the amount owed. Upon investigation, the borrower is sometimes discovered to have falsified the loan application by submitting false financial statements or appraisals. If a bank victimized by such a borrower were to file a claim under a financial institution bond, the claim would be denied under the "loan loss exclusion" clause that states that loans obtained through "trick, artifice, [or] fraud" on the part of the borrower are excluded. The loan loss exclusion specifically disallows claims for losses as a result of dealings with a deceitful borrower if no bank employee is involved in collusion with the borrower or other third-party beneficiary.

If the credit officer had an undeclared interest in the borrower and accepted a loan application he knew to be fraudulent, the financial institution bond might provide coverage for a loss. The loss must be shown to have been a direct result of his dishonesty and his manifest intent both to cause a loss to the financial institution and to obtain a financial benefit for himself or a third party. (See Section 3.3.1, Insuring Agreements, and Figure 3-1.)

As with commercial crime policies, legal counsel should always guide a forensic accounting assignment involving a financial institution bond. This is true not only for the purpose of maintaining privilege but because certain provisions of the bonds are subject to varying and often conflicting interpretations in different jurisdictions. Moreover, certain elements of the coverage itself are controversial due to these same conflicting court interpretations or the lack of applicable court rulings.

Guidance and advice should be sought from legal and insurance advisors when acquiring coverage under a financial institution bond and making a claim.

The Kindly Old Loan Officer Case Study

A large multibank holding company acquired a small bank. Approximately one year after the acquisition, the bank experienced significant losses from a portfolio of small business installment loans that were all collateralized by 18-wheeler tractor-trailers.

Initially, the bank did not have any proof of employee dishonesty but the size of the loss encouraged a closer look. Since loans can be manipulated in two ways, that is, to make dishonest loans or disguise the loan's performance by making a delinquent loan look current, the bank decided to look first at those individuals who made decisions affecting the loan portfolio. A review showed the portfolio had been created and administered by one particular loan officer in the bank, who immediately became suspect. The bank's investigation revealed that the loan officer had manipulated the monthly reports to show delinquent loans as current. The bank filed a claim with the insurance company alleging employee dishonesty.

The forensic investigation that followed included a review of bank documents as well as the personal financial records of the bank loan officer. Each loan was reviewed to determine whether it had complied with the bank's loan policy and had been approved by the loan committee. Loan department reports were also reviewed for proper disclosure and loan histories examined for any payments made.

The documents reviewed included the loan applications, internal analysis and approval memos and documents, financial information provided by the borrowers, collateral information, and verifications. The loan closing documents, specifically the settlement or disbursement sheets, were also reviewed to discover whether the loan proceeds might have been used to pay kickbacks. Loan histories and loan delinquency reports were analyzed in detail. The delinquency and cash payment reports were compared to determine whether the loan payment status had been manipulated to show the loans as current when, in fact, they were past due.

This comparison showed the loan officer had intentionally falsified loan delinquency reports to make the loans look current. When confronted with the evidence, he admitted he had falsified the loan records to show payments when none had been made. He said he felt sorry for the borrowers who were suffering from the economic difficulties of the area and wanted to give them every chance to repay the loans. If the loans had been reported as delinquent, the bank would most likely have repossessed the vehicles. The loan officer either had a heart of gold or, as the bank suspected, was receiving kickbacks from the borrowers.

The loan officer's personal bank accounts were examined for evidence of financial benefit. The bank interviewed some of the borrowers and, in some instances, obtained updated financial information. The forensic investigation showed the loan officer did not obtain any financial benefit from making the loans and the borrowers obtained only the obvious benefit of the use of the loan proceeds.

A detailed review of the loan origination documents showed the loan officer initiated the loans, which were approved with no evidence that false information had been submitted to the loan approval committee. Moreover, the loan proceeds were indeed used to purchase the 18-wheelers. It was also noted that in most cases, the borrowers made consistent monthly payments for at least a year and all acknowledged their debt and made efforts to repay past due amounts.

The bank filed a claim under its financial institution bond with the insurer for reimbursement of the unpaid interest costs. The insurer denied the claim, and the bank turned to the courts for recovery. The court ruled in favor of the insurer on the grounds that the bank had failed to prove manifest intent to defraud on the part of the loan officer.

The Bank President Makes His Move Case Study

A bank made a large loan to a condominium developer for a new project that was bigger than anything the developer had built before. After a few months, the developer was unable to make interest payments and the loan appeared on the bank's delinquency list. A preliminary review of the borrower's history showed he had had financial troubles with other banks and should never have been granted the loan. A subsequent forensic investigation focused on the bank president who was also the senior loan officer. Deeper probing showed the bank president/loan officer had received a financial benefit in the form of ownership of a condominium unit in the project. The bank president held title through a shell company set up as a limited partnership whose general partner was a corporation he also owned. The manifest intent of the president was determined by the way the project financing was structured on false and/or incomplete information that was presented to the bank's loan committee, which ultimately approved the loan.

The documents examined to discover the fraud included:

1. The loan request/application
2. The financial information provided by the borrower
3. The bank's analysis of the financial information, including:
 - Project budget and costs
 - Projected sales proceeds
 - Use of proceeds and loan repayment
4. The bank's internal approval documentation, including:
 - Loan officer's recommendation
 - Loan committee minutes
 - Board of directors' approval minutes

5. Loan closing documents including disbursements
6. Settlement sheets and closing information for the sales of the condominium units.

A background investigation of the project developer/borrower showed that he had been a small player on other projects and lacked the resources to finance the kind of project presently in question. A review of the documents prepared and presented to the loan committee by the president raised serious questions about the borrower's cash-flow projections and his capacity to service the loan. A search of the public records to discover the owners of units whose sale had already closed showed a company owned by the bank president holding title to a luxury unit whose price was far beyond anything he could have afforded on his known financial resources.

The bank filed a claim under its financial institutions bond and was ultimately reimbursed by the insurer.

3.4 INSURED'S RESPONSIBILITIES IN THE EVENT OF A LOSS

3.4.1 Duties of the Insured

Issuers of dishonesty policies typically impose several duties on the insured to protect their ability to recover. The insured must take action to prevent further loss, mitigate the damage, and recover from any loss sustained. These duties include:

1. Timely notice of potential loss
2. Filing of a "Proof-of-Loss" form
3. Cooperation with any insurance investigation

See Figure 3-4, Insured's Duties to Insurer in the Event of Loss, for an example of the specific language spelling out the insured's duties in a commercial crime policy.

Most dishonesty policies typically contain two additional obligations for the insured: agreeing not to prejudice the rights of the insurance carrier and accepting the procedures for filing a lawsuit in the event of a claim denial. See the following section for more information on these duties.

3.4.2 Handling the Discovery of Employee Dishonesty

Dealing with an allegation of wrongdoing against an employee provokes feelings of shock and betrayal within the firm and often causes a decline in internal morale and external goodwill. A large loss may also hurt the bottom line if it is not covered by fidelity insurance.

Dishonest acts must be addressed immediately whether by the police or pursued within the organization. In either case, your actions will influence whether or not you can recover under your fidelity insurance. Therefore, it is important to know how to respond when allegations of wrongdoing arise. Most victims (and even most claims adjusters), however, rarely deal with these types of situations and, as a result, they are often an education for all concerned.

Figure 3-4. Insured's Duties to Insurer in the Event of Loss

INSURED'S DUTIES TO INSURER IN THE EVENT OF LOSS

After you discover a loss or a situation that may result in a loss of, or loss from damage to, covered property you must:

- (1) Notify us as soon as possible.
- (2) Submit to examination under oath at our request and give us a signed statement of your answers.
- (3) Give us a detailed, sworn proof of loss within 120 days.
- (4) Cooperate with us in the investigation and settlement of any claim.

Source: Crime General Provisions (CR 10 00)

Victims of dishonesty should never forget that it is their property that has been lost. No one can relax when this kind of incident occurs. You must conduct yourself as if there were no insurance policy, make every effort to minimize or prevent additional loss and initiate proceedings for maximum recovery.

It is important to note the *right of first recovery* provisions in fidelity coverage. Typically, if a loss does not exceed the policy limit and recoveries are made, the right of first recovery is to the underwriter and then to the insured to satisfy any policy deductible. If, however, the loss exceeds the policy coverage amount, the right of first recovery is to the insured for the amount of the loss in excess of the bond coverage only and the aforementioned rule applies.

3.4.3 A Course of Action

The first decision to make on the discovery of any form of dishonesty is whether or not to conduct an investigation. Some victims choose not to proceed even when they have fidelity coverage. They consider the potential cost of an investigation, including time lost, external investigators' expenses, legal fees, and the possibility of unknown additional costs, to be prohibitive.

There are, however, many reasons to proceed with an investigation. The loss may be covered under the fidelity insurance policy and therefore would be recoverable. In addition, there may be more to the dishonest scheme than was initially realized. Failing to investigate and take appropriate action when the crime is first discovered may prejudice the insured's rights and result in coverage denial when the true extent of the loss surfaces. The involvement of more people than originally believed could make any initial corrective actions ineffective.

A victim who fails to report a loss or reports it late risks the possibility of coverage denial. The typical policy includes the standard requirement that a loss be reported as soon as possible (see Section 3.4.4, "Notice of Loss"). In addition, the insurer also immediately cancels coverage for any employee discovered to have committed any dishonest act. Therefore, it is extremely risky to continue the employment of an individual who has

defrauded or stolen from the company. If management determines that the best course is to continue the employment of the dishonest employee, they should consult with the insurer and request a waiver of the provision canceling coverage for that employee.

Assuming the organization decides to proceed with an investigation, management should assign a representative of the firm the responsibility of coordinating efforts to investigate, document, and prepare a proof of loss. In view of the timing obligations under the policy, this individual should be available immediately to prepare the claim. This *claim coordinator* should have a financial background and the authority to cross departmental boundaries if necessary. The claim coordinator must also understand all the policy details before beginning an in-depth investigation. This individual, together with legal counsel, should bear responsibility for all communications with the dishonest employee, the insurer, and its representatives including the agent.

3.4.4 Notice of Loss

Immediate action after discovery is critical because discovery triggers the policy's notice and proof-of-loss timing requirements. The insured should notify the insurer by telephone and a follow-up letter. Although the coverage states "as soon as possible," sooner is always better than later, as the date of notification is determined by the circumstances of the case and can become a question for a jury. One jury found seventeen days to be an unreasonable delay in notifying the insurer but for another a fifteen-month delay was not deemed too long.

Some victims opt to allow the dishonest individual to continue his or her wrongdoing in an attempt to gather evidence. This is not advisable because, as previously discussed, an insurer will cancel coverage for any dishonest employee immediately upon discovery, and, therefore, the policy will not cover subsequent losses.

When providing notice, it is not necessary to have developed all the facts or even the extent of the loss. After a more comprehensive investigation, the insured can then provide the details of the claim in the form of a written and sworn proof of loss. The typical policy requires the insured file the proof of loss within 120 days from the discovery of the dishonest act—not from the time the insured gave notice. If it seems impossible to meet this deadline, ask for an extension—in advance—from the insurer and request a response in writing. Most insurers will accommodate this request, thereby providing an extension under a reservation of rights.

3.4.5 Supporting Documents

Although insurers value statements made by the dishonest employee, they also require documentation supporting the claim of dishonesty and the resulting loss amount. Make it a priority to obtain and secure the relevant documents. Verify what may seem obvious or conclusive in appearance using the most complete documentation possible. Use discussions with other employees to determine the existence and importance of the documentation. Since dishonest employees often purposely understate or overstate the extent of their transgressions, the gathering of supporting documents is critical to correctly quantifying the loss.

Early in the investigation, identify those employees or outside parties who may be able to assist in the loss analysis. Although there are myriad factors that affect the timing and appropriateness of interviewing these employees, remember that over time memories not only fade but also become selective. Conduct these interviews individually and take detailed notes. If possible, the claim coordinator should attend all interviews.

An Academic Love Story Case Study

The president of a small liberal arts college became concerned about possible wrongdoing as rumors reached him that a certain professor Smith was having extramarital affairs with some of his young students. The college had been founded by a Protestant denomination in the nineteenth century, and was known for its competitive admissions. In the president's view, such conduct by a faculty member put the college's very reputation at stake.

The president, a wise old bird, knowledgeable in the ways of the world, knew professor Smith's salary and general financial circumstances were such that he could not finance his amours out of his tight family budget without alerting his wife. If the rumors were true, professor Smith would have to find the money elsewhere. He also knew that as a department head, professor Smith had a great deal of discretion in approving departmental expenditures, including those he made for himself.

The president began his investigation by assigning the college's internal audit department (IAD) to look at professor Smith's departmental purchases and travel expenses for the previous three years. Supporting documentation for all departmental purchases was analyzed, including purchase orders, invoices, shipping documents, and printouts of the relevant general ledger accounts. A "routine" inventory count of departmental equipment was also performed. The IAD noted that the transfer of equipment was properly documented on a few occasions. Nevertheless, of the 59 items purchased within the past three years, 33 could not be located in the departmental offices or elsewhere at the college.

A special review was made of all departmental travel and entertainment expenses, including individual time and expense reports (TERs) and original restaurant, hotel, airline, and taxi receipts. Usually, professor Smith maintained detailed, descriptive records when he traveled or entertained on college business. He wrote the names of his dinner companions on the actual restaurant receipts and included these names plus additional details such as titles, companies, and events on the TERs. The information could always be corroborated by other documents such as promotional material for an out-of-town conference or the visit of a distinguished scholar who had been entertained by professor Smith during his or her stay.

A review and analysis of recent TERs, however, revealed certain departures from these practices. Beginning in November 2000, professor Smith began using descriptions such as titles, organizations, etc., for his eating companions on the TERs but not the actual names. Of the approximate 67 dining companions on the TERs from November 2000 through June 2002, a total of 32 were not specifically named. Conversely, of the approximate 69 dining companions from January 1999 through October 2000, all 69 were named.

Examples of descriptions used on the TERs during the period from November 2000 through June 2002 included the following:

1. Dinner at the ABC Restaurant with three representatives from the DEF Medical School
2. Dinner with Dean of Undergraduate Studies and Associate Dean [at GHI University]
3. Dinner and beverages at M&S Chicago [with] Sr. Program officer-JKL Foundation
4. Lunch with MNO faculty and staff-PQR Restaurant.

In addition, professor Smith no longer wrote names or descriptions of dining companions on restaurant receipts for six of the TERs that were submitted for February through June 2002, as had been his normal practice prior to that time.

Without original supporting documentation, patterns (or deviations from patterns) such as these may not have been noted. Departures from previously used procedures can be an indicator of potentially fraudulent activities. The choice of periods for selecting the documents to be reviewed must also include a "clean period," that is, a period before the dishonest individual was employed or before the fraudulent acts began. In this matter, it was suspected that the fraud began sometime in 2001. If the period selected for review had been limited to just 2001 and 2002, the deviations from the "normal" patterns or procedures evident in 1999 and 2000 might not have been discovered.

As the fraudulent activity escalates, patterns can also often be found in either the increasing frequency of the occurrences or the increase in dollar amounts. This often occurs as a result of the dishonest individual becoming bolder as more and more of the dishonest acts go undetected.

Since professor Smith could not name legitimate dining companions to include on his submitted receipts as he had done during the "clean period," he used instead vague or general descriptions that made it appear that his travel expenses were for legitimate college business. This deviation was noted both on the original receipts and on the TERs. The analysis provided other deviations from the "clean period" including more out-of-town stays that extended into the weekends and later meal times.

Based upon these findings, a number of individuals from organizations outside the college were contacted in order to corroborate the information recorded on the TERs as part of a "routine" IAD examination. A total of 26 documented dining companions were contacted in an attempt to verify the information recorded on the submitted TERs. Fifteen of the 26 interviewees stated that they did not dine with professor Smith on the date or at the location noted on the TERs.

Conclusion and Analysis

Professor Smith was confronted with this information and confessed to bringing “a friend” and submitting false expenses on a number of his purported business trips. Professor Smith also admitted, to submitting false and fraudulent TERs to the college including false statements of business meetings and fictitious dining companions as methods for justifying meal, travel, and hotel costs as reimbursable expenses incurred in connection with college business. He also admitted to giving equipment that had been purchased for his department to these same “friends” as gifts. So much detailed information and supporting documentation was gathered for each missing piece of equipment and questionable “business” trip that professor Smith was compelled to admit the full extent of his wrongdoing.

This detailed information gathering also simplified the quantification of the loss to the college. After all of the original receipts and invoices had already been collected, it became a simple matter to add up the fraudulent expenses and costs of the stolen items. Finally, the corroborative evidence also facilitated the insurer’s claim verification process.

After the full story had been pieced together, it turned out that professor Smith was indeed wayward and had been supporting one-half of his double life on the departmental budget. As the college president had suspected, professor Smith could not afford these activities on his academic income alone and did not want to reveal his philandering to his wife. He had his cake and ate it too by developing this crude scheme to finance his amours and escape the oversight of both his wife and the college auditors. He was reprimanded but not dismissed and the college was successful in its claim against the insurance company. His wife was never any the wiser.

3.5 THE INSURER

3.5.1 The Insurer’s Investigation

After receiving the proof of loss, the insurer may send an independent investigator to analyze the claim. Start preparing for this investigation by designating one contact person—usually the claim coordinator—to act as liaison for all requests from and discussions with the insurer’s representative. Provide a secure working area close to the contact person and segregated from the general business operations so that the insurer’s investigators can review documents but are in no danger of having unauthorized communication with the insured’s staff.

Control the flow of documents. All documents to support the claimed loss should be segregated and examined by the claim coordinator before the insurer’s examiner arrives. They should be well organized and, if possible, indexed. The investigators should address any requests for additional documents in writing to the designated contact person. No documents should be given to the insurer’s investigators without having been first reviewed by the claim coordinator.

The independent investigators will probably want to interview the dishonest employee's superiors and coworkers and talk to the person who "discovered" the loss. The insured's representatives have the right to attend these interviews and should do so. The investigators may request the interviews be taped but either the insured or the interviewees may refuse this request. If the interview is recorded, ask for a transcript; if not, take comprehensive notes.

Do not give independent investigators access to a photocopier. Instead, designate someone from the insured organization to copy all documents. Two copies of each document should then be made or the copied documents should be flagged in some other manner.

3.5.2 Subrogation Rights and Duties

If the insurer pays any portion of the claim, the insurer is subrogated to the insured's recovery rights. This is covered under Section B 17 of the *crime general conditions* policy form.

Although subrogation is thought of as arising in the context of a resolved claim, it also imposes a further duty on the insured long before resolution. The insured must in no way jeopardize the subrogation rights of the insurer.

However, if the insured has the opportunity to maximize its recovery as a result of accepting a settlement offer from the dishonest employee or the employee's attorney, the insured could appear to be acting contrary to the language of the subrogation provision. In this case, the insured should bring the settlement offer to the attention of the insurer and demonstrate its benefits. Generally speaking, insurers will agree to reasonable settlement offers. As always, get all such "side agreements" with the insurer in writing.

3.5.3 Response to a Claim Denial

Denial of a claim is not necessarily the end of the matter. Request a detailed, written explanation for the denial. Ask independent advisers to review the claim and the reasons for its rejection to determine carefully whether the denial is warranted. If you can make a good argument for coverage and it becomes necessary to file a lawsuit against the insurer to invoke coverage, the provision form stipulates certain procedures for the insured to follow (see Figure 3-5, Legal Action Against Insurer Provision).

As stated in the clause in Figure 3-5, the insured must give the insurer at least 90 days from the date the proof of loss was filed to investigate and make a decision about the claim. Only after this period has expired, may the insured file a lawsuit against the insurer. The insured, however, is permitted two years following discovery of the crime to bring such an action.

Figure 3-5. Legal Action Against Insurer Provision

LEGAL ACTION AGAINST INSURER PROVISION

You may not bring any legal action against us involving loss:

- (1) Unless you have complied with all of the terms of this insurance;
- (2) Until 90 days after you have filed proof of loss with us; and
- (3) Unless brought within 2 years from the date you discover the loss.

3.5.4 Summary

Fortunately, most organizations experience few employee dishonesty losses of any consequence. The strict policy requirements and sensitive nature of the investigation required to document claims and the entire process of asserting a fidelity coverage claim can be quite intimidating. If addressed in a well-thought-out and logical manner, however, you can effectively handle employee dishonesty claims. The process reviewed in this *Handbook* should give risk and insurance professionals some guidance for planning a response.

3.6 FRAUD INSURANCE CHECKLIST

Table 3.1, “Fraud Insurance Checklist,” is designed to assist CPAs in addressing risk financing and insurance for fraud and dishonesty in their organizations and in those of their clients. If necessary, investigate and follow up “No” answers, and then document the results. Use the “Ref” column to cross-reference the checklist to any additional documentation.

The checklist is intended for general guidance and information only. If risk financing is a concern, seek the advice of a risk management specialist.

TABLE 3.1 FRAUD INSURANCE CHECKLIST

| Fraud Insurance Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| 1. Purchase of Insurance Coverage Against Fraud | | | | |
| a. Has management reviewed operations to determine the nature and extent of potential losses from fraud and commercial crime? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| b. Has management considered the extent to which the organization can self-finance this risk (that is, could it survive a major or catastrophic loss without insurance)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| c. Has management taken all reasonable steps to remedy any previously identified vulnerable areas of the business or any weaknesses in internal controls? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| d. Has management established contact with a reputable insurance broker capable of placing the required fraud and theft coverage? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| e. Has management assigned an appropriate person the task of liaising with the broker to determine alternative kinds, levels, and costs of coverage, and to report back to management on these alternatives with appropriate recommendations? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| f. Are procedures in place to provide for the timely and appropriate response to circumstances where dishonesty is identified, suspected or alleged? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| g. Prior to finalizing the recommended coverage, has management and, if necessary, legal counsel, carefully reviewed the wording of the policy to ensure the following: | | | | |
| ● Definitions, exclusions, and other clauses are acceptable and consistent with the nature of the business. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● When possible, duplication with other insurance (for example, fire policies) has been avoided. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● All statements and information provided on the application for insurance are complete and accurate (for example, where an internal control is indicated, does it exist and is it operating effectively). | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

TABLE 3.1 (continued)

| Fraud Insurance Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| b. Internally, or in cooperation with the underwriter (or both), are adequate resources in place to undertake a thorough and timely investigation? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. After establishing reasonable suspicion of a criminal act, has management called in the police? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Has management ensured that no actions are taken to prejudice the insurance claim, or the underwriter's ability to make recoveries, or both (for example, obtain underwriter's permission before reaching settlement with third parties or suspected perpetrators)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Has management considered initiating legal proceedings to ensure maximum recovery? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Are adequate personnel and procedures in place to perform the following: | | | | |
| ● Document the insurance claim (that is, the "Proof of Loss") | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Follow up with the underwriter as required until the claim is settled | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

CHAPTER 4:

Computer Security and System Recovery

| | | |
|-------|---|----|
| 4.1 | The Role of Computers in Modern Corporations..... | 3 |
| 4.2 | Management's Security Issues | 4 |
| 4.2.1 | Components of Security | 4 |
| 4.2.2 | Management's Key Concerns..... | 6 |
| 4.2.3 | Effective Computer Security Systems..... | 8 |
| 4.3 | Physical Security | 9 |
| 4.3.1 | Computer Room Construction..... | 10 |
| 4.3.2 | Fire Detection and Suppression | 11 |
| 4.3.3 | Water Protection | 12 |
| 4.3.4 | Electrical Power Reliability..... | 12 |
| 4.3.5 | Environmental Control | 13 |
| 4.3.6 | Physical Access Controls..... | 14 |
| 4.3.7 | Physical Security for PCs | 15 |
| 4.3.8 | Physical Security for Portable Computers..... | 15 |
| 4.4 | Logical Security..... | 16 |
| 4.4.1 | Communications Security | 16 |
| 4.4.2 | Data Security | 18 |
| 4.4.3 | Software Integrity..... | 21 |
| 4.4.4 | Computer Operations Security | 22 |
| 4.4.5 | Logical Security for Personal Computers..... | 22 |
| 4.5 | System Recovery..... | 22 |
| 4.5.1 | Recovery From Operational Failures | 23 |
| 4.5.2 | Disaster Recovery Plans | 24 |
| 4.5.3 | Insurance..... | 26 |
| 4.5.4 | System Recovery for Personal Computers and Servers..... | 27 |

| | | |
|-------|---|----|
| 4.6 | Management's Responsibilities in a Security Program | 27 |
| 4.6.1 | Policy, Standards, Guidelines and Procedures..... | 28 |
| 4.6.2 | The Security Function | 29 |
| 4.6.3 | Policing | 29 |
| 4.6.4 | Evidence Recovery | 29 |
| 4.7 | Computer Security Checklist..... | 30 |

CHAPTER 4:

Computer Security and System Recovery

4.1 THE ROLE OF COMPUTERS IN MODERN CORPORATIONS

It is fair to say that modern multinational corporations could not exist without the computer. The size of today's enterprises, the globalization of trade, the velocity of business and the sensitivity of financial marketplaces to news are all driven by the ability to move, store, analyze, and present huge volumes of information quickly, cost-effectively, and accurately. Computers track every type of asset, manage accounting, handle word processing, operate phone and voicemail systems and control communications. Computers have evolved from large mainframes to networks of PCs—each of which has capabilities greater than most of the mainframes from the sixties and seventies—to provide a wide range of services to the modern corporation. Even in those systems whose development was the prime mover of computers from government laboratories to corporate use such as airline reservation systems and banking, we are witnessing a rapid development away from the legacy mainframe to networks of file servers. COBOL, FORTRAN and the other programming and machine languages that facilitated the computer revolution have become largely anachronistic and will inevitably become the digital equivalent of ancient Egyptian hieroglyphs.

This trend toward *digitization* is not hidden within corporations and government agencies. More and more, it intrudes into everyone's life. Going to the bank used to mean dealing with a teller. Now we interact with an ATM or perform many of our transactions through an internet connection with our bank. Our phone systems have digital backbones where our words are translated into binary impulses speeding through optical fibers or shooting into space on their way to or from satellites. The same phone system can simultaneously carry our voice conversations and provide us with high-speed always-on internet connections.

If those computers on which we depend both as corporations and as individuals fail or are compromised, whether by accident or by deliberate action, we are in trouble. Preventing an incident is infinitely preferable to dealing with one after the fact. If an incident occurs, however, the corporation must have a way of recovering operations quickly and efficiently and of understanding how and why the incident happened. Therefore, the establishment of appropriate policies, procedures, and tools to provide computer security and to facilitate system recovery has become a vital function of any organization.

Make no mistake: computer and information security are complex subjects that grow and become even more complex every day. Surveys indicate that the security of information stored in and processed by computers has become a major issue at the most senior levels of management. Businesses spend many billions of dollars each year on hardware and software to control access to computers, secure the data they contain, and detect intrusions.

They invest hundreds of millions more in systems that permit efficient recovery should a problem occur. The federal government has recognized the importance of computer security in the post 9/11 world and has not only established requirements for security within federal systems, but has established an office to coordinate computer security as part of the larger Homeland Security infrastructure. There are firms, some with thousands of employees, specializing in computer security. Clearly, this is a highly specialized field. One chapter in this *Handbook* cannot make you an expert in computer security and it is not intended to do so.

This chapter orients you to the field of computer security so that you, as a CA or CPA, can be certain not only to handle computer security and systems recovery appropriately but also to consider the major risk factors.

4.2 MANAGEMENT'S SECURITY ISSUES

In the modern, global business environment, the computer has evolved from being a *number cruncher* used by the accounting department and tended by a priesthood of mathematical geniuses in a glass-fronted, fire-protected, climate-controlled computer room, to infiltrate virtually every facet of the corporation. The computer has replaced typewriters with word processors, adding machines with spreadsheets, and voluminous physical files with database programs. Time clocks have morphed into automated timekeeping systems or become integrated into access control systems. The eyes of inventory control specialists have become bar code scanners. In many companies, all significant information concerning assets, transactions, and operations are held on one or more computers. The twenty-first century organization likely makes use of hundreds or even thousands of computers connected in various local area networks (LANs) and wide area networks (WANs) connected through switches, bridges, routers, firewalls, Virtual Private Networks, frame relay connections, and the global Internet. An organization may have dozens of these networks each using servers ranging in power from PCs to mainframes.

4.2.1 Components of Security

Data Communications

Businesses do not exist in a vacuum. Increasingly, companies are dedicating more resources to data communications. Many companies—perhaps most, by now—have moved onto the Internet both as a way of distributing information and transmitting information between people or units. Usually, this refers to the World Wide Web, but often includes the use of what are called *Virtual Private Networks* (VPNs). VPNs are secure channels for communicating between a central site and distributed users. Through the use of encryption technology, a VPN provides the means for sending secure traffic over insecure networks like the Internet. The Internet also includes the technology that facilitates electronic mail (email) which has become ubiquitous, instant messaging, which has moved from being a favorite communication tool of teenagers to an increasingly important tool in business, and the use of various techniques (or protocols) to move files across the Internet. Some of these provide a good level of security. Others do not. The space on business cards that in former years held a Telex address now is far more likely to display an email address and a Web site identifier.

Many companies are developing and fielding what are sometimes called *extranets* that link their suppliers and distributors through Internet technology. Other businesses seeking more security than is provided on the global public Internet have turned to private network providers who operate worldwide data communications networks. These providers use the same tools and protocols as the Internet but limit their availability to subscribers and employ various encryption tools to safeguard the information from eavesdroppers.

The latest communication tools have eliminated the use of wires or fibers. Businesses are rapidly installing wireless communication systems either entirely in-house, for example, a wireless LAN, or globally, through tools such as Internet-enabled cell phones. Unfortunately, the security of proprietary information broadcast through the air is not automatically assured. We have entered the age of the “drive-by hack”. Intruders can now sometimes enter our networks by simply driving near our buildings with a wireless-enabled laptop computer to intercept or send messages over insufficiently secured wireless network connections.

Security and System Structure

Before computers, businesses achieved information security by installing locks on file cabinets and file-room doors and by restricting access to various rooms, files and documents. “Intelligent” security systems generally involved underpaid security guards who might (or might not) provide an increased level of protection. During the initial period of computerization, systems were characterized by extreme centralization. Organizations used mainframe computers with attached terminals; if effective access control existed on the central system, since the hardware outside of the computer room generally consisted of “dumb” terminals and local printers, the security situation seemed manageable. Today, the situation is different. How is it possible to secure computer networks and data communications structures that are not only complex but also may exist on a global scale? How do we secure systems that may have hundreds of servers in dozens of locations and communications networks that use private circuits, the Internet, and wireless channels to tie the pieces together?

As businesses increasingly rely on computers and networks, they have a greater need to secure their information-processing infrastructure against accidental or deliberate damage and to provide an efficient, effective, and secure system for backup of data and programs on a regular basis. Organizations need security systems that will facilitate restoring information following an incident or outage. Systems are virtually impossible to manage and keep secure if they are not properly organized, structured and documented. As a key aspect of security and recovery and as a measure of preventive maintenance, businesses should implement a structure for organizing and storing information, for example, data files, spreadsheets, word processing documents, and so on. In developing an effective information storage structure, you should consider issues such as file nomenclature and file access privileges.

There is a lesson that too many organizations have learned the hard way: the worst possible time to discover that your data recovery and business continuity plans are not good enough is just after an incident has occurred and your management and your users are screaming for the system to be restarted.

External Versus Internal Security

As people recognize that information has enormous value—sometimes, in fact, an even greater value than anything else in the organization—their need to safeguard this information increases. The risks inherent in the processing, storage, and transmission of that data have also increased, however, particularly as the Internet has flourished. There have been many documented cases of industrial and economic espionage designed by organizations attempting to jump-start their business activities by stealing proprietary information. In a number of countries, governments also recognize the value to their economies of conducting active intelligence programs that can include what is sometimes called “Industrial Espionage”. When you are being targeted by a hostile or supposedly friendly foreign government, you have to understand that it is only your data security that protects you.

Companies have also been victimized because management believed the major risk they faced was from outside the organization. They spent substantial resources on firewalls and anti-virus protection and very little on other forms of security. Unfortunately, study after study indicates that 80 percent or more of crime against business is perpetrated from within the company, that is, from *inside* the firewall. This is *not* meant to suggest that the external threat can be ignored. That threat is growing, as we can see from the highly publicized incidents of viruses, worms, and “denial of service” attacks. But many of these could be prevented by using a combination of straightforward technological safeguards and common sense.

As systems grow more complex with the increase in bandwidth connecting to the Internet, it is important when assessing security that you consider a wide range of threats and a wide range of ways in which to thwart those threats. Although an outsider can hack into your network to gain access to a specific file, an insider might be able to pick up a carelessly stored backup tape and walk out with a copy of every file in your system recorded on a tape small enough to fit into a shirt pocket.

Because of a corporation's vulnerability, no one should question the need for computer security and the ability to recover from problems both natural and human. It is useful, therefore, to focus on some of management's key concerns.

4.2.2 Management's Key Concerns

Managers in business and government have recognized the growing importance of computer processing to their organizations. Over the last few years, they have expressed their concerns in a wide variety of surveys and publications. These concerns generally fall into one of the following three functional categories:

1. Theft of confidential information
2. Information integrity
3. System availability

Each of these concerns is addressed in the sections that follow.

Theft of Confidential Information

Because companies increasingly store more information in computer systems, corporate governance theorists and practitioners must recognize that in the current environment internal controls have to provide reasonable assurance that this information is well protected both in use and through backup and that only properly authorized employees have access.

For example, theft of proposed pay scales or negotiating positions during labor negotiations would be detrimental to the spirit of the collective bargaining process not to mention a violation of a number of criminal statutes. Theft of marketing or pricing plans would result in a loss of competitive advantage. Similarly, theft of personal or financial customer information could result not only in embarrassment but also in a direct loss of business and possible litigation. Even where information is given out voluntarily, it can cause substantial damage. In 2003, JetBlue Airlines voluntarily provided data on more than a million customers to a U.S. Defense Department contractor engaged in research to identify characteristics of potential terrorists. This was done in violation of the airline's published privacy policy. Aside from very negative publicity, several investigations have been opened, and a number of passengers have filed lawsuits and are attempting to gain class action status.

The threat to the national economy of the loss of valuable intellectual property has become so great that the government has enacted the Electronic Espionage Act, which makes the theft of intellectual property a federal crime punishable by up to ten years in prison. Increasingly, the Digital Millennium Copyright Act is also being used as a basis for safeguarding confidential information and for prosecuting those who seek to distribute protected proprietary data.

Information Integrity

Because of the large volume of information processed by computers, it is not always feasible to confirm the validity or accuracy of processing results. To a large extent, users of a system make the assumption that the information presented to them by various applications is correct. Therefore, management seeks assurance that computer-generated information is reasonably protected against unauthorized tampering by employees, computer viruses, hackers or other forms of sabotage or accident.

For example, tampering that results in inaccurate reporting of sales figures could, in turn, cause inappropriate production, excessive (or inadequate) inventory levels, and lost product sales. Inaccurate unit production costs could result in disastrous pricing decisions. Unauthorized altering of the accounts-payable records could result in incorrect check routing and amounts, and thus create direct financial loss.

System Availability

While recognizing their organization's dependence on the data processing service, management needs to be reassured not only that everything has been done to reduce the likelihood of disruption but also that there are plans in place for resuming data processing in the unlikely event of a major catastrophe. The total or partial loss of data processing services would make it difficult, if not impossible, for most organizations to perform routine business operations. This must also be understood in light of so-called "denial of service" attacks in which hackers do not attempt to break into a system but just to flood it with data

and thus render it inaccessible to authorized users. An information systems disaster recovery plan is not necessarily enough, however. A document with broader coverage, usually called a Business Continuity Plan must take into account the issues of personnel availability, customer demand levels, availability of alternate office locations, changes to business process that will be necessary during the critical period, etc.

4.2.3 Effective Computer Security Systems

An effective computer security program can help to manage and, to a certain extent, alleviate the above concerns. The design of an effective computer security program must take into account the nature of the risk as well as the nature and cost of the controls required to reduce exposure. Note that there is no such thing as 100 percent protection. The growth of networking and particularly of the Internet has materially increased the risk of computer crimes and incidents. The following areas are among those that management must address.

Accidental Versus Deliberate Events

The events that result in breaches in confidentiality, integrity or availability may be accidental or deliberate in nature and may be the result of actions either internal or external to an organization.

On a day-to-day basis, statistics indicate that management should be able to trace most incidents to internal accidents such as an employee entering incorrect data or inadvertently deleting an essential file. Accidents also include failures arising out of undiscovered program errors or bugs.

Virtually every system in use today is built on a software platform that exists as one or more software packages procured from manufacturers. A few may be custom written but even these almost universally operate on a standard, purchased operating system such as Windows® or Linux. In any case, the systems that support an organization, whether procured or written in-house, may consist of tens or even hundreds of thousands of lines of code. It is virtually impossible to test every possible condition that might occur in these immensely complex systems. Indeed, most companies will never actually see the computer code that makes up the programs they use every day, because software companies consider that to be their exclusive property. Program bugs exist in every major system. With the marketplace demanding speedier program development cycles, manufacturers have converted at least a part of their traditional testing procedures into *beta testing* in which the manufacturers release an advance version of the software to customers who test its capabilities on their systems.

It is important to understand the difference between beta testing and the more traditional system testing. In system testing, the software is stressed with deliberate input errors, processing problems and anything else the testing team can do to cause the software to fail. In beta testing, however, the users are not deliberately stressing the system in an attempt to make it break down. Nonetheless, commercial-software beta testing is valuable, and results in reports to the manufacturer of hundreds or even thousands of potential program bugs. Regardless of how thoroughly a program is tested, it can still fail and fail disastrously as the result of an accidental bug. Indeed, there has been a continuing problem with newly identified security issues in widely used packages, which has forced vendors to issue a series of software "patches" designed to close specific security holes. Any organization that is not

closely monitoring the manufacturers of every piece of installed software for newly identified problems and that does not have a procedure in place to rapidly install new patches across all relevant systems is likely to be running with security “holes” that may place the integrity of proprietary information at extreme risk!

Prevention, Detection and Recovery Controls

Prevention is the best and most effective way to minimize the impact of an unwanted event that could affect information confidentiality, integrity or availability. In the case of deliberate acts, preventive controls will reduce opportunity and thereby remove temptation. Another important factor in preventive control is the notion of deterrence because it creates a belief in the mind of would-be perpetrators that they are likely to be caught and punished if they attempt a computer-related crime.

Preventive controls, however, cannot and do not provide a 100-percent guarantee that a problem will not occur. As a result, organizations typically use complementary *detective* controls to highlight any actual or attempted security violation. For example, existing software features may successfully prevent unauthorized users from gaining access to data. In these situations, the software is programmed to produce reports that document all attempts by unauthorized users to access restricted data—a feature known as detective control.

In addition to preventive and detective controls, organizations must prepare in advance for recovery from unexpected events. For example, a plan to use backup copies of files to retrieve an accidentally deleted data file constitutes a recovery control as would having software available to repair simple problems that can make files on a disk unreadable.

A well-designed security program includes elements of all three types of control:

1. Preventive
2. Detective
3. Recuperative

The mix of controls used depends on the nature of the information stored on the computer taken together with the degree of reliance that can be placed on the computer plus management’s willingness to accept the associated risks. In the rapidly changing global environment in which we work, where Internet connectivity grows at an unprecedented rate and new equipment and software may become obsolete in months, it is no simple matter to keep security features ahead of or at least in line with potential threats.

4.3 PHYSICAL SECURITY

Physical security is the generic term used to describe the protection of the computing facility. The controls exercised under the heading physical security are typically preventive and detective in nature.

Many may think that physical security has become unimportant in the age of the personal computer when virtually every employee has a powerful workstation with a fast processor and access to company networks that are often equipped with huge local storage disk drives. But the reality is that mid- to large-size organizations still use midrange computers (such as the IBM AS400, Digital Vax and Alpha systems, HP 9000s, and similar systems

from other manufacturers), mainframes (such as the IBM System 390) and large scale DEC, SUN, HP, Dell and Unisys servers. Even managers at companies that base their computing on a LAN often realize that smaller file servers are best protected by placing them in a dedicated and protected operating facility. In some cases, the servers are placed in the former mainframe room, where they take much less space, and where there is certainly plenty of power, cooling and fire extinguishing capabilities.

Physical security primarily addresses the accessibility concern—the ability to physically access a machine—and attempts to minimize the potential for system loss as a result of equipment theft or damage. To achieve physical security, consider each of the following areas:

1. Computer or Server Room Construction
2. Fire Detection and Suppression
3. Water Protection
4. Electrical Power Reliability
5. Environmental Control
6. Physical Access and Surveillance Controls
7. Physical Security for PCs
8. Physical Security for Portable Computing Devices

Details on each of the components of physical security are presented in the sections that follow.

4.3.1 Computer Room Construction

The National Fire Prevention Association (NFPA) standards provide the most concise specifications for recommended mainframe, midrange, and server computer room construction. In summary, to provide an appropriate level of protection, computer room perimeter walls should be constructed to a minimum of a one-hour fire-resistance rating. These walls should extend from concrete ceiling to concrete floor (slab to slab). Obviously, slab-to-slab walls also protect the facility against unauthorized entry from a false ceiling or a raised floor.

This construction minimizes the possibility of fires originating in general office areas migrating to the computer room before they can be extinguished. The use of standard-glass partitions to segregate the computer room from the general office environment usually does not provide sufficient protection against a migrating fire.

Computer rooms have come full circle. During the sixties and seventies, the only computers in most organizations were large mainframes kept in presumably secure computer rooms. As companies changed from central computers to client-server environments, file servers, which had become the departmental version of a mainframe, did not need special environments. They were placed anywhere—on the floor, under a table, or sometimes in a closet. This led to a lot of problems. Often, they were accidentally turned off or damaged. They did not always have power protection and, on more than one occasion, companies suffered when someone accidentally pulled the server's plug from the wall. With servers in a closet or under someone's desk, backup was sometimes forgotten,

and even when carried out, the backup tapes were often stored adjacent to the server. The trend now is to collect servers and large-scale storage devices into dedicated rooms that can provide proper protection.

4.3.2 Fire Detection and Suppression

Fire detection and suppression systems are essential in the computer room to protect the investment in computer equipment and the information stored thereon. These systems are designed to detect and suppress fire before it advances to a serious state. Security experts recommend automated detection and suppression systems because these systems reduce the dependence on manual fire-fighting techniques that may prove unsatisfactory or arrive too late.

The most common fire-suppression systems are water sprinklers and various fire-suppressing gases. A gas, Halon 1301, formerly the most popular fire suppression gas, is no longer manufactured because it turned out to be a significant environmental hazard. There are a number of fully acceptable replacement fire-suppression gases that do not have Halon's environmental issues. These can be engineered to fit any size computer facility and, although they can be expensive, they provide a very high level of protection. It is particularly important to recognize that these gases do not damage computer equipment.

Water-based systems may serve as the primary fire-suppression system or as a backup to a fire-suppressive gas system. Some building codes may require that sprinklers be installed. Water sprinkler systems may be "wet" or "dry". *Wet* systems contain water in the pipes at all times. *Dry* pipe systems, also called *pre-action* systems, do not contain water until an alarm is activated that usually involves a products-of-combustion detection unit. At this point, a valve automatically opens to charge the system. A high-temperature event must also occur to open a sprinkler head.

Fire detection systems can also provide a direct linkage to other significant support functions such as opening fire exits, shutting off equipment and fans and providing immediate notification to an alarm company or the fire department via a communications link.

In thinking about the use of sprinkler systems, remember that water is not a good mix with computers or any other electrical equipment. Severe damage can be done to system components. A sprinkler system should be considered a backup to alternative systems.

It is also important to have handheld extinguishers around. A handheld unit can put out many fires and prevent the room-wide system from being used. If you have them, please take the time to have your staff trained in their use. Fire departments will usually be glad to help provide this kind of training if you contact your local department's fire prevention unit.

Finally, remember that a large percentage of computer-room fires result from having too much combustible material lying around. A computer room is not a good place to store paper, checks, or anything else that can burn. For a computer-room wastebasket, consider a "self-extinguishing" waste container. These containers have domed tops, which are designed to snuff out a fire by blocking the supply of air.

4.3.3 Water Protection

Water and electrical systems do not mix but both are generally found in computer rooms protected by sprinkler systems. Water can also enter computer rooms through leaks that may originate on another floor of the building. Therefore, it is vitally important to ensure that precautions are taken to detect and remove water leakage before it contacts the electrical supply. Water protection usually involves the provision of the following:

- Underfloor water detectors normally located in the vicinity of air-conditioning units. Water detection systems are usually monitored in the same manner as fire alarms.
- Floor drains remove any water buildup. Unless specified during construction, floor drains typically are not provided in modern office towers.
- Waterproof equipment covers should be on hand where sprinkler systems or other above-floor water sources are present. If they are available, equipment covers or rolls of plastic can be pulled over the equipment in the event of a problem. A simple and inexpensive solution might be to have some rolls of plastic table-covering material (available from party-supply stores). These can be quickly unrolled and cut to size when emergency water protection is needed.

4.3.4 Electrical Power Reliability

Unless suitable precautions are taken, a disruption of the electrical power supply will result in the loss of computer service. The provision of backup-power sources can be expensive and may not be cost justified if the computer center is located in an area where the electric-power supply is reliable. If the electric-power supply is unreliable or the nature of processing critical, consider using uninterruptible power supply (UPS) and backup generators.

Uninterruptible Power Supply (UPS)

UPS provides battery backup in the event of power failures or brownouts. The regular power supply is monitored at all times and battery power automatically provided when required. These systems have become increasingly affordable. Systems sized for PCs can be purchased at discount stores and warehouse clubs. However, it is important to remember that these systems generally have a very limited operational time. Some may only give a few minutes of power if an outage occurs. If power fails when no one is present, the UPS can run until its battery power is expended. You will then find that you have both a dead system and a dead UPS. If reliable operations are critical, you need to add a backup generator to your UPS. Some UPS systems can also tell the server it is running on backup power and that any pre-programmed notification or safe-shutdown routines can be run. UPS systems, even with very limited capacity, can be of great value in helping to step over brief outages ranging from a fraction of a second to a few seconds that would otherwise cause systems to fail.

Backup Generators

Backup generators are recommended because UPS can only provide battery-backup power for a limited time. In computer centers that provide critical processing services or in areas where electric power is unreliable, diesel or turbine generators that can produce electric power for as long as the fuel lasts, often support UPS systems. For PC-based servers,

smaller gasoline powered generators are often readily available through home supply stores and can provide enough power to keep key servers running without the necessity of investing in a large fixed UPS installation.

Power Conditioners and Surge Suppressors

Finally, regardless of the local power supply outage record, it is likely that power conditioners will be used in larger computer installations and surge suppressors provided for desktop PCs. Power conditioners and surge protectors monitor the electric power supply and remove voltage sags and surges that can severely damage computer equipment.

4.3.5 Environmental Control

Environmental control is an issue that primarily has been a concern for larger mainframe computer environments. Even the users of the smaller machines which their manufacturers claim can operate in a general office environment cannot totally ignore the following environmental issues:

1. Temperature
2. Humidity control
3. Environmental contamination

Temperature Control

Computers cannot operate in extreme temperatures. It is true that the range of operating temperatures has increased over the years. However, even when the specifications indicate that the machine will operate in a wide temperature range, for example, 59 to 90 degrees Fahrenheit or 15 to 32 degrees Celsius, it is not advisable to operate these machines near either limit. Air conditioning is usually installed to reduce the likelihood of system outage or damage as a result of overheating. Where it is necessary to install an unusual amount of heat-generating equipment in a PC case, for example, if a number of hard drives are added, consideration should be given not only to operating the machine in a climate-controlled location but also to installing an extra fan in the case to dissipate the heat. There are fan units available through a number of vendors that can be placed into a standard drive bay or standard circuit card position.

Humidity Control

The computer manufacturers normally indicate a range of humidity acceptable for their machines, for example, a 20-to-80 percent humidity tolerance. Normally, the air conditioning unit provides humidity control.

Environmental Contamination

Dust can cause major problems in a computer environment. If dust gets into a removable storage unit, it may cause a head crash and make information on that disk inaccessible. In addition, accumulations of paper dust from printers are a potential fire hazard. To minimize the potential for dust contamination, you should regularly vacuum the areas where dust normally accumulates.

4.3.6 Physical Access Controls

The importance of physical access controls over all assets and related records is obvious. Such controls help to reduce the risk of fraud and commercial crime for the following reasons:

- Physical access controls are often most visible to potential perpetrators. Strong controls in this area send a powerful deterrent message vis-à-vis the other controls in the system. Conversely, loose physical controls invite challenge.
- Perpetrators of many frauds must come into physical contact with either the asset being misappropriated or the related-asset records in order to cover up the fraud. Reducing physical access reduces opportunity.
- Access controls that fail to prevent fraud and commercial crime still often assist in the investigation process, for example, the determination of what actually happened and the narrowing of the list of possible suspects.

The physical security of computer installations and equipment is particularly important. Sometimes white-collar criminals and irate employees resort to blue-collar crimes, such as arson and the willful destruction of property. When this happens, these blue-collar crimes may be classified as being commercial or economic in nature. There are also new categories of computer crimes defined by most states and the federal government. To combat these new crimes, new laws have been passed specifically directed at protecting computers. The destruction of a computer may involve a number of chargeable offenses, some of which are general in nature, for example, malicious mischief. Others are more specific, such as economic espionage or computer tampering.

The only employees who should require physical access to computer equipment are those responsible for its operation. Any third-party engineers performing maintenance should be accompanied by operations staff or otherwise monitored at all times. Providing more access increases the potential for vandalism, mischief, and human error; any of these threats could result in processing disruptions.

Limiting access to the computer/server room involves securing the doors and keeping them closed at all times. There are a variety of devices available for achieving this. The most common include the following:

- *Key locks.* These are the cheapest to install but are usually the least secure because duplicate keys can be made and distributed without control. At the very least, all authorized keys should be marked by the locksmith with the words DO NOT DUPLICATE. Reputable locksmiths will not duplicate a key with such a marking. This does not prevent extra keys from being made, but it sharply reduces the number of sources for such duplication.
- *Cipher locks.* These are push-button combination devices and are generally more secure than key locks provided the combination is changed on a regular basis. The downside of these locks is that the combination can be easily shared with unauthorized persons. Whereas a physical key is needed for a standard lock, only knowledge of the combination is required to operate a cipher lock.
- *Card-access devices.* These are among the most secure mechanisms because cards cannot be readily duplicated and card distribution can be controlled. There are also card-access

devices that require the user to enter a pass code along with the card key. These are more secure than standard card-access devices since the user must have both a physical device (the card) and knowledge of a secret piece of information (the pass code).

- *Biometric locks.* These provide access based on physical characteristics. Perhaps the most commonly used involve hand geometry, but devices based on fingerprints, iris recognition, and facial recognition are also becoming commercially viable.

4.3.7 Physical Security for PCs

Much of the preceding discussion relates to computer systems of any size. The following is important information for the physical security of PCs:

- Restrict physical access. Lock doors during off-hours or whenever an office is vacant, or both.
- Use the security features provided on many PCs, such as passwords, that prevent access by unauthorized individuals.
- Ensure that all employees watch for unauthorized personnel in areas where personal computers or servers are located.
- Consider using any of the various devices that can prevent the removal of PCs for those that have high-value data stored in them. These devices include pads that are screwed or pasted down or cables that can lock a PC to a desk.

4.3.8 Physical Security for Portable Computers

Portable computers such as laptops, notebooks, sub notebooks, and personal digital assistants (PDAs) also present security issues. Their large storage capacities can hold huge volumes of confidential information. Experience indicates that these are attractive targets to both thieves and those who would commit industrial espionage. Some security tips follow:

- When taking a computer through an airport security checkpoint, do not put the computer into the X ray machine until the metal detector is clear for your use. There have been a large number of incidents in which one member of a criminal gang delays you after you have put your computer case onto the x-ray belt by finding more and more metal objects on his or her person. By the time you can go through the metal detector, a confederate of the “blocker” has already taken your PC case off of the belt and departed. Since in the U.S. you are required to put your PC through the X ray machine separately, and since most portable PCs look alike, make sure to prominently mark your machine on the top and bottom. A label with your name, or even a large sticker is good. The objective is to make it easy for you to recognize your machine, and others to recognize that the machine is not theirs.
- Do not leave your PC unattended in your hotel room. Where possible, put it in the safe in your room (if one is provided) or in the hotel safe-deposit box. Another option is to keep all of your confidential data on a removable device or to remove the hard drive from the laptop and take the data with you. If the machine gets stolen while you are out, you still have the data. It is now very cost-effective to use flash memory devices. A flash memory device that plugs into either the PC card slot or the USB port can store up to 4 gigabytes of data.

- Consider installing software that can detect whether the computer has been stolen. This software attempts to contact a data center through an Internet connection to report its location. Such software is available from several vendors.
- Use encryption software which is often included with new PCs. You can set your machine to encrypt the hard drive's contents which only become usable when the correct password is entered.

4.4 LOGICAL SECURITY

Logical security is the term used to describe the overall method for the protection of information stored on a computer system. The controls involved are usually a blend of preventive and detective controls. Organizations use logical security to address confidentiality and integrity concerns and to reduce the potential for inappropriate information disclosure, modification, destruction, or deletion.

Achieving an appropriate level of logical security involves giving careful thought to how the user gains access to information. In addition to the security controls for the data itself, you should consider the controls over the software that provides access to the data and to the system. In so doing, keep in mind the following:

- Communications security
- Data security
- Software integrity
- Computer operations security
- Logical security for personal computers

A description of each follows.

4.4.1 Communications Security

Communications security focuses on controlling the various methods of access to the computer system. Of course, communications security serves primarily to ensure that valid transmissions between computer systems are complete and accurate. As an added benefit, communications security also presents an obstacle to criminal activity.

Passwords and Administration

A valid user identification and password is the first line of access control on most computer systems. The validation of the ID and password by a computer program represents the preventive part of the control while the rejection and recording of an invalid ID or password represents the detection control. To be effective, the detective aspect of password control requires an investigation of all reported access failures.

For effective password controls, procedures should be installed to ensure the following:

1. Users choose passwords that are not simplistic in nature. Because simplistic passwords can be readily guessed and the system compromised, never use initials, a spouse's name, or other similar personal passwords. For example, you could implement a policy that

requires passwords to have a defined minimum length and require them to contain at least one letter, one number, and one special character. A password like *interaction* would be more secured if it was replaced by *!nterAct10n*.

2. Management distributes new user IDs and passwords to users in a controlled manner. The initial password should be required to be used within a limited period and users required to change the initial password to a new one on their initial login.
3. Users change passwords regularly, approximately every thirty to ninety days, depending on the nature of the information accessed. The system should keep track of a number of prior passwords to prevent their reuse.
4. Management revokes IDs and passwords of users who have left the organization. Similarly, when users move from job to job within an organization, management modifies their access rights so they can only access the data required for their current job.

Network Security Features

The programmed network security features that are available vary from system to system. Some of the common features include:

- *A maximum number of log-on attempts.* If the user has not successfully logged on in the specified number of attempts, the session is terminated and the incident is recorded on a log for investigation. To prohibit additional attempts to compromise the account, some systems lock the user's account either for a limited time (5 to 30 minutes) or until reset by the information security unit.
- *Automatic log-off of inactive terminals.* If an employee leaves a terminal logged-on, anyone who gains access to that terminal has the access rights of the previous user thereby breaching password security. Therefore, many systems automatically log off users when the terminal has been inactive for a defined period of time. Alternatively, some systems invoke a screen-saver that prevents using the system until the password is re-entered.
- *Restriction of users to specific terminals.* Users must be restricted not only to specific terminals, but also to specific times of the day, or both.
- *Echo checking.* The protection of transmitted information by echo checking ensures the information is complete and accurate. This is achieved by a retransmission of the message to the source terminal for validation.
- *Firewalls.* Provide the security necessary to control unauthorized access to the system from the Internet with firewalls. Ranging from relatively simple hardware or software to complex and hard-to-maintain packages, firewalls have become a requirement for systems attached to the Internet. Careful planning is essential to prevent making unintended access points available to an invader by putting the firewalls in the wrong place in the network. In complex networks, multiple firewalls may be required. Firewalls must also be carefully configured with the proper instructions entered into the firewall. Errors can leave security "holes" that may be exploited by intruders.
- *Intrusion Detection Systems.* Intrusion detection systems (IDSs) consist of hardware and software that monitor activities within a system to determine whether those activities represent a potential problem. For example, a user who suddenly begins to download large amounts of proprietary information might be reported for investigation or, alternatively, have their access privileges suspended pending a review. These systems,

which are now evolving, may be either network-based, that is, they review traffic on a given communication channel, or host-based, whereby they monitor the work of a given server.

Remote-Access Security

Hackers have received considerable publicity in recent years after successfully gaining unauthorized access to numerous computer systems. In response to the problems created by hackers, several companies have developed and marketed security devices to limit remote access to authorized employees.

One common device available to help control dial-up computer access is the callback device. When an employee dials in, the callback device intercepts the call, the employee enters a special code, and the device then *calls back* the phone number associated with the code entered. The communications link is then established and the user ID and password are entered in the normal way. This, of course, is based on dial-up access. As more and more corporate communication goes over the Internet, this security tool is becoming less important.

For both dial-up access and Internet access, there are a number of devices that provide security by effectively providing authorized users with a new password for every log-on. Some systems accomplish this by providing the user with a small keychain-sized device called a *token*, which has a window that displays a new code every minute. The user must enter this code along with a memorized password to gain access.

Another version looks much like a calculator. When a user requests access, the system provides a random number (the challenge) that the user then enters into the *special calculator* along with a password. The calculator then displays another number (the response), which is entered into the system to gain access.

Another class of access control based on biometrics involves the measurement of a physical characteristic. Currently, manufacturers offer devices that can check identity based on fingerprints, hand or facial geometry, and iris or retinal patterns. Systems based on voiceprint or signature dynamics are also under development. These systems are becoming increasingly cost effective. For example, a number of fingerprint-reading devices can be had for less than one hundred dollars.

4.4.2 Data Security

Unauthorized access to information can result in its disclosure, modification, or deletion. To achieve efficient data security, you should implement a system capable of evaluating the sensitivity of the data to provide a level of protection commensurate with the nature and perceived value of the information. Data security addresses the issue of protecting information stored on computer files, magnetic media, and hard copy reports.

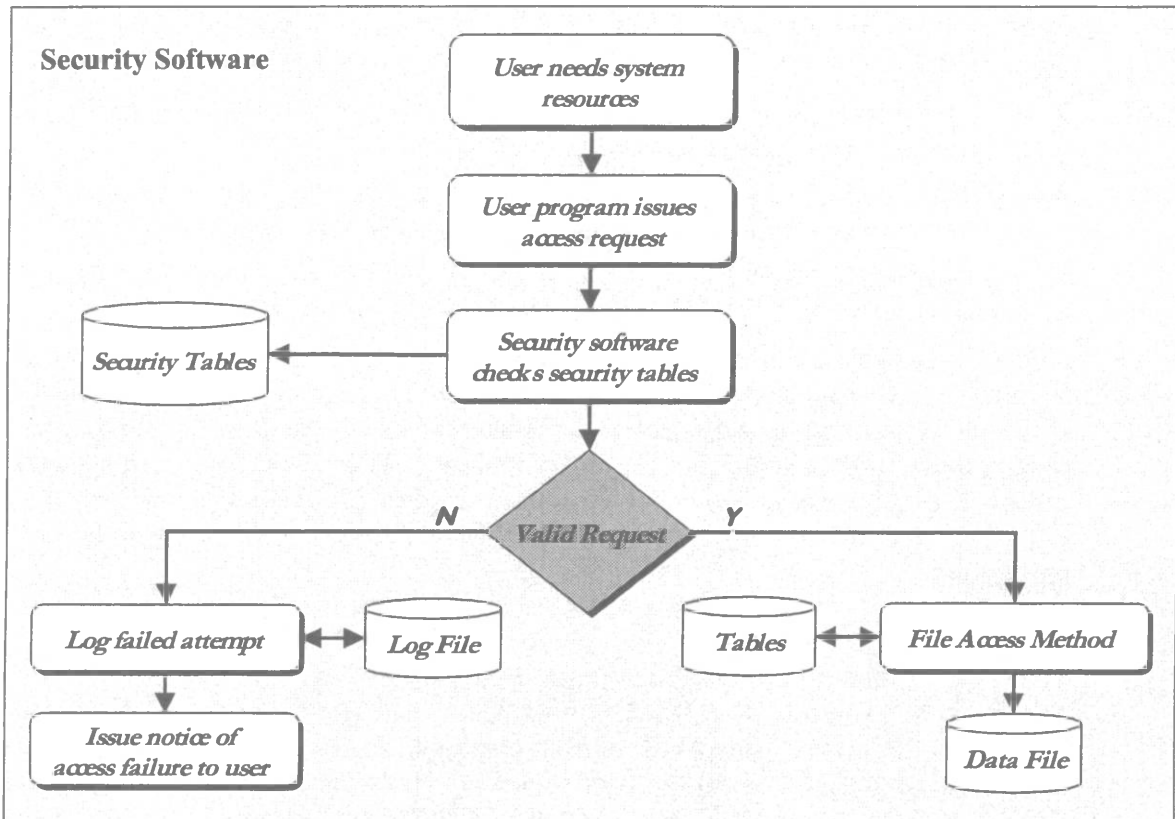
On-line Data Files

On-line data files are those files stored on a computer system that users can access directly. The following two effective techniques are available to secure on-line data files:

1. *Software restrictions.* A program or series of programs that reference established security tables to determine whether the user is allowed the requested access, for example, to read or write, to the requested data file. If the request is valid, the user will be permitted

access; if not, access is denied and the access violation is reported on a log file for subsequent investigation. The security software process is illustrated by Figure 4-1, "The Security Software Process."

Figure 4-1. The Security Software Process



On some computer systems, the software restriction facility is an integral part of the operating system, while on others a separate security software product that interfaces with the operating system is used.

2. *Data encryption.* This technique scrambles information using a predefined algorithm or key so that the information is not meaningful to anyone who merely gains access to the disk file. There are a number of mathematical systems (algorithms) in use as the basis of encryption systems. These systems use keys of various lengths and complexity. Longer keys usually provide more security than shorter ones. On the Internet, all browsers provide some level of security through encryption. Some have short-key capabilities generally employing 40-bit keys that provide a basic level of security while other versions are often export-restricted and use much stronger 128-bit keys. Some data-encryption packages, for example PGP, can provide for even longer keys often 1,024 bits in length, which provide incredibly robust security against unauthorized interception. Companies using the Internet to transmit confidential data should

seriously consider using encryption to protect that information from unauthorized interception. Encryption should also be considered for email as well because standard email is not secure.

Offline Data Files

Offline data files are information stored in libraries on magnetic tape, removable disks, and diskettes. Information stored on these media is as readily susceptible to inappropriate disclosure, amendment, and deletion as online data files unless it is properly controlled. The preventive controls usually applied include the following:

- Keep the media library in a physically secure room where the door is locked unless an authorized staff member is present.
- Adhere to media library procedures requiring that files be issued from the library only for approved purposes, for example, production use and transport to off-site storage.
- Assure that the media, when no longer needed for storage of confidential data, are erased or destroyed. As long as they contain data, they should be protected.

Detective controls normally include an investigation of all materials borrowed but not returned in a reasonable time as well as the performance of periodic inventory checks. However, many smaller organizations consider the use of comprehensive library procedures impractical because of limited staff availability. In these situations and in personal computer environments, you should regularly back up computer information on hard disks and diskettes and store the backups in a secure location away from the computers.

Reports and Documents

It is easy to become preoccupied with protecting information on computer systems while neglecting the information printed on input forms and computer reports. Generally, people rely on internal controls exercised by user departments to ensure that data approved for input is not modified before it is entered into the computer. Frequently, however, people pay less attention to securing input documents before and after input. Yet these input documents contain all of the confidential information ultimately stored on disk.

You should also pay attention to printed output, including the following:

- *Printing control.* Completely destroy any partially printed reports that result from printer problems.
- *Distribution control.* Ensure that the appropriate staff distributes computer-printed reports, particularly reports containing sensitive or confidential information, only to authorized recipients.
- *Storage security.* Staff should secure computer reports in the user department for protection after office hours.
- *Destruction control.* Staff should completely destroy all reports when no longer required. This practice applies to all offices, not just computer areas. Even when information is outdated, improper disclosure may still prove embarrassing.

4.4.3 Software Integrity

Software integrity refers to the protection of all system software stored on magnetic media and the migration of programs to production. The integrity of information depends not only on the accuracy of the input data, but also on the integrity of the programs that produce and use that information. Integrity of information also depends on the integrity of the communications software, transaction processors, file access software, security software and operating system—known collectively as the system software—that control the operation of and possible use by application programs.

Online Software Libraries

Computer programs are stored on disk files in libraries or software directories. The most effective means of restricting user access to these libraries is through security software restrictions as described earlier in the section entitled “Online Data Files”, although library control software may also assist in restricting user access.

The programming staff requires access to copies of the programs to perform their jobs. They do not, however, require access to the production versions. Providing programmers with direct access to production versions compromises software control and increases the possibility that unauthorized changes may be made. In general, only qualified *production librarians* should require access to the production programs and those individuals should copy only new versions of programs into production as required.

Offline Software

Offline software refers to the backup copies of program libraries or directories stored on magnetic tape, exchangeable disks and diskettes. The controls required to secure these versions of the software are identical to those described earlier in this chapter in the section, “Offline Data Files.”

Migration of Programs to Production

If a programmer can gain access to a program and make changes between the program tests being performed by the user and the program being put into production, the version used in production may not be the same version that was originally tested and approved. Changes may be introduced that could affect information integrity and expose the organization to financial loss. Organizations can address this problem in a variety of ways including the following:

- Restricting access to the test version of the program to the users who are running the test and the individual(s) who are performing the librarian function responsible for the transfer to production.
- Record and monitor the time when the last change was made provided the system or library control software retains that information. The date of the last change should not be later than the date the tests were run and the software approved for use.
- Assure that all updates provided by software manufacturers are applied promptly. These should always be tested before being put into production to assure that the updates have not had an unintended result.

4.4.4 Computer Operations Security

Improper operator intervention also can affect the proper operation of computer programs and, therefore, the integrity of information. In particular, computer operators can create problems by performing the following:

- Run the incorrect version of a program against the correct data files. This may introduce errors through the use of untested program code or the possibility of fraud through the use of unauthorized code.
- Run the correct version of the program against incorrect versions of data files. Obviously, the results produced by this action would be incorrect and could have serious implications.

To control operator activity effectively, you should consider taking certain measures including the following:

- Restrict an operator's ability to change the Job Control Language. Job Control Language directs the processing of a program and identifies the program to be run and the data files to be used.
- Use internal tape, disk-label checking, or both, to ensure use of the correct file.
- Provide detailed operating instructions to reduce accidental error.
- Monitor operator intervention by reviewing the computer activity-console logs and investigating unusual activity.
- Reconcile data file totals from run to run to ensure use of the correct version of the file.

4.4.5 Logical Security for Personal Computers

The important points to note with respect to logical security for PCs include the following:

- Be wary of leaving sensitive information on hard disks unless the files are encrypted. Consider using removable disk-cartridge devices or removable hard drives. Data may also be stored on flash memory cards.
- Use cryptic passwords. Do not leave passwords on or near computer workstations.
- Back up hard disks regularly to CDs, network drives, or tape.
- Remember when erasing a hard disk that the normal erase procedures of some operating systems leave the file on the disk, that is, it may only remove the file name from the directory. Even reformatting a PC hard drive does not make the data unrecoverable. To prevent any possible recovery of sensitive files, use the disk-wiping functions provided by commercial hard-drive utilities programs. These programs overwrite the space used by the file—often several times—to make the information completely unrecoverable.

4.5 SYSTEM RECOVERY

If properly applied, the preventive and detective controls provided by physical and logical security will minimize the possibility of problems occurring. However, problems do occur—either accidentally or deliberately. System recovery procedures are intended to

assist in implementing an orderly and controlled return to normal operations in the event of a problem.

You should consider using recovery controls to address any computer-related availability concerns. These controls are necessary to address short-term problems as well as more catastrophic long-term events.

4.5.1 Recovery From Operational Failures

Operational failures are those problems that occur during the performance of day-to-day processing. Examples include the following:

- Incorrect file usage
- Disk files deletion
- Disk files destruction
- Job processing failure
- Computer equipment or media failure. For example, most people have seen cassette tapes that have been “eaten” by players. Drives fail. Tapes can break.

Overcoming problems of this nature requires an appropriate combination of back-up and written recovery procedures.

Data File and Software Backup

To protect against accidental or deliberate destruction by hackers, for example, it is essential that you and your staff regularly make copies of all data files and software library directories. How often is “regularly?” This will vary from installation to installation. To determine an appropriate backup cycle, you should consider the following factors:

- The frequency at which file managers update the file, library, or directory. This will help managers determine when to make backup files. For example, for system-software libraries that are rarely changed it may be more effective to make backup copies only after making changes.
- The number of transactions processed each time the file is updated. This total helps managers determine the amount of effort required to reprocess all transactions entered since the last available backup was taken.
- The amount of processing time available for backup.

In the past, a backup cycle was often determined on an application-by-application basis. Today organizations typically take a weekly copy of all files and libraries and supplement this with daily *incremental* backups. Incremental backups take copies of only those files and libraries that have been updated during the day.

In many firms, employees frequently work off-line from their server either away from their office or saving files directly to their local drives. To ensure that all necessary data is properly backed-up at appropriate times, you should establish guidelines that stress the importance of the employees moving their work to the server as soon and as often as possible. This not only provides back-up protection in the event of a personal computer failure but also maintains a complete data record on the server for back-up purposes.

To assist in recovery from day-to-day operational failures, keep a backup copy of the data files and software on site. In addition, send a copy off site for use in the event of more catastrophic problems such as when all on-site material is either unavailable or destroyed. (See section 4.5.2, "Disaster Recovery Plans").

With the growing availability of high-speed data lines, other new forms of backup are evolving. Remote vaulting and remote backup involves transmission of backup files to another location so that the backup is actually created offsite. It is also possible to maintain disk storage at a remote location and to keep it updated on an essentially real-time basis. The tremendous increase in storage efficiency has made hard drives of as much as 160-gigabyte capacity available for as little as \$100. The use of RAID (Redundant Array of Inexpensive Drives) arrays can provide for storage units that not only have high capacity, but can also write multiple copies of each record to different disks, so that a failure of any one disk drive will not result in loss of data.

Recovery Procedures

In addition to providing backup copies of the files and libraries, give sufficiently detailed written instructions to the operators so they can efficiently and effectively recover any necessary files. These procedures are described in most computer-operational manuals and should address issues such as:

- *Application failure recovery measures.* These measures are normally documented for each application and for each job step within the application. These measures describe how operators can restore processing at an earlier point, and reprocess transactions. In some cases when restoring and reprocessing is not possible, the manual should provide direction for obtaining programming or technical support to resolve the problem.
- *Use of utilities to recover from backup copies.* The involvement of operators in recovery varies from organization to organization. In some installations, the operators copy the files and libraries to a predefined recovery area on disk and it is the responsibility of a user or support group to copy them from the recovery area to the production area. Other organizations will recover directly to the production areas.
- *Vendor support for equipment failures or head crashes.* Users should document all equipment failures including details of the request for vendor assistance and the vendor's response.

4.5.2 Disaster Recovery Plans

Disaster recovery plans are intended to assist with recovery from a catastrophic event. They are not intended to deal with day-to-day operational failures. The term *disaster* is used in the broadest sense; it need not be an act of God. It could be anything from a drunken driver knocking down a power pole to terrorism. As previously noted, white-collar criminals can also arrange disasters to cover up their crimes.

Definition

A disaster recovery plan is a documented description of the course of action to take, resources to be used, and the procedures to be followed before, during and after a disruption of data processing capability.

Given the business community's current reliance on computers, many executives would probably find the loss of the computer center for a lengthy period of time inconceivable.

However, the same executives' organization has probably taken little or no action to develop or maintain a contingency plan. A survey completed several years ago suggested that less than 50 percent of the *Fortune* 1000 companies had disaster recovery plans and, for the companies that did, only half the plans were feasible.

Elements of Effective Disaster Recovery Plans

Before disaster occurs, you should take action to ensure that off-site backup is capable of supporting recovery operations. Keep off-site backup copies of data files and software some distance from the principal site so that these vital records will be accessible in the event of a disaster affecting the local geographic area. Where appropriate, companies should contract for services with disaster recovery centers that maintain hardware for use when needed.

Consider what happened when a train derailed in Mississauga, a suburb of Toronto, Canada, a few years ago. In this case, the authorities closed access to a sizable area of the city for five days because of a dangerous chemical spill. Any organization housing both its data center and off-site storage in that geographical area would have had difficulty implementing its disaster-recovery plan.

In addition to keeping off-site backup copies of data files and software, consider keeping off-site supplies of other materials required for processing. Examples include: check stock files, special invoice forms and forms for laser printers, operations documentation, and a copy of the recovery plan.

Documenting detailed recovery procedures and implementing regular tests of the recovery plan are the most important actions to be taken before the advent of a disaster. Disaster-recovery operations require the channeling of information to management to assist in decision making during the chaos of a disaster. Without clearly identifying reporting channels and decision points in advance, employees may later take inappropriate action.

Prepare detailed procedures for system recovery because operations staff may not perform standard procedures as expected when affected by the stress of a disaster. Remember that in a disaster, personnel who might be expected to participate in the recovery—either on the operations team or the management team—may themselves be victims of the disaster. The plan must anticipate this possibility by designating one or more alternates for each recovery position. Regular testing ensures that the plan is workable and helps to keep the plan current.

During the disaster, the staff with recovery responsibilities should follow documented procedures to:

1. Notify all necessary parties that a problem has occurred.
2. Assess the extent of the damage and the expected period of system outage for communications to the recovery team.
3. Report to a predetermined emergency control center.

After invoking the disaster recovery plan, the recovery staff should follow the documented procedures for:

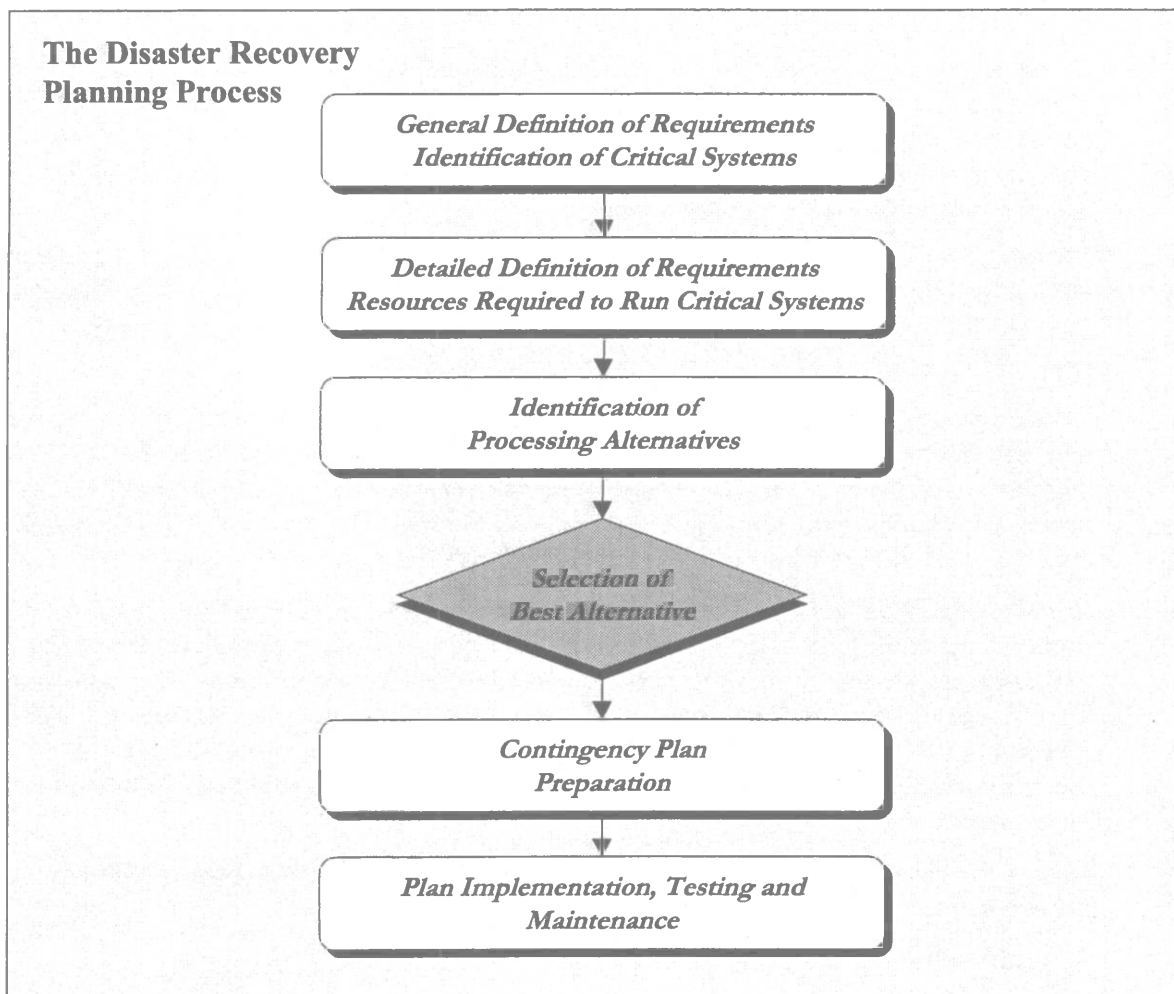
1. Recovering the critical systems at the identified alternative-processing location.
2. Operating at the alternative site.
3. Refurbishing or replacing the damaged site.

4. Returning to normal operations once the damaged site has been refurbished.

Most organizations plan to recover only the critical systems at the alternative-processing site. These are the application systems needed to ensure continued business operations. If sufficient resources exist at the alternative site to run other systems, do not recover them until the critical systems are running.

See figure 4-2 for a schematic of an approach to developing a disaster-recovery plan.

Figure 4-2. The Disaster Recovery Planning Process



4.5.3 Insurance

For most businesses that rely heavily on computer processing, an effective disaster-recovery plan is likely the only effective means of ensuring continued business survival following a major computer-system disruption. However, it is possible to mitigate some of the financial loss through insurance coverage. Some examples of the kinds of insurance coverage available include:

- *Data processing equipment coverage.* These policies assist in defraying the cost of replacement-computer hardware and air-conditioning equipment. Some policies also cover the cost of removing the debris from covered equipment.
- *Data, computer programs, and media coverage.* These policies cover only data and programs in computer format, not hard copy. Organizations can take out insurance to cover the estimated potential loss if data and programs are destroyed.
- *Extra expense coverage.* These policies cover the extra expenses involved in continuing data processing operations if the equipment, air conditioning, or building housing the equipment is damaged.
- *Business interruption.* These policies cover the business losses incurred following a disaster in the computer department but are subject to limits on the amount to be paid per day and a total amount payable.
- *Fidelity coverage.* These policies may cover costs associated with the unlawful acts of a dishonest employee. There are various new forms of crime coverage that may extend to certain acts by outsiders as well.

4.5.4 System Recovery for Personal Computers and Servers

Equipment failure for PCs generally is not a major concern for organizations, particularly compared with similar situations associated with larger computer systems. It should be given more attention, however, considering the dependence of many businesses on PCs and local area networks. If a PC fails, normally another machine is available or can be obtained with relative ease. LAN file servers and the communications gear associated with connecting LANs to private and public networks, including the Internet, may be highly specialized and take one or more days to replace and reconfigure. The biggest concerns are the potential damage to communications facilities that would cause a loss of electronic mail functions and the loss of data stored on hard disk or diskettes. If the failed system was running the firewall, loss of a PC server could seriously compromise the security of the organization's information.

Good PC and LAN security should be a priority to avoid situations requiring recovery. However, as noted earlier, disasters do occur. Therefore, a regular policy of backing up hard disks is advisable. Consider using one of the specialized backup-software packages that will help you manage the process. Also be aware that computer data recovery specialists can, under some circumstances, help you recover information that has been accidentally or deliberately lost. You should consider establishing a relationship with a data recovery company before you have need for their services. Selecting a vendor during a crisis is not a recommended procedure.

4.6 MANAGEMENT'S RESPONSIBILITIES IN A SECURITY PROGRAM

Management is responsible for protecting the organization's assets against both dishonest employees and outside criminal acts. The information asset, administered in most organizations by the information systems or computer department, is as vital and vulnerable as any other asset. Although many organizations have invested heavily in the development of computerized systems to support their business operations, they have not

necessarily invested sufficient effort to establish a security program that would adequately protect that investment. Computer security is often neglected because of pressures to deal with day-to-day operating needs first, yet security can be *fundamental* to business survival.

You can implement effective security by identifying the following:

- The information in your organization that requires protection
- The level of protection currently provided for that information
- The risks and exposures that currently make that information vulnerable
- The right combination of information security tools and techniques based on your needs analysis

Using this approach you can achieve a level of security that is appropriate to the requirements of your organization. The objective is to provide sufficient security without going overboard and making security more complex than necessary. After taking the steps outlined in this chapter, your organization can implement a security program to address the exposures. This program should incorporate the development of policies, standards, guidelines and procedures, the assignment of security responsibilities and the monitoring of progress.

4.6.1 Policy, Standards, Guidelines and Procedures

It is generally unwise to assume that employees will act in a security-conscious manner particularly if the organization's expectations in this regard have never been communicated. Companies can communicate policies through the development and implementation of policy statements on computer security and should emphasize security and fraud awareness.

Effective policies must be succinct. If policies are too detailed and lengthy, they probably will not have the desired effect, especially with junior-level employees. For brevity, simply cross-reference the more detailed standards rather than attempting to include this material in the policy statement itself. The policy, standards, guidelines and procedures provide a framework for effective security in any organization.

Many organizations in consultation with legal counsel have determined that it is important to have employees sign security and confidentiality agreements that define the person's responsibility for safeguarding information in all forms. Indeed, many organizations have also developed agreements to be completed by contractors, vendors and temporary workers who require access to confidential and proprietary information. You should give careful consideration to implementing a policy calling for employees and others, such as temporary workers, who have access to your systems to sign these security and confidentiality agreements on an annual basis, perhaps in conjunction with an annual review program.

There is an international standard for information security called ISO/IEC 17799, consisting of a policy guide (ISO/IEC 17799-1) and implementation guide (BS 7799-2) which many organizations are using as the basis for their information security programs. The standard gives a way of measuring your program against an accepted set of policies as a step to a comprehensive solution.

4.6.2 The Security Function

Having recognized the importance of computer and information security to the organization, management must assign responsibility for carrying out the duties associated with this function. The person identified to take on the security function will usually be responsible for:

- Assisting in the development of policies, standards, and guidelines and procedures.
- Developing a formal security program to improve the level of security in accordance with management's expectations.
- Raising security and fraud awareness.
- Reporting on progress to senior management.
- Remaining in close contact with specialists such as police, forensic accountants, computer forensics experts, and specialists in computer viruses who can assist in implementing the program or help in the event of a crisis.

This may be either a full- or part-time responsibility according to the size of the organization. Initially, setting up the program probably will require a full-time position and can be aided by outside, experienced assistance. One important function of the person or team charged with the computer-security function is to check the Internet regularly for new information about the latest trends in fraud prevention and fraud techniques. Another specific responsibility is to maintain liaison with the manufacturers of the hardware and software that is in use within the company to get the latest security "patches" as they are issued. There are also a number of organizations that one can join that can provide useful information and ideas for the security professional. These range from large national organization like the American Society for Industrial Security to government sponsored groups like Infogard.

4.6.3 Policing

Once the security program is underway and the policy, standards, and guidelines and procedures are in place, an organization must ensure compliance with expectations on an ongoing basis. This is a policing function.

Most organizations have an internal audit department that performs the policing function for controls that operate in other areas of the business. As such, internal audit may be an ideal candidate to become involved in testing compliance with corporate security expectations. Alternatively, external auditors or consultants can fill this role. In addition, it should be remembered that many software packages generate both activity and security logs. Reviewing the security logs is an important aspect of the policing function.

4.6.4 Evidence Recovery

If a security incident occurs, computer and security personnel may find themselves pursuing different objectives. In an actual case in which a company's email servers suddenly reformatted their hard disk drives, the computer operations department saw as its objective repairing the damage and restoring email services within the company as quickly as possible. In contrast, the security people regarded the data center as a crime scene and wanted to collect evidence to determine whether the incident had been a technical accident

or the deliberate act of a perpetrator. The two groups had to work together to ensure that the technical personnel assigned the task of restoring service and the hastily summoned outside consultants would understand the importance of identifying any evidence of wrongdoing and call in the security people to gather and secure the evidence so that it would be admissible in court.

In cases in which the crime scene is, in fact, the surface of a hard drive, the collection of evidence becomes critical. As with any other evidence, it is necessary to ensure that the process of collecting and safeguarding the evidence also preserves that evidence from any changes. Courts will not turn a blind eye when recovery technicians have made changes and later claim that the hard drive bears evidence of a crime. Under these circumstances, how would it be possible to prove that the purported evidence of a crime was not planted to incriminate an innocent person? In complex or important cases, this task is often assigned to experts in the field of computer evidence recovery—a discipline known as *computer forensics*. Computer forensics is discussed in more detail in Chapter 8.

4.7 COMPUTER SECURITY CHECKLIST

Table 4.1, “Computer Security Checklist,” is designed to assist CPAs in dealing with computer security in their organizations and those of their clients. Generally, all *No* answers require investigation and follow-up. The results should be documented. Use the “Ref” column to cross-reference the checklist to any additional working papers.

The checklist is intended for general guidance and information only. Use of the checklist does not guarantee the adequacy of computer security, and it is not intended as a substitute for audits or similar procedures. If computer security is an especially vital concern or if computer fraud is suspected, seek the advice of a knowledgeable computer professional.

TABLE 4.1 COMPUTER SECURITY CHECKLIST

| Computer Security Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| 1. Physical Security | | | | |
| a. Computer Room | | | | |
| ● Does the room have minimum one-hour fire-resistance rating plus smoke detectors, fire alarms, extinguishers, and sprinklers? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Is the room protected with a remotely monitored alarm system? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Are there underfloor water detectors, floor drains and waterproof equipment covers to protect against water damage from sprinkler systems? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Are there battery-equipped Uninterruptible Power Supplies (UPS) or backup generators and surge protectors for PCs? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Are temperature, humidity and dust particles in the air in the computer room monitored? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

TABLE 4.1 (continued)

| Computer Security Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|-----|
| <ul style="list-style-type: none"> ● Are computer centers operating without personnel present, for example, late at night or weekends, equipped with sensors to monitor and report temperature, humidity, flooding, or fire to a control center or responsible official? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Is access to sensitive computer installations restricted by key locks, combination or cipher locks or card-access systems together with access-control policies and procedures? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. PCs and Workstations | | | | |
| <ul style="list-style-type: none"> ● Are PCs and workstations in areas where theft is a threat secured by cables, locks, or other antitheft devices? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Are PCs and workstations secured by cables, locks, or other antitheft devices? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Are PCs and workstations secured with screen-saver programs requiring passwords to unlock? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Are computer users prohibited by written policy from installing unauthorized software including encryption software on company PCs and notebook computers? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● Is there a procedure for regularly examining company-provided PCs for unauthorized software? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 2. Communications Security | | | | |
| a. Is a user ID and password or stronger system with one-time passwords or biometric security in place? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. Are the distribution of new IDs regulated and those of terminated users promptly deleted? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Do controls prohibit multiple persons from sharing a single account or log-in code? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Are passwords secured by requirements for adequate length and use of numeric and special characters? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Are there written policies requiring employees to sign computer-use and confidentiality agreements, to maintain password secrecy and forbidding the use of simplistic or easily guessed passwords? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Are passwords changed regularly at intervals no greater than 90 days? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. Does the system monitor and control use by restricting users to specific terminals or times, automatically logging out inactive users, limiting the number of log-on attempts, and recording all use for later follow-up and investigation if required? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

(continued)

TABLE 4.1 (continued)

| Computer Security Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| h. Is remote access controlled by callback, biometric, or one-time password devices? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| i. Is anyone responsible for security and required to check Internet sources and vendors for information on fraud prevention? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Data Security | | | | |
| a. Is access to on-line data limited to authorized individuals through built-in software restrictions or screening? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Has encryption been considered for the transmission of sensitive data? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Are backup files stored on magnetic or optical media and kept in a physically secure place away from the computers and accessible only by authorized persons? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Are backup files stored in a fire-rated safe? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Are printed records retained on- and offsite and destroyed according to statutory requirements and recognized records management schedules? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 4. Software Integrity | | | | |
| a. Is access to production versions of all software tightly controlled by a production librarian or similar authorized person? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Does the alteration of tested and approved software programming code require documented authorization? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Is the installation of any anti-virus software authorized and screened? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Is anti-virus software installed on every computer and updated continuously through a contract with the software provider? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Are there adequate controls to prevent the installation of pirated software? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 5. Operations Security | | | | |
| a. Are detailed operating manuals available? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Is computer activity logged and any unusual use investigated? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Are computer-operations personnel prohibited from altering program code and Job Control Language that match the program and data files? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Are all software and data storage media clearly and correctly labeled and dated? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Are data files reconciled from run to run? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

TABLE 4.1 (continued)

| Computer Security Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|-----|
| f. Are all data storage media electronically wiped clean by a suitably designed wiping program before disposal? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 6. System Recovery | | | | |
| a. Are backup copies of all transactions files made daily, and data files and software made at least weekly? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Do guidelines ensure all employee work is saved to the network server? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Is at least one backup copy of all data files and software stored off site? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Have employees been provided with written instructions and training in disaster recovery procedures? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. In the case of catastrophic failure, do alternative processing arrangements exist? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. Have the backup plans been tested in a realistic simulation? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| g. Is there adequate insurance to cover computer equipment, software, recovery expenses, and business interruption? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| h. Is there a written agreement in place to provide recovery services? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| i. Are all PC hard drives backed up on a regular basis? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| j. Does the company have a written arrangement with a data recovery vendor to retrieve data from a hard drive, tape or other storage device, which has become unreadable, and for which no backup exists? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

CHAPTER 5:

Internal Fraud

| | | |
|-------|--|----|
| 5.1 | Asset Misappropriation from Within | 3 |
| 5.1.1 | Classification of Fraud | 3 |
| 5.1.2 | Cycles | 3 |
| 5.2 | Sales and Collection Cycle..... | 4 |
| 5.2.1 | Functions..... | 4 |
| 5.2.2 | Financial Statement Accounts..... | 4 |
| 5.2.3 | Perpetration | 4 |
| 5.2.4 | Detection..... | 5 |
| 5.2.5 | Prevention..... | 6 |
| 5.2.6 | Sales, Receivables and Receipts System..... | 8 |
| 5.3 | Acquisition and Payment Cycle..... | 14 |
| 5.3.1 | Functions..... | 14 |
| 5.3.2 | Financial Statement Accounts..... | 14 |
| 5.3.3 | Perpetration | 15 |
| 5.3.4 | Detection..... | 16 |
| 5.3.5 | Prevention—Key Controls | 17 |
| 5.3.6 | Prevention—Policies | 17 |
| 5.3.7 | Purchasing, Payables and Collection Systems..... | 19 |
| 5.4 | Payroll and Personnel Cycle | 25 |
| 5.4.1 | Functions..... | 25 |
| 5.4.2 | Financial Statement Accounts..... | 25 |
| 5.4.3 | Perpetration | 25 |
| 5.4.4 | Detection..... | 26 |
| 5.4.5 | Prevention..... | 27 |



- 5.5 Inventory and Warehousing Cycle27
 - 5.5.1 Functions28
 - 5.5.2 Financial Statement Accounts.....28
 - 5.5.3 Perpetration28
 - 5.5.4 Detection.....28
 - 5.5.5 Prevention.....29
- 5.6 Capital Acquisition and Repayment Cycle29
 - 5.6.1 Functions29
 - 5.6.2 Financial Statement Accounts.....30
 - 5.6.3 Perpetration30
 - 5.6.4 Detection.....30
 - 5.6.5 Prevention.....31
- 5.7 Cash Misappropriation.....31
 - 5.7.1 Perpetration31
 - 5.7.2 Detection and Prevention.....32

CHAPTER 5:

Internal Fraud

5.1 ASSET MISAPPROPRIATION FROM WITHIN

As difficult as it is to believe, many experts are convinced that the worst threat to business is from the people who work there. Fraud committed against an organization by a perpetrator from within that organization is probably the most common form of fraud. Certainly it is the most widely recognized.

It is estimated that at least one-third of all employees steal to some degree. In retail organizations, shoplifters are responsible for only thirty percent of retail losses; employees steal the remainder. Probably the worst case of insider misappropriation is the infamous U.S. Savings and Loan scandal; the billions of dollars stolen by *trusted* insiders has no equal in history.

5.1.1 Classification of Fraud

Regardless of the industry, you can classify internal fraud in several different ways. One way is by the method of concealment, including on-book and off-book frauds.

On-Book Fraud

On-book fraud principally occurs within a business when an employee creates an audit trail (which is sometimes obscure) that inadvertently aids the employer in detection. Examples include phony vendors and ghost employees. On-book fraud is normally detected at the point of payment.

Off-Book Fraud

Off-book fraud occurs outside the accounting environment where no audit trail is likely to exist. Examples include bribery and kickbacks. If an employee receives a bribe for selecting a certain vendor, that payment would be made by the vendor and, therefore, would not be reflected on the books of the affected company. These frauds are detected in an indirect manner (that is, responding to other vendor complaints, investigating the life-style of the person receiving the bribes, and so on). If you suspect that an employee is receiving illicit payments, examining the employee's personal finances should prove this.

5.1.2 Cycles

You can classify fraud occurring within the business environment by one of the five cycles in the accounting system. These cycles are:

1. Sales and collection
2. Acquisition and payment

3. Payroll and personnel
4. Inventory and warehousing
5. Capital acquisition and repayment

All of these cycles flow through the cash account. Accordingly, cash misappropriation is discussed separately in this chapter. The following sections discuss the more common frauds occurring within each cycle.

5.2 SALES AND COLLECTION CYCLE

The sales and collection cycle deals with the billing of goods or services to customers' accounts receivable and the collection of funds relating to those receivables.

5.2.1 Functions

The functions of the sales and collection cycle include:

- Receiving orders from customers
- Administering credit approvals
- Invoicing customers
- Collecting receivables
- Adjusting sales and receivables for allowances, returns and write-offs

5.2.2 Financial Statement Accounts

Sales revenue on the income statement and accounts receivable and cash on the balance sheet are affected by the sales and collection cycle. See Chapter 10 for further information on reducing the risk of financial statement fraud.

5.2.3 Perpetration

Frauds in the sales and collection cycle most commonly involve the theft of cash, the theft of other assets, and kickbacks to customers. It can also involve off-book fraud in a situation described as front-end fraud, that is, when an employee diverts company revenue before entering it on the books.

Theft of Cash

By far, the most common sales-cycle fraud is the theft of cash. The main schemes include: not recording sales, under-ringing sales, lapping, theft of funds from voids and returns, overbilling and keeping the difference, simple theft of cash, writing off receivables as uncollectible, and issuing bogus credit memoranda.

For example, in one lapping fraud, a cashier was able to misappropriate cash receipts totaling over \$35,000 and cover the shortage by subsequent receipts. The prelisted receipts were not compared to the deposits by an independent person, allowing the fraud to go undetected over time. This scheme was eventually discovered as a result of a CPA following up on the clearing of deposits in transit listed on the year-end bank reconciliation.

Theft of Other Assets

These schemes include ordering and shipping company goods to the residence of the employee, and ordering goods for personal use.

Kickbacks to Customers

The most common schemes for kickbacks to customers include underbilling for merchandise and splitting the difference, and writing off receivables owed to the company for a fee.

Front-End Fraud

A front-end fraud occurs when a company's customers are improperly directed to take their business elsewhere, thereby depriving the company of profits it could otherwise have made. Another example is the receipt of a purchase rebate that is misappropriated and not deposited to the company's bank account.

5.2.4 Detection

Generally, CPAs can best detect frauds in the sales and collection cycle by analyzing cash or inventory, or both.

Theft of Cash and Front-End Fraud

Following are some methods for detecting the theft of cash and front-end fraud:

- Investigate customer complaints.
- Insist that customers examine receipts.
- Use statistical sampling of sales invoices.
- Compare receipts with deposits.
- Follow up on deposits in transit at the end of each period.
- Account for consecutive sales orders and cash register transactions.
- Compare volume of credit memos by period.
- Verify independently customers who don't pay.
- Examine gross margin by product.
- Use a computer to—
 - Identify missing invoices by number.
 - Match shipping documents, sales invoices and customer orders.
 - Verify numerical sequence of documents.
 - Analyze sales volume by employee.
 - Match daily deposits with customer credits.

For example, in one fraud case, a CPA for a retail client noted a skip in the perpetual transaction count for one of the cash registers. During a one-year period an employee had destroyed sections of cash register tapes totaling \$17,000. The irregularity was directly related to the company's failure to institute and maintain adequate internal controls and procedures over cash register tapes.

Theft of Other Assets

You can detect theft of other assets by using the following methods:

- Resolve customer disputes.
- Conduct periodic surprise inventory counts.
- Use statistical sampling of sales invoices, including examining the shipping address.
- Use a computer to—
 - Match sales invoices with customer orders.
 - Compare customer names and addresses with employee names and addresses.
 - Verify delivery addresses against addresses of customers.

Kickbacks to Customers

You can use one or a combination of the following to detect the common schemes in kickbacks to customers:

- Follow up on customer disputes.
- Conduct statistical sampling of sales invoices by contacting customers regarding prices and terms.
- Conduct computer analysis of—
 - Prices charged by product to customer.
 - Credit granting approval versus actual sales to customers.
 - Customer balances versus sales.
 - Customer balances versus length of time doing business with the customer.
 - Receivable write-offs.
 - Credit memos to customers.
 - Time between order and delivery.
 - Discounts to customers in descending volume of purchase.

5.2.5 Prevention

Employers can generally prevent sales and collection frauds by using adequate internal controls. More specifically, the following methods typically form part of an overall prevention strategy:

- Honesty testing
- Separation of duties
- Physical safeguards over assets
- Proper documentation
- Proper approvals
- Independent checks on performance

Honesty Testing

The legality of using certain kinds of honesty testing as part of the hiring process varies from jurisdiction to jurisdiction. For example, since the advent of the U.S. Polygraph Protection Act of 1988, generally it has been unlawful to require preemployment polygraphs of prospective employees. A number of companies have turned to pencil and paper honesty tests, which their designers tout as accurate.

Separation of Duties

Employers can prevent most frauds by properly segregating the custody, authorization, and record-keeping functions. In the case of sales and collections, it is important to separate the functions of credit granting and sales. In addition, the functions of sales, record keeping, and cash handling should also be separate.

Physical Safeguards over Assets

If assets and records have physical safeguards, misappropriation is much more difficult. In the area of computers, physical safeguards such as restricted access, locks, and similar controls are especially important.

Proper Documentation

Proper documentation requires adequate records, including prenumbered checks and invoices, to make fictitious entries more difficult. Documentation in sales and collections should include the following prenumbered documents:

- Sales orders
- Shipping documents
- Sales invoices
- Credit memos
- Remittance advices

Proper Approvals

Approval should be sought and evidenced before each of the following:

1. Granting credit
2. Allowing write-offs
3. Shipping goods

Independent Checks on Performance

In addition to a necessary independent review of employee adherence to internal controls, you should make the potential perpetrators aware that their performance is being monitored. Independent verification steps include reconciling bank accounts, audits and supervision.

5.2.6 Sales, Receivables and Receipts System

The sales, receivables and receipts system is the part of the accounting system that records a company's sales and revenue collections. Individuals can use false books and supporting documentation for sales, receivables and receipts to perpetrate a fraud on a company. This section covers three such methods:

1. Front-end fraud
2. False sales invoices
3. Lapping

Front-End Fraud

As discussed in section 5.2.3, employees may divert company revenues before that money ever reaches the sales, receivables and receipts system, thus circumventing the accounting system entirely. This is commonly called front-end fraud.

A front-end fraud occurs when company products are sold for cash, the sale and the receipt of the cash are not recorded, and the cash is diverted—usually, directly into the pocket of the perpetrator. A front-end fraud also occurs when a company's customers are improperly directed to take their business elsewhere, thus depriving the company of profits. Finally, a front-end fraud occurs when an employee receives and misappropriates special or unusual revenues and cost reductions, such as a purchase rebate.

The questions to address when investigating this kind of fraud are:

1. Do recorded sales represent all company sales? Where no sale has been recorded, there is nothing in the sales accounting system to *red-flag* an unpaid or overdue account. As a result, unrecorded sales are difficult to detect; however, actual inventory on hand has been depleted. Therefore, if the company has a good inventory accounting system, unrecorded sales may be detected.
2. Has the company unexpectedly lost some of its oldest and best customers?
3. Are all revenues recorded? Service businesses, such as parking lots, theatres and movie houses operate primarily with cash sales and have no inventory systems. Front-end frauds in these kinds of businesses, therefore, are extremely difficult to detect.

When allowed under local law, a review of a suspected perpetrator's personal bank accounts may reveal unexplained cash deposits, which could be important in establishing circumstantial evidence of front-end cash skimming. Otherwise use of the *net worth* approach may be necessary to establish that the suspected perpetrator has benefited.

Investigators should analyze the sales records and other supporting documents of the victim company for the period both before and after the assumed *occurrence* date of a front-end fraud. When possible, the investigators should interview customers as well.

“Taxes ‘R Us” Case Study

Jane Brown and Jack Smith were cashiers who worked at a county tax office. Investigation revealed that, over a two-month period in 1997, thirteen individuals apparently paid tax for vehicle tags and did not receive an official receipt.

On a review of all the official receipts issued during this period of time it was found that:

1. The numerical continuity of the prenumbered receipts was complete; that is, all of the issued receipts were accounted for in the bureau’s records.
2. There were no receipts to support the thirteen payments made by those individuals identified as exceptions.

The county tax office’s banking records were then reviewed for the days on which people reportedly paid for their tags but did not receive a receipt. The review disclosed that the amount of cash and checks relating to the tax deposited to the county bank account totaled only the amount of receipts issued for that date.

Five of the individuals who reportedly paid for their tags, but were not issued an official receipt, paid by check. In the case of each of these five individuals, the checks were deposited to the county bank account, but the checks, upon deposit, were applied to cover actual receipts issued. With respect to those individuals who were known to have paid for their tags by check, but who did not receive an official receipt, it was noted that a like amount was included on the county tax office deposit slip.

During the same period, cash totaling \$4,600 was deposited to the known bank accounts of Jane Brown. The source of that deposited cash was not identified.

Front-end fraud of this type is very difficult to detect. Larger frauds may be uncovered if the perpetrators become too greedy because the resulting unusually low daily deposits may highlight the problem. In fact, skimming of small amounts may be detected only through customer complaints: as in the case study, by the lack of an official receipt. This illustrates the need to thoroughly investigate similar complaints and any other irregularities.

False Sales Invoices

Employees can alter a company sales invoice to show a lower sale amount than what was actually received. They can misappropriate the difference between the real sale amount and the adjusted lower amount without the accounting system showing a *red flag*.

The questions to address when investigating this kind of fraud include:

1. Are recorded sales amounts the actual sales amounts?
2. Can customers confirm the sales?
3. Are sale amounts reasonable in the circumstances?

Investigators should obtain and examine all original copies of invoices and all the related books of original entry. Again, the investigator must become familiar with the accounting system in effect and understand the accused's position within that system. Did the accused have the necessary authority to perpetrate this crime? Did the accused have the opportunity?

"Ms. Wanda Cash" Case Study

Wanda Cash was the bookkeeper for Anytown Animal Center. She looked after all customer records including preparing bills and collecting payments. The owners of the business became suspicious when daily bank deposits were not as high as expected considering the level of business. Upon investigation by the owners, the police and forensic accountants, it was discovered that Wanda Cash, through altering sales invoices, had misappropriated approximately \$11,700.

The investigation revealed that:

1. The 183 customer copies of sales invoices showed a total-charge amount higher than the total-charge amount recorded in the cash receipts journal. The customer copy of sales invoices indicated total charges to be higher by \$2,579 than the amount recorded in the cash receipts journal.
2. The 549 office copies of the sales invoices indicated a total-charge amount higher than the total-charge amount recorded in the cash-receipts journal. The office copy total-charge amount was higher by \$8,941 than the amount recorded in the cash-receipts journal.
3. Approximately 68 office-copy invoices were apparently altered so that the total charge after alteration balanced with the total charge recorded in the cash-receipts journal.

To uncover this fraud and measure its magnitude, investigators compared the following:

- Customer copies of invoices obtained by the investigating officer
- Office or accounting copies of the company's sales invoices
- Entries in the customer ledger cards and the cash-receipts journal

The result was that the amount of the total charge on the customer copies of sales invoices exceeded the amount of the total charge recorded in the cash-receipts journal by an aggregate amount of \$2,579. An examination of these documents disclosed that in 54 separate cases the corresponding office copy of the invoice was altered so that the altered amount agreed to the total-charge amount recorded in the cash-receipts journal.

Investigators compared the office copies of the sales invoices with the total charge recorded for those invoices in the cash-receipts journal and found that the total charge amount on the office copy exceeded the total charge amount recorded in the cash receipts journal. In aggregate, the excess was \$8,941.

This case illustrates the need for close supervision in small businesses, in which adequate division of duties is difficult to achieve.

Lapping

Lapping occurs when cash receipts from Customer A are misappropriated and the misappropriation is subsequently concealed by recording the receipt of monies from Customer B to the credit of Customer A (to the extent of the earlier misappropriation).

The questions to address when investigating this kind of fraud are as follows:

1. Are the amounts recorded as owing to the company actually still owing to the company?
2. Are deposits from *Peter* being used to cover *Paul's* debts?

To handle these questions, the investigator should understand the organization's system for receiving customer payments, making bank deposits, and preparing entries to customer accounts. The following is a guide to understanding an organization's account management.

1. Who first received the payments?
2. Who prepared the company bank deposit?
3. Who updated the customer accounts?
4. Has an individual *written off* any accounts?
5. Who approved the write-offs? (It is also often necessary to contact customers and obtain their records of payments, including paid checks and remittance advices.)
6. Do the customer's records show payment of specific invoices that are shown as unpaid in the victim company's records?

"Ms. B. A. Lapper" Case Study

Jones Transport Company operated a trucking terminal in Norcross, GA. Their accounts receivable clerk, Ms. B.A. Lapper, had been a loyal employee for over eight years. The terminal manager often complimented her for the extra effort she put into the business, evidenced by the amount of work she frequently took home. This employee was so loyal that her only time off was attributable to sickness.

Ms. Lapper was responsible for preparing the day's deposit to the bank and for preparing input to the computer systems for updating payments on accounts receivable. (The processing of the sales invoice as an account receivable was outside her control.) Every month the head office in Atlanta forwarded aged listings of accounts receivable to the manager's attention at the terminal. He gave the analysis to the accounts receivable clerk—Ms. Lapper—satisfied that the aged analysis was relatively current.

Investigators determined that Ms. Lapper had conducted a lapping scheme over a period of six years. The lap grew so large during this period that she had to take the aged receivable analysis home in the evenings, along with the *paid* and *unpaid* sales invoices. There, she would set aside invoices for payment during the next day to ensure a favorable aged receivable analysis in the following month. As the lap grew,

the new cash receipts were no longer sufficient to cover the previously misappropriated funds. Accordingly, Ms. Lapper began to apply checks received from the larger customers of the company to cover up the already-paid sales invoices.

Investigators examined the known personal bank accounts of the accused and her husband. An amount of \$35,000 was found deposited to these bank accounts over and above personal income during the relevant period.

Accounts Receivable Routines: Ms. Lapper's main function each day was to balance the cash with the pro-bills (sales invoices) and prepare a cash deposit for the bank in Norcross and a cash report for processing by the head-office computer. She would process all incoming checks from charge account customers by matching checks to the applicable pro-bill control copies and preparing a deposit for the bank in Norcross and a receivable report for the head office. She would present the deposit slips and receivable reports to the manager for his signature, along with the customer's checks and cash in an envelope.

The supporting documents were always in sealed and stapled envelopes for each report. The envelopes were not opened and verified by the manager. If the total of the bank deposit agreed with the total of the receivable report, he would sign the report. One copy of the report, the bank deposit slip, and pro-bills were then forwarded to the Atlanta head office, while a second copy of the report and the remittance copies of pro-bills were retained on file at the Norcross terminal.

Ms. Lapper would work on the company's *Accounts Receivable Aged Analysis*, a listing of all outstanding pro-bills prepared at the Atlanta head office, and would appear to question certain delinquent accounts for payment. She would often take the analysis home because she said she was too busy during the day to perform this function.

The Atlanta terminal manager would look at the receivable analysis printout and tell Ms. Lapper to question certain delinquent customer accounts, which she appeared to do. She would inform the manager of checks arriving after her contacts with the customer. For instance, in regard to the Best Quality Cheese account, she informed the manager that Best Quality was having serious problems converting to a computer accounting system and as a result had requested that Jones Transport be patient with the amount of old outstanding receivables.

Jones Transport hired a new person to replace Ms. Lapper when she became seriously ill. Her replacement began the collection work on the two largest charge-account customers, Best Quality Cheese and Anyco Inc. Successful collection of these accounts would immediately reduce the analysis' sixty- and ninety-day totals, which had become very high.

Customer Best Quality: Best Quality was advised that their pro-bills dated July and August were still outstanding on the receivable analysis. Ms. Brown asked Best Quality if they were having computer problems and the response was negative. Subsequently Best Quality informed Jones Transport that the pro-bills mentioned as outstanding were all paid by checks issued in July and August.

Jones Transport then examined copies of the reports around the dates of the Best Quality checks, together with check stubs and supporting pro-bills. Although the pro-bills that were paid with the Best Quality checks were all Best Quality, all were dated April and May. Jones Transport wondered if Best Quality had made an error, because their August check, which was paying July and August pro-bills, did not appear to apply to the pro-bills in the deposit that were all dated May and June. Best Quality responded that there was no error on their part, and they could not understand how there could be a mistake because they had attached all the applicable pro-bills with their remittances.

Customer Anyco: Jones Transport then called Anyco Inc. and asked when they would be paying certain outstanding pro-bills. Anyco indicated that these bills had been paid by checks that had been issued and received as paid. When Jones Transport checked their copies of the reports, they found that Anyco checks were deposited, but that the checks were applied to older Anyco pro-bills and other customer pro-bills and not to the pro-bills submitted by Anyco with its checks.

The outstanding pro-bills totaled about \$47,000 at Best Quality and about \$12,000 at Anyco. At this point Jones Transport recognized that the customer checks were not applied to the pro-bills as intended by the customer. Instead the checks were applied either to the customer's older pro-bills or to other customers' pro-bills. Further investigation revealed that these other customers were normally cash-paying customers.

Examination of the Amount of Money Due Jones Transport: To determine the correct amount of money owing to them by all their customers, Jones Transport communicated directly with each customer, based on their accounts receivable analysis. For each customer, Jones Transport prepared from their analysis a list of pro-bills by number, date, and amount that the customers had not paid and requested verification that the information concerning the outstanding pro-bills was accurate.

A reply made by all customers indicated that several pro-bills shown in the analysis of Jones Transport were, in fact, paid and were, therefore, not outstanding. This finding confirmed the evidence of the samples and the discussion by Jones Transport with both Best Quality and Anyco, that a customer's check was applied not to his current pro-bills as intended by the customer, but rather to a combination of the customer's older pro-bills and other customer's pro-bills that had been paid in cash.

From the information provided by the customers, the investigators determined that the dollar value of the pro-bills, which had been paid by these customers, was \$115,132.

Jones Transport fell victim to a fraudulent scheme commonly called lapping. Cash and checks were received at the Hamilton terminal of Jones Transport and controlled by Ms. Lapper. The cash was removed from Jones Transport while the checks were applied to the pro-bills that were to have been paid by the cash. Consequently, the pro-bills remitted with the checks remained outstanding on the accounts-receivable analysis published at the end of each month.

As a result, the amount of the outstanding pro-bills, which Jones Transport found through direct communication with their customers to have been paid, represented that amount of the cash that had been misappropriated over the time period under investigation, that is, \$115,132.

Victims most often detect lapping frauds through accounts-receivable reconciliations or confirmations, or both. Supervision is also important. Organizations can prevent lapping by appropriately dividing duties (for example, assigning someone other than the accounts receivable clerk the duty of handling cash receipts). You should also consider establishing a policy of mandatory vacations, which could be helpful.

5.3 ACQUISITION AND PAYMENT CYCLE

The acquisition and payment cycle includes the procurement and payment of all goods and services except for payroll and capital acquisitions. This cycle is especially vulnerable to fraudulent transactions because this is the point where funds flow out of an entity.

5.3.1 Functions

The functions of the acquisition and payment cycle include:

- Processing purchase orders and dealing with vendors.
- Receiving and recording goods and services.
- Accounting for the liability of items or services purchased.
- Processing and recording cash disbursements.

5.3.2 Financial Statements Accounts

Balance Sheet

The following balance sheet accounts are affected by the acquisition and payment cycle:

- Cash
- Inventories
- Prepaid expenses
- Land
- Buildings
- Equipment
- Accumulated depreciation
- Accounts payable
- Deferred taxes
- Other payables

Income Statement

The following income statement accounts are affected by the acquisition and payment cycle:

- Cost of goods sold
- Advertising expenses
- Travel and entertainment expenses
- Miscellaneous expenses
- Income tax expenses
- Professional fees
- All expense accounts
- Gains and losses on sales of assets

5.3.3 Perpetration

By far the most common fraud in the acquisition and payment cycle involves the purchasing agent (buyer), who is especially vulnerable to the temptation of accepting kickbacks and gifts from outside vendors.

One study revealed that companies who caught employees accepting small gifts were hesitant to discharge their employees. Two percent suspended the employees, while only 12 percent fired them. Sixty-six percent reprimanded the employees and made them return the gifts.

There are three general kinds of acquisition and payment-cycle frauds:

1. The buyer-employee acts alone, and without outside assistance.
2. The vendor acts alone.
3. The buyer acts in collusion with the vendor. As is the case with other methods of prevention and detection, the collusion between both parties is the most difficult to prevent and detect.

Buyer Acting Alone

Noncollusive purchasing frauds usually involve the use of a nominee entity, commonly called a shell company, that is, an apparent third party owned by the buyer. Examples include the use of a nominee entity to submit fictitious invoices (the most common fraud), or to order goods for personal use.

Shell company schemes can be quite sophisticated using bank accounts, corporate filings, and mail drops to assist in the fraud. One common shell company failing is using a post office box rather than a street address. The post office box address has come to be recognized as a red flag.

In one case, a 61-year-old employee of a major department store was indicted for allegedly stealing \$2 million from the company. His responsibilities included leasing buildings to house the retailer's stores. On twenty-two leases over a two-year period, through a nominee company, he altered leases to receive overpayments, and forged invoices billing the company for fictitious legal and building services.

In another example, an executive was indicted for defrauding a large cosmetics company of \$1.1 million over four years. During this period, he allegedly approved more than 150 vendor invoices for services that were never rendered in connection with a newsletter the company was going to publish. The executive (whose salary was \$124,000 per year) helped set up two nominee printing companies, which bilked his employer with the fraudulent invoices.

Finally, a director of customer-service technology was able to defraud his employer of over \$2 million in one year by taking advantage of defects in internal control. The fraudster set up a legitimate agreement with a legitimate vendor to provide certain equipment. Then he set up a fake distributorship and told the vendor the company would purchase only from this one distributor. The vendor was content to have the business and proceeded to invoice the distributor. The fraudster, through his nominee distributorship, then inflated the invoices and billed them to his employer. The fraud was possible because the employee had the authority to set up the agreement, and to approve invoices for payment. The fraud was discovered by a manager who thought it was strange that the employee was delivering the invoices to accounts payable by hand.

Buyer and Vendor in Collusion

Nearly all collusion between buyer and vendor involves some form of secret commission or kickback from the vendor to the buyer. In these cases, secret benefits are given by a vendor in order to *buy* business, or are requested by the buyer for direct financial benefit. Collusion fraud often involves more than one kind of scheme perpetrated over time. Of course, there is always the question of who took the initiative, that is, the buyer or the vendor.

For example, one case started out involving inferior goods and later graduated to inflated invoices. A county purchasing agent was responsible for acquiring a long list of janitorial supplies, including mops, pails, soap, plywood, rakes, and paper goods. Area paper jobbers—experienced connivers—approached the purchasing agent with a deal. “Without changing our invoice price,” they told him, “if you agree, we can deliver a cheaper brand of paper towels. Half the extra is for us; the other half is for you.” Once the purchasing agent accepted a lesser brand, the vendor began squeezing for more by raising the price on the invoice and billing for five times the amount of merchandise actually shipped.

Monetary payments are not the only benefit that can be offered. Other common ways of corrupting a buyer include products or services; gifts, trips, or sex; promises of subsequent employment; reduced prices for personal items; and employment of friends or relatives.

Vendor Acting Alone

Common schemes used by vendors include product substitutions, billing for work not performed or services not provided, undershipping, padding overhead charges, and courtesy billings.

5.3.4 Detection

Because of the difficulty of detection, fraud awareness and prevention is the best policy, that is, know your vendors, and have an effective tendering process for all contracts. Fraud in procurement contracts always poses special problems, and detection is difficult. Common red flags include sole source contracts, unhappy purchasing agents, significant price changes or changed orders (especially after a contract is awarded), and vendor complaints.

In one case detected through vendor complaints, a buyer with six years' seniority obtained purchase requisitions from various departments at his plant. He then created a nominee company and placed orders with this firm. The nominee company would place real orders with a legitimate vendor and have them ship the merchandise to his employer. The merchandise would be billed through the buyer's company at 150 percent of the real amount. The scheme was unraveled when the buyer failed to pay one of the vendors, who then complained to the buyer's employer.

Sometimes you can also detect schemes through a computer analysis of the following:

- Timing of bids
- Patterns of bids
- Amount of work performed by vendors
- Patterns of hiring new vendors
- Vendors with post-office-box addresses

In an example involving post-office-box addresses, a junior buyer, who had been with his company for two years, created five nominee companies that he then placed on an approved vendor list. Thereafter, he did business with these phony companies, placing various orders with them. The scheme was unraveled when the auditors noticed that these particular vendors all had post-office boxes for addresses and were not listed in the telephone book. The amount of money lost was in excess of \$250,000 over a period of more than a year.

If you suspect that a buyer and vendor are in collusion, consider the following items:

- Assessment of the tender process, if any
- Patterns of business and bids
- Noncompetitive pricing
- Products of inferior quality
- Buying unnecessary goods or services
- Lack of competitive bidding

5.3.5 Prevention—Key Controls

As previously noted, prevention of procurement fraud can be achieved best through fraud awareness, effective tendering and budgeting, and knowledge of your vendors. Other prevention controls include proper documentation, approvals, and segregation of duties.

Proper documentation includes prenumbered purchase requisitions, purchase orders, receiving reports, and checks. Proper approvals should include detailed background information on the vendor; ideally, purchase contracts should include a right-of-audit-access clause to the vendor's books. In addition, conduct both irregularly scheduled audits of the purchasing function as well as assessments of the performance and happiness of the purchasing agent.

5.3.6 Prevention—Policies

Organizations should have established prevention and detection policies. The following are some policies to consider implementing.

Accepting Gifts

The following is a sample policy statement covering the acceptance of gifts and gratuities:

“Employees, and members of their immediate families, should not accept gifts, favors or entertainment that might create or appear to create a favored position for someone doing business with the company. Advertising novelties or trinkets are not considered as gifts and are excluded from these restrictions.

Gifts that are received by an employee should be returned to the donor and may be accompanied with a copy of this policy. Perishable gifts should be donated to a charitable organization and the donor notified of the action taken.

It is not the intent of this policy to preclude the acceptance by the company's employees of occasional meals or refreshments that are provided in the normal course of business-work relationships, with other individuals. Discretion must be used, however, in the limited acceptance of meals, refreshments or incidental hospitality to avoid situations that could create a conflict of interest or appear to do so.”

Providing Gifts

The following is a sample policy statement covering the giving of gifts:

“Occasionally, it may be appropriate for employees, acting for the company, to provide people outside the company with promotional items, meals, refreshments, transportation, lodgings or incidental hospitality. Expenditures for such purposes should be moderate and should be done only within the framework of good taste. All expenditures are subject to the overall company policy that an employee shall avoid constituting improper influence over others.”

Use of Hotlines

You should study the feasibility of installing hotlines to monitor complaints by employees and other vendors. Make sure the hotline staff is not associated with either the purchasing or payment functions. Failure to take this precaution could result in the fraudster receiving the whistle blower's call.

Disposition of Materials

The purchasing department normally should not be in charge of disposing of obsolete inventory, scrap, or fixed assets.

Rotation of Jobs

Rotate buyers frequently within a department to keep them from getting too close to vendors. In addition, enforce a mandatory vacation policy.

Competition in Bidding

Ensure that bidding policies and procedures are thoroughly reviewed. Whenever possible, enforce competitive bidding.

Compensation of Buyers

Buyers should be well paid to reduce the motives and rationalizations for fraud.

5.3.7 Purchasing, Payables and Collection Systems

The purchasing, payables, and collection systems are part of the accounting systems that record a company's purchases and expense payments. Employees can falsify books and supporting documentation for purchases, payables and collections to perpetrate a fraud on their employing company. This section covers three categories of perpetrating fraud:

1. False expense reports
2. False supplier invoices
3. Other false information

False Expense Reports

Expense reports prepared and submitted to the company for payment are false if they include any of the following:

- Overstated items
- Fictitious items
- Duplicate items

An employee could use a company credit card for personal items. If the company pays the entire amount of an employee's account, that employee may be committing a fraud. Ultimately, the answer depends on the first accountability for the disbursements.

Address the following questions when investigating this kind of fraud:

1. Is the expense item an allowable business-related expense? It is necessary to determine the company's policy regarding allowable business expenses.
2. Is the expense amount the actual amount incurred? It is necessary to obtain the suppliers' copies of the original expense vouchers and compare them with those submitted in support of the expense report.
3. Is the expense ultimately charged directly to the business? If yes, is there evidence of any reimbursement?

It is also necessary to understand the approval and payment system in effect. Who approved the expense reports? How were the expense reports categorized in the accounting records? Were the expense reports adjusted at a later date to reflect those items of a personal nature? Was there any pattern in the submission, approval or recording (or any combination thereof) of the fraudulent expense reports?

“Manny Miles” Case Study

Manny Miles had been the Business Administrator and Secretary-Treasurer for The County Hospital since shortly after it was formed in 1983. In addition to overseeing the administration of the hospital and its 145 employees, Miles' duties included preparing budgets. He had check-signing authority and payment approval for the hospital's annual budget of about \$5 million.

The governing body of the hospital consisted of a board comprised of twelve members; eight were elected and four were appointed as representatives of the county. In 1993, the board members hired Dr. Jane Wilson as Medical Officer. Almost immediately Miles and Wilson developed a severe personality conflict; accusations and negative feedback caused a division between the personnel of the hospital and members of the board. Attempts to terminate Dr. Wilson's services failed due to the intervention of the hospital board members on her behalf. The hospital conducted studies to improve conditions but never implemented any recommendations.

In mid-1996, during its audit, the auditors found irregularities in travel claims submitted by Manny Miles, and the hospital referred the matter to the police for investigation. In December 1996, and January 1997, the police executed search warrants not only on the hospital but also on the residence of Manny Miles. They seized the hospital's financial records along with Miles' personal banking records.

Examination of the records revealed that from 1993 to 1996, Miles had continually made claims for travel expenses while using a hospital car. Additionally, he claimed mileage from both the hospital and the county for the same trips. Furthermore Miles had used his hospital credit card to repair his own vehicle and purchase numerous personal items, including restaurant meals on weekends, when he was not working. The card was in Miles' name but the hospital paid the bills.

As business administrator, Miles could approve his own expenditures and authorize the checks. To conceal his spending, Miles had authorized the listing of these expenditures in the hospital's financial records under other categories. Invoices were missing for some checks issued and for credit-card expenditures. The financial records of the hospital did not show any reimbursement by Miles to cover the vast majority of his personal purchases, although on several occasions he had made restitution for small purchases on the hospital card.

The Manny Miles case shows that independent approval and division of duties is essential in the payment of all travel claims and other expenses. Employees should not be able to approve their own expense reports. In addition, check signers should not be the same people approving expense reports.

False Supplier Invoices

Suppliers' invoices prepared and submitted for payment to the company are false if either:

1. No goods have been delivered or services rendered
2. The quantity or value (or both) of the goods are inflated

The delivery of goods or services to a location other than a business location (for the use and benefit of the perpetrator) is a common technique, as is the payment to a *friendly* supplier when no goods or services were actually provided. Payments of inflated amounts to suppliers often reflect the existence of secret commissions.

Address the following questions when investigating this kind of fraud:

1. Were goods and services actually provided? Find out, first, whether the supplier company actually exists and next, whether any goods or services were in fact provided. If they were provided, determine to whom.
2. Did the company receive the benefit? It is often necessary to obtain the bills of lading, that is, the freight companies' proof-of-delivery slip, to confirm where the goods and services were delivered.
3. What was the approval and payment system? As with false expense reports, you should understand the approval and payment system.

“Credit To You Inc.” Case Study

In January 1993, Jones and Smith signed an agreement to start Smith Construction, a business that primarily consisted of erecting service stations. It was agreed that Smith would provide the financing while, for a salary of \$600 per week plus expenses, Jones would manage and operate the business. Smith and Jones were to share equally any profits from the business. The business progressed well and showed a profit for the first three years.

Smith did not take an active part in the construction business, as he continued to operate his own plastering company. Smith Construction operated as a division of Smith Plastering Corp. Smith initially invested \$42,000 as capital to start the construction business, and as sole signing officer, would attend the Smith Construction office regularly to sign checks, some of which were blank when signed.

Jones tendered and obtained contracts, hired subcontractors, hired and fired employees and purchased the goods necessary to operate the business, without interference from Smith. Jones could also purchase material he required for himself through the construction business and charge these amounts to himself on the business books as a form of salary.

Smith was aware that over the years Jones had erected a barn on his farm, renovated other buildings including his residence, and continued to operate the farm. Jones informed Smith that he had obtained a grant from the government of \$300,000 to finance these endeavors.

In 1998, Smith Construction had difficulty paying its suppliers (creditors) and was eventually forced into bankruptcy by creditors in June 1998. The company's debts exceeded \$300,000. Jones gave no explanation for the shortage of funds except to say that he had miscalculated the actual cost of various construction jobs. An examination of Smith Construction's books, canceled checks and available supporting documentation revealed that Jones had defrauded Smith Construction of \$861,000 by various means.

As general manager, Jones was responsible for the day-to-day operations and in this capacity, he was afforded a degree of trust. At the same time, Smith, the absentee owner, retained signing authority over all checks and, thus, thought he had control over all policy decisions.

In his private life as a farmer, Jones incurred debts with suppliers who also dealt with him as general manager of Smith Construction. Jones personally owed one of these suppliers, Credit To You Inc., more than \$25,000. In June 1997, Jones purchased a \$12.30 item, documented by the supplier invoice made out in pencil. Later, the penciled information on this invoice was erased. Information was typed onto the invoice, indicating instead that the company, Smith Construction, had purchased \$9,500 worth of material for a job then in progress. On the strength of this typed document, Smith signed a check for \$9,500 to the supplier, believing, of course, that the disbursement was for the benefit of Smith Construction. When the supplier received the check, on Jones' instructions, he credited Jones' personal account, reducing the debt to \$15,500. This altered document was the prelude to a fraud of more than \$861,000.

The alteration of documents (erasures, stricken information, or both) is at times the only indication of a fraud as it can disclose a change of mind (intent) by the person making the entry. Such alterations frequently occur in the earlier stages of a fraud as the perpetrator has yet to perfect the scheme.

Acme Products Inc. invoiced Smith Construction for the sale of roof trusses, with delivery scheduled for a gas station being built by Smith Construction. However, a description of the route to Jones' farm appeared on the back of the invoice. The building of Jones' barn required roof trusses. A review of the bill of lading confirmed the redirection.

Investigators can also review delivery instructions as another technique for identifying fraudulent transactions.

Other False Information

A business receives vast amounts of information, and subject to the existing systems of internal control, relies on it in making decisions, initiating, executing and recording transactions. If this information is false, a business can be deceived, resulting in deprivation of some sort and hence the company is put at economic risk.

Examples of false information that businesses may rely on include:

- False financial statements (See Chapter 10 for further information on financial statement fraud.)
- Overstated accounts receivable listings
- Overstated statements of income and net worth
- False general journal entries
- Altered internal company records
- Fictitious customer credit information
- False asset valuations

Address the following questions when investigating this kind of fraud:

1. Is the summary information presented (accounts receivable listings, financial statements) consistent with the underlying books and records, and are the real assets on hand? It is necessary to determine the representation made by the person or entity under investigation and the understanding reached between that person or entity and the victim. Once accomplished, you can examine the books and records supporting the summary financial information in question from the appropriate perspective.
2. Have the correct authorities properly approved entries in the general ledger? Are the entries appropriate and consistent with the facts?
3. Can customers confirm transactions?

To address the second and third questions above, you should understand the accounting systems in effect. Also, you should contact third parties to review and discuss with them their books and records, and then compare that information to the victim's information.

“Ms. I. O. Much” Case Study

Ms. I.O. Much was the office manager of Anyco Inc. from May 1995 to May 1998. As office manager, Ms. Much, together with the general manager and president of the company, had check-signing authority for the company payroll account.

While Ms. Much was office manager, the company's auditors frequently had difficulty completing their audit work primarily because of the poorly maintained books and records. Finally, Ms. Much was replaced with a new office manager, who found irregularities in the company's bank reconciliations. After the company, police, and forensic accountants completed an investigation, they determined that I.O. Much received unauthorized payments from the company totaling at least \$11,195. These payments were covered up in a variety of ways.

After examining banking records for the payroll account of Anyco Inc., investigators noted all checks payable to the order of I.O. Much. They found that eight checks totaling \$9,126 were paid to I.O. Much but were not recorded in the payroll journal.

June 15, 1997: A check dated June 15, 1997, in the amount of \$2,500 was paid to I.O. Much but not recorded. Attached to the December bank statement was a note dated June 15, 1997, which stated, “This is to certify that I.O. Much received a loan of \$2,500 from Anyco Limited to be repaid before the end of the year.” The bottom of the note had a legend stating “paid Dec. 28/97.” It appeared that no record had been made of this apparent loan transaction until December 1997.

A review of relevant accounting records disclosed that on December 28, 1997, a deposit of \$2,500 was made to the Anyco general bank account. The deposit slip for this \$2,500 showed that the deposit consisted of three checks, as follows: \$350, \$178, and \$1,971. The sources of the three checks noted on the deposit slip appeared to be as follows:

1. William Smith—\$350: A check was issued to Anyco on the account of William Smith, dated September 8, 1997. The current office manager at Anyco stated that this check was a repayment to Anyco as a result of an over-advance of funds to Smith, an Anyco employee.
2. Anybank—\$178: A check was issued from Anybank to Anyco Limited.
3. Bank draft—\$1,971: The check was a bank draft purchased from Otherbank. When this deposit was recorded in Anyco's records, someone apparently recorded it as a reduction of the company loan to I.O. Much. This loan was reflected in the books as having been advanced and repaid in the same month, that is, December 1997.

March 1, 1998: A check dated March 1, 1998, in the amount of \$2,500 was paid to I.O. Much but not recorded in the payroll journal. It appeared that a journal entry was prepared to record this check. This journal entry suggested that the \$2,500 was paid with respect to five different accounts as follows:

1. Account #99-6, salespeople's salaries, Boston
2. Account #99-2, salespeople's salaries, Dallas
3. Account #99-7, salespeople's salaries, Washington, D.C.
4. Account #199-12, delivery salaries, New York
5. Account #99-8, salespeople's salaries, Seattle

The journal indicated that this entry was "to record checks cashed but not recorded or deposited." The only check apparently not recorded in March 1997 was check #2000 for \$2,500 payable to I.O. Much.

It is significant that the checks paid to I.O. Much in 1997 and 1998, which were not noted in the payroll journal, were not available in the corporate records. Investigators obtained copies of these checks from the microfilm files at Anybank.

A review of the payroll records indicated two apparent discrepancies related to I.O. Much. The April 7, 1997, payroll records indicated "income tax withheld" of \$200 more than apparently had been withheld from I.O. Much's pay. Similarly on August 11, 1997, payroll records indicated \$1,000 more income tax withheld than apparently had been withheld to date. In that time period an offsetting adjustment was made to the net pay figure, thereby indicating that the net amount of money paid to I.O. Much was \$1,000 less than apparently had been paid to her at that time.

The effect of these adjustments was an apparent benefit to I.O. Much of \$1,200. Her W2 for the year ended December 31, 1997, indicated that she paid \$1,200 more income tax than she had actually paid. The Anyco Limited employee deduction account was not reconciled at the time of the investigation, and thus it was not readily apparent how the \$1,200 tax benefit was accounted for in the company's books.

While the amounts involved were not terribly large, this case points out a number of internal control weaknesses that can result in fraud, including lack of supervision, inadequate division of duties, and failure to perform appropriate accounting reconciliations.

5.4 PAYROLL AND PERSONNEL CYCLE

The payroll and personnel cycle handles the hiring, firing, and payment of employees, along with timekeeping, expense-account and travel reimbursements, and insurance matters.

The hiring function can play an important role in reducing the risk of potential fraud through the careful vetting of employment applications. Adding an employee whose resumé is not truthful is opening the business's door to a potential fraudster.

5.4.1 Functions

The functions of the payroll and personnel cycle are as follows:

1. Personnel and employment
2. Preparation of timekeeping and payroll
3. Payment of payroll
4. Payment of payroll taxes and other withholdings
5. Reimbursements of expense accounts and travel expenses
6. Processing and payment of employee insurance, pension withholdings, and other employee benefits

5.4.2 Financial Statement Accounts

Balance Sheet

The following balance sheet accounts are affected by the payroll and personnel cycle (see Chapter 10 for further information on financial statement fraud):

1. Cash
2. Salaries payable
3. Payroll taxes payable
4. Other withholdings payable

Income Statement

The following income statement accounts are affected by the payroll and personnel cycle:

1. Travel and entertainment expenses
2. Salary and commissions expenses
3. Payroll tax expenses
4. Medical and insurance expenses

5.4.3 Perpetration

Payroll is particularly ripe for internal fraud. Common schemes include nonexistent or ghost employees, fictitious hours and overtime abuses, overstating expense accounts, and fictitious or overstated medical claims.

In one case, approximately one month after the payroll check date, Mr. Smith attempted to pick up his check from Ms. Doe, who was responsible for all departmental check distributions. Ms. Doe stated that the check was lost and that she would process the paper work necessary to obtain a new check. She then entered false payroll data in order to generate the check. Within a few weeks, Mr. Smith received a new check. However, upon reviewing his year-to-date earnings, he discovered that the lost check amount was included in his earned income. When confronted with the situation, Ms. Doe admitted to her supervisor that she had forged Mr. Smith's name and cashed the check for personal reasons. Ms. Doe, who had been with the company for seven years, had her employment terminated.

Expense accounts are easily and frequently abused. For example, the president of a subsidiary submitted requests for business travel and entertainment advances with the parent company. The chief accountant issued the checks for the requested advances. After one-and-a-half years, the president had not repaid the advances. When pressed, he could not support the advances with proper business receipts. He confessed that he had none. The president who had ten years of service, had his employment terminated. The amount involved was \$120,000.

5.4.4 Detection

Organizations typically discover ghost employees when payroll checks are hand-delivered, and extra checks are left. For businesses employing vigorous payroll fraud detection procedures, investigators can perform significant computer and statistical analysis. For example, time card approvals, which are the same as signatures and endorsements on checks, can provide items for further investigation. Computer-generated detection methods could indicate:

- Payments to employees not on the master lists
- Payments to employees versus those not authorized for payment
- Write-offs of employee accounts
- Duplicate payments to employees
- Overtime by employee
- Password use during vacation
- Social security numbers listed in descending or ascending order
- Employees with no withholding
- Each kind of withholding in descending order
- Salary expenses in descending order
- Hours worked in descending order
- Time-card hours versus authorized job orders
- Hours worked by employee by pay period
- Pay rates in descending order
- Dates of employment versus authorized dates of payment
- Travel reimbursement by employee overtime
- Travel reimbursement compared to other employees

- Travel reimbursement for specific function by employee
- Travel reimbursements by kind of expense, that is, rental car, hotel, airfare, and so on
- Date of travel reimbursements compared to dates employee worked
- Numerical sequence of employee travel reimbursements

5.4.5 Prevention

Proper Documentation

Proper documentation for payroll purposes includes time cards for appropriate employees, prenumbered travel reimbursement forms and payroll checks, and verification of medical services.

Proper Approval

Proper approval includes hours worked and wage rates, hiring and terminations, overtime, medical benefits, and travel allowances.

Separation of Duties

At a minimum, you should consider separating the following duties to reduce the possibility of one employee acting alone.

- Accounting for hours worked and processing checks
- Processing and distributing paychecks
- Hiring and firing from timekeeping
- Claims processing, approval, and payment
- Travel expense approval and payment

Independent Verification

Independent verification is especially important for preventing payroll and personnel fraud, and includes the following:

- Using time clocks wherever possible, and verifying the hours worked against the clock
- Ensuring hours worked are approved by someone other than the employee
- Conducting surprise audits of the personnel and payment cycle

5.5 INVENTORY AND WAREHOUSING CYCLE

The inventory and warehousing cycle includes functions relating to the purchase and warehousing of merchandise for manufacture and resale. Because of the volume of activity and funds involved, fraud represents a significant risk.

5.5.1 Functions

The functions of the inventory and warehousing cycle include:

- Processing purchase requisitions.
- Receiving raw materials and finished goods.
- Storing raw materials and finished goods.
- Cost accounting.
- Processing goods for shipment.
- Shipping finished goods.

5.5.2 Financial Statement Accounts

Inventories on the balance sheet and cost of goods sold on the income statement are affected by the inventory and warehousing cycle. (See Chapter 10 for further information on financial statement fraud.)

5.5.3 Perpetration

The more common frauds in the inventory and warehousing cycle include: ordering unneeded inventory, appropriating inventory for personal use, theft of inventory and scrap proceeds, and charging embezzlements to inventory.

For example, a loading-dock employee and delivery-route driver were able to steal \$300,000 of inventory through collusion over a six-month period. The load sheets at the dock were either not filled out or inaccurately completed by both employees (control procedures required the dock employee and route driver to verify the quantities loaded and sign a load sheet). The products were transported to an independent distributor and subsequently sold. The defalcation surfaced when outside sources informed the company that certain products were being stolen as the result of collusion between particular employees and an independent distributor.

In a case involving a theft of inventory, an inventory records supervisor and a security guard colluded to steal \$400,000 from a jewelry warehouse over a two-year period. The security guard stole the merchandise, and the supervisor concealed the theft by manipulating inventory records. An undercover investigator, who was hired because of a significant increase in year-end inventory shortages, eventually discovered the theft. After this experience, and following a consultant's recommendation, the company started to perform surprise physical inventories at varied times during the year.

5.5.4 Detection

The three primary ways for detecting inventory and warehousing frauds are: statistical sampling of documents, computer analysis, and physical counts.

Statistical sampling includes looking for inconsistencies and discrepancies in purchase requisitions, as well as receiving reports, perpetual inventory records, raw material requisitions, shipping documents, job-cost sheets and similar documents.

Computer analysis includes identifying the following items:

- Purchases by item
- Purchases by vendor
- Inventory levels by specific kinds
- Inventory shipped by address
- Costs per item over time
- Direct labor per inventory item
- Direct materials per inventory item
- Overhead per inventory item
- Disposals followed by reorders
- Shortages by inventory item
- Shipments by address

5.5.5 Prevention

Prevention is critically important in the case of inventory and warehousing fraud because of the amounts of money involved and the relative ease with which this kind of fraud can be concealed. Prevention includes: receiving reports, keeping perpetual records, using prenumbered and controlled requisitions, raw material requisitions, shipping documents, and keeping job-cost sheets.

Someone independent of the purchase or warehousing function should handle approvals of purchasing and disbursement of inventory.

Separation of duties becomes critical in preventing this kind of fraud. Authorization to purchase should be handled by someone not performing the warehousing function. Someone other than the individual responsible for inventory should handle the receipt of inventory.

Independent checks on performance are also important prevention measures. Someone independent of the purchasing or warehousing functions should conduct the physical observation of inventory.

Physical safeguards include ensuring that merchandise is physically locked and guarded, and that entry is limited to authorized personnel.

5.6 CAPITAL ACQUISITION AND REPAYMENT CYCLE

The capital acquisition and repayment cycle, sometimes referred to as the financing cycle, includes borrowing money and accounting for the debt of an entity.

5.6.1 Functions

The functions of the capital acquisition and repayment cycle include: borrowing funds and accounting for debt, accounting for and paying interest, accounting for and paying dividends, accounting for stock transactions, and equity financing.

5.6.2 Financial Statement Accounts

The following balance sheet and income statements are most often associated with the capital acquisitions and repayment cycle (see Chapter 10 for further information on financial statement fraud):

- Cash
- Notes
- Mortgages
- Accrued interest
- Capital stock
- Capital in excess of par value
- Retained earnings
- Dividends
- Dividends payable
- Interest expense

5.6.3 Perpetration

The common schemes in this cycle include borrowing for personal use, misapplication of interest income, and theft of loan and stock proceeds.

In one case, a factoring company obtained a credit facility from a regional bank to fund the purchase of qualified assets, primarily accounts receivable. The vice president of the company, in collusion with a customer, purchased fictitious accounts receivables with the proceeds of the credit facility. Part of the purchase proceeds was wired to offshore bank accounts beneficially owned by the vice president. The activity was discovered when the bank manager reviewed the bank account of the factoring company and saw wire transfers made to Caribbean tax havens. He hired forensic accountants who discovered the bank had been defrauded of \$9.5 million over a two-year period.

5.6.4 Detection

Most frauds in the capital acquisition and repayment cycle involve tracing the proceeds of loans to ensure that all of the proceeds go to the benefit of the company. This can be accomplished by tracing loan proceeds to the bank deposits, and tracing authorization for borrowing from the minutes of the board to the loan ledgers. In addition, a computer analysis can do the following:

1. Compare addresses of interest payees.
2. Match borrowings with repayments.
3. Check the schedule of late repayments.
4. Check the schedule of authorization of loan proceeds.
5. Check the list of loan recipients.
6. Check the list of addresses where loan proceeds were delivered.

5.6.5 Prevention

Proper documentation of loan documents, journal entries, interest coupons and stock certificates can aid in prevention of capital acquisition and repayment frauds.

Proper approvals include receiving approval of the board of directors for: borrowing, paying dividends and refinancing debt. Physical safeguards include keeping stock certificates and loan documents under lock and key. Also, conduct independent checks on the transfer agent and registrar.

Segregation of duties is also important in prevention. The authorization to borrow should be separate from handling cash and accounting. Authorizations to issue stock should be separated from the handling of cash; and accounting should be separated from handling cash, and dividends and interest.

5.7 CASH MISAPPROPRIATION

Although not a cycle, cash is the focal point of most entities. All other cycles flow through the cash account. Because there are so many different ways to misappropriate cash, this section covers cash exclusively.

Most organizations can divide their cash into two major categories: petty cash and demand deposits. Petty cash consists of cash on hand that is accounted for separately. It is reimbursed periodically, and the expenditures are then booked to the various accounts. Demand deposits consist of checking accounts maintained by the entity; savings or interest bearing accounts; and certificates of deposit and all other liquid investments that can be easily converted to cash.

5.7.1 Perpetration

Frauds perpetrated on the cash accounts are normally committed in conjunction with other cycles. The most common are the theft of petty cash and the theft of bank deposits.

Theft of Petty Cash

Petty cash thieves usually forge or prepare fictitious vouchers for reimbursement from petty cash. As an alternative, perpetrators frequently *borrow* from the petty cash account and fraudulently represent that the petty cash account is intact.

For example, the head security officer had custody of petty cash. He had altered legitimate receipts—primarily for postage—to reflect higher amounts. Postage is an overhead item that was loosely monitored. At a surprise count of the fund, only about \$700 in currency and receipts were on hand of the \$4,000 fund. Polygraph examinations were given to all security officers, but the head officer resigned before his test. A promissory note for the approximately \$3,300 shortfall was executed by the former head officer. He had been with the company for seven years. The company estimated the loss at \$12,000 but was unable to prove that this amount had been stolen.

Theft of Bank Deposits

Many times employees steal cash receipts prepared for deposit. In some instances, they change the amount reflected on the deposit. In other cases, they make no attempt to conceal the theft.

In one case, an employee of a food services business received daily receipts from sales along with the cash register tapes from two or three cashiers. The employee mutilated the tapes so they could not be read, then prepared the transmittal of funds for the comptroller, but kept the difference between the amount transmitted and the amount submitted to her by the cashiers. She sent the mutilated tapes to the comptroller with the deposit. The comptroller's office did not compare the deposit with the cash register tapes. The fraud was detected when one of the cashiers noted that the transmittal to the comptroller was small for a comparatively busy day. When questioned about tracing the transmittal amount to the cash register tapes, the perpetrator was unable to show completed tapes. The employee, who had been with the company two-and-a-half years, was fired but not prosecuted.

Employees, officers, and even outsiders can steal checks, both blank and signed. One case involved an employee—a grandmother—who was the sole bookkeeper for an electrical supply company in Omaha, Nebraska. She wrote the company's checks and reconciled the bank account. Over a period of five years she stole checks totaling \$416,000, which she spent on herself and her family. In the cash receipts journal, she coded the checks as inventory; in fact, however, she wrote the checks to herself using her own name. When the checks were returned with the bank statements, she would simply destroy them. She confessed after she had a nervous breakdown, caused by continuous guilt from stealing, which she knew was wrong.

5.7.2 Detection and Prevention

Because cash can be counted exactly, most detection methods involving cash relate to its timely counting. The proof of cash is a standard audit technique that compares cash in the bank to reported cash on hand. Properly done, the proof of cash can not only account for theft, but also show overstatements or understatements by expense classification.

Timely and regular bank reconciliations by a person not responsible for handling cash will frequently reveal discrepancies. Good reconciliation methods include examining endorsements and dates, and if staff and time permit, referencing the checks to invoices, orders, and other relevant documentation.

For example, a misappropriation of funds was detected through a reconciliation of bank deposits with a collection log, which was normally kept by the accounting clerk, who at the time of the reconciliation was absent on sick leave. Because the accounting clerk prepared the collection log, the daily cash report, and the bank deposits, she was able to alter individual accounts receivable records and misappropriate almost \$24,000. She accomplished this by preparing daily cash reports that reflected fewer cash receipts collected than were actually received, and depositing the lesser amount in the company's bank account. The accounting clerk processed virtually the entire accounting transaction. After the discovery of missing funds, she was fired, prosecuted, pleaded guilty, and was sentenced to ten years' probation. She had been with the company three-and-a-half years.

Auditors frequently use cutoff bank statements to ensure that expenses and income are reported in the proper period. Surprise cash counts sometime turn up situations of employees *borrowing* or floating small loans. It is critical that these counts be done on an irregular basis.

Cash thefts are sometimes reported by customers who have either paid money on an account and have not received credit, or in some instances when they notice they have not been given a receipt for a purchase.

As an example, a client of a branch of a large bank complained that there had been a \$9,900 forged savings withdrawal from her account. The client indicated that she had recently made a \$9,900 deposit at the branch and suspected that the teller who accepted the deposit may have been involved. The employee was interviewed and admitted to forging and negotiating the savings withdrawal. The teller had obtained the client's mother's maiden name and birthplace, fabricated a duplicate savings receipt book, and on an unscheduled work day went to the domiciling branch and posed as the client. The employee did not have any identification, yet was persistent enough to obtain an approval on the savings withdrawal.

Computer analysis of the following categories can sometimes turn up fraud in a cash account: checks that are missing, checks payable to employees, checks that are void, comparisons of deposit dates to receivables, and listings of cash advances.

It is absolutely imperative to implement tight control of cash and to maintain the duties of accounting, authorization, and custody.

In one case a fraud occurred at one of several campus cashier's offices maintained by a university for collecting and processing student tuition bills and other related charges. The perpetrator was employed as a teller for approximately five years before being promoted to head cashier. This position required reconciling daily cash register receipts to the cash transmittal and bank deposits, as well as preparing deposits for funds received from outside departments, such as the bookstore or dining service operations. These deposits involved substantial amounts of cash. As head cashier, the employee also prepared the initial accounting documents that served as the input to the various general ledger accounts, including accounts receivable.

The perpetrator's extensive knowledge and experience, coupled with the employer's trust, resulted in diminishing supervision, particularly of the cash register reconciliations. As a result, the perpetrator was able to manipulate the documentation and the control procedures necessary to conceal the continued embezzlement of funds. The employee, who had six-and-a-half years' service, was fired and prosecuted for stealing an estimated \$66,000.

CHAPTER 6:

External Fraud for Personal Gain

| | | |
|-------|---|-----|
| 6.1 | Fraud Perpetrated by Outsiders..... | 3 |
| 6.1.1 | Classification of Internal and External Fraud | 3 |
| 6.1.2 | Reasons for Classification..... | 3 |
| 6.1.3 | Classification of Fraud in this Handbook..... | 4 |
| 6.2 | Individuals Versus Individuals and Corporations | 4 |
| 6.2.1 | Lawyers' Schemes | 4.1 |
| 6.2.2 | Directory Advertising Schemes | 7 |
| 6.2.3 | Property Improvement Schemes..... | 7 |
| 6.2.4 | Personal Improvement Schemes | 8 |
| 6.2.5 | Insider Trading Schemes..... | 8 |
| 6.2.6 | Homicide-for-Profit Schemes..... | 9 |
| 6.3 | Individuals Versus the Government | 12 |
| 6.3.1 | Income Tax Fraud | 12 |
| 6.3.2 | Benefit-Program Fraud | 12 |
| 6.4 | Individuals Versus Financial Institutions..... | 13 |
| 6.4.1 | Financial Institutions and Fraud | 13 |
| 6.4.2 | Credit-Card Fraud..... | 13 |
| 6.4.3 | Loan Fraud..... | 14 |
| 6.4.4 | Real Estate Fraud | 16 |
| 6.4.5 | Money Transfer Fraud..... | 17 |
| 6.4.6 | Money Laundering | 18 |
| 6.4.7 | Check Fraud | 23 |
| 6.5 | Individuals Versus Insurance Companies | 29 |
| 6.5.1 | Life Insurance Fraud..... | 29 |
| 6.5.2 | Casualty Insurance Fraud..... | 30 |
| 6.5.3 | Health Insurance Fraud..... | 31 |
| 6.5.4 | Property Insurance Fraud..... | 32 |

CHAPTER 6:

External Fraud for Personal Gain

6.1 FRAUD PERPETRATED BY OUTSIDERS

Fraud is not merely the product of internal thieves acting against their employers. Fraud in the accounting records may originate with outside suppliers and service providers as well.

It is not possible to determine the number of persons and bogus business operators engaged in crimes of this nature. Suffice it to say that the problem is extensive. By some estimates, nearly everyone at one time or another has been either a direct victim of such a crime, or an indirect victim through higher fees or income taxes.

6.1.1 Classification of Internal and External Fraud

As introduced in chapter 1, for the purposes of this Handbook, commercial fraud can generally be classified into two categories:

1. Internal fraud—that is, fraud committed against an organization by its employees, officers, or directors
2. External fraud—that is, fraud committed against an organization by arms-length parties (either individuals or corporations) who are outside the organization

Noncommercial fraud and other forms of white-collar crime also exist in which the fraudster is unrelated or external to the victim (an individual).

The Impact of Collusion

Some forms of external fraud can also be committed with the help of an internal fraudster—someone internal to the organization who is willing to assist the external fraudster commit his or her crime. Generally, internal personnel would need some form of an incentive—often in the form of a secret commission, kickback, or bribe—in order to be induced to assist in this manner.

Fraud involving parties both internal and external to an organization are sometimes referred to as *collusive frauds*. Another form of collusive fraud involves fraud committed by a group of people within an organization. Both kinds of collusive frauds exist because most internal controls are based on the principle of segregation of duties—this is circumvented by collusion.

Another form of collusive fraud, committed totally externally, is price fixing. When competitors agree to raise, fix, or otherwise maintain the price at which their products or services are sold, it is price fixing. The victimized customer of the colluders usually is not aware of the price fixing unless there is a whistle blower. And, as markets are served by

fewer and fewer entities resulting from mergers, price fixing will probably become a bigger problem.

6.1.2 Reasons for Classification

Without some form of classification, the numerous kinds of fraud would overwhelm and confuse the *student* of this topic. Learning is enhanced when long lists are grouped and classified—for instance, students of a foreign language don't start at *a* in the English translation dictionary. Instead they start by studying the common elements of verb conjugation, pronouns, nouns and adjectives so that they can grasp a wider cross section of the language, and then put it all together when they begin to speak it. Of course, languages have many exceptions to the rules. Similarly, most foreign-language pocket guides present phrases by topic. For instance, phrases relating to money are separate from phrases relating to restaurants, travel, shopping and health; however, certain phrases could be applicable to more than one situation.

Much the same way, this Handbook's approach to grouping and classifying fraud enhances the CPA's ability to learn about the numerous kinds of fraud. As a result, you should have a greater appreciation for the wide variety of fraud that can occur, and should be better equipped to recognize the signs of fraud at first sight. However, some frauds are difficult to classify, fall into more than one category, or don't exactly fit into any of the established categories. These instances are mentioned as appropriate within the body of this Handbook.

6.1.3 Classification of Fraud in this Handbook

In chapter 5, we discussed a restricted group of frauds—those committed against an organization by its employees, officers or directors—otherwise known as internal fraud.

External frauds cover all remaining forms of fraud and represent a wide variety of frauds. This chapter covers those external frauds that can be classified by perpetrator. These frauds include:

1. Fraud committed primarily by individuals against a company, government, or other individuals; this is referred to as *external fraud for personal gain*.
2. Fraud committed primarily by a company against another company, government, or individuals; this is referred to as *commercial crime*.

Note that individuals using a corporate veil could also conduct certain of the frauds presented in this chapter. Similarly, chapter 7, which primarily covers fraud by corporations, includes fraud that could be conducted by individuals directly.

6.2 INDIVIDUALS VERSUS INDIVIDUALS AND CORPORATIONS

Individuals can commit many kinds of fraud against other individuals and corporations. Most of the victims of the crimes described in this section are generally manufacturers, retailers, wholesalers, service companies or other individuals; however, in some instances, victims can also include governments, financial institutions, and insurance companies.

6.2.1 Lawyers' Schemes

Overbilling for Time

Lawyers can easily commit fraud, largely because of the nebulous nature of the services provided. As one commentator indicated: the law lends itself to confidence scams.

Contrasted to a plumber, for example, whose failure to make the contracted repair is quickly noticed, a lawyer's performance of an agreed to service is not always discernable. It

(Text continued on page 5)

could be merely some advice, a brief phone call or any number of innocuous, commonplace actions.

The victims of overbilling can include the lawyer's clients who are unable to assess whether the time billed by the lawyer is reasonable, and can also include government funded legal aid programs whose organizers are unable to assess whether the services billed were actually performed. When in doubt, a lawyer's invoices can be vetted; that is, they can be assessed by another lawyer for reasonableness regarding whether the services billed needed to be performed, and whether the time taken to perform the services was excessive or not.

Misappropriation of Trust Funds

Lawyers have access to funds provided to them by clients *in trust* to complete transactions. There are many cases of lawyers *borrowing* client funds because they are in personal financial difficulty. The most common crime associated with lawyers' trust funds is the misappropriation of client funds held in trust and the use of the money for the lawyer's personal purposes (for example, to subsidize a business, pay gambling debts, or support a life-style).

There are three kinds of misappropriation:

1. *Single transaction*: Client funds can be traced to an unauthorized disbursement (one-shot).
2. *Several transactions*: All trust-account activity is analyzed to determine which clients funds were used for unauthorized disbursements (lapping).
3. *Trust-account chaos*: Usually, this kind of misappropriation is caused by poor record keeping. Actual misappropriation of funds may or may not be found. Is the chaos the result of poor bookkeeping practices? Are there reasons for the failure to account (such as bad health, bankruptcy, intent to defraud, or loss of control due to numerous misappropriations)? The answers to these questions may emerge after a complete analysis of the trust account's activity has been made. According to the ethical rules of most states, if not all states, any use by an attorney of funds held in a trust account other than that for which the funds were placed in trust is considered a serious breach of professional conduct that may lead to disbarment, suspension or possible prosecution. There can never be a legitimate misappropriation of funds that an attorney holds in a trust account.

To uncover a case involving misappropriation of trust funds, the accountant should realize that lawyers regularly maintain two sets of bank accounts and related records, consisting of:

1. One or more bank accounts, books of account, and supporting documentation for the law practice itself.
2. A trust account together with any records reflecting the trust-account activity carried out on behalf of the lawyer's clientele. These are the most relevant records for investigating alleged misappropriation of trust funds. The primary documentation required for trust-account activity consists of bank statements and bank reconciliations for the trust bank account; the client's ledger, which outlines all receipts and disbursements made by the lawyer on behalf of the client concerning a particular transaction; and the client's file, which contains evidence of the transactions (for example, correspondence, the lawyer's

reporting letter, statement of receipts and disbursements, statement of adjustments, mortgage documents, out-of-pocket vouchers, and billings).

CPAs conducting an investigation of an attorney's trust account might also want to review the financial statements for the law practice. These records can be used to assess the successfulness of the lawyer's practice, and are most relevant when the lawyer is a sole practitioner.

See table 6.1, below, for an example of a misappropriation that would only be uncovered by a detailed investigation of the banking transactions conducted within a trust account.

TABLE 6.1 EVIDENCE OF A MISAPPROPRIATION OF A TRUST FUND.

| | | |
|------------------|------------------------|-------------------------|
| January 1, 1991 | Deposit of \$30,000 | Agrees with client file |
| January 5, 1991 | Withdrawal of \$10,000 | Unauthorized by client |
| January 29, 1991 | Deposit of \$10,000 | Unauthorized by client |
| January 31, 1991 | Balance of \$30,000 | Agrees with client file |

At the end of the month the trust liability to the client, as disclosed in the client file, is \$30,000. However, \$10,000 was temporarily removed during the month by an unauthorized transaction. Thus a misappropriation of the trust fund occurred.

Skip Towne, Esq. Case Study

After twenty years in practice, a lawyer, Skip Towne, Esq., had built up a large client base, including friends, business people and fellow church-goers. Mr. Smith, who was selling his home, retained Mr. Towne's services. At the time the transaction closed on August 3, 1998, Mr. Towne received \$176,574 from the purchaser's attorney for deposit into the Skip Towne, Esq. trust account. Mr. Towne disbursed \$5,000 of the funds in his trust account to cover various closing adjustments including outstanding utilities and tax bills. Mr. Towne also distributed \$21,176 to his own account to cover the legal fees and other disbursements related to the closing. The balance (\$150,398) due to Mr. Smith, as shown in the Closing Statement, was apparently paid in two distinct disbursements to Mr. Smith: an initial amount of \$65,000 on August 10, 1998, with the balance of \$85,398 on October 13, 1998. This final payment to Mr. Smith was, however, financed by the deposit into the trust account of funds that Mr. Towne received from new clients and other nefarious acts.

The specific funds in question, that is, \$85,398 on hand as of August 10, 1998—were not paid to the benefit of Mr. Smith. Between August 10, 1998, and October 13, 1998, Mr. Towne made a payment of \$80,000 to himself that he used to invest in his own real estate venture, and a payment of \$5,398 to his other clients, to replace trust funds that had already been spent on unauthorized disbursements. To keep the ball rolling, Mr. Towne had to misappropriate funds from a number of other clients in

order to repay Mr. Smith, in addition to producing false mortgage documents, forging signatures, and resorting to other acts of deceit.

Ultimately, Mr. Towne cleared out his trust account, abandoned his law practice, and disappeared, leaving behind at least eighty-five clients who had been defrauded. He has not been heard from since.

6.2.2 Directory Advertising Schemes

Perpetrators of directory advertising schemes usually target businesses. In this scheme the fraudster sells advertising in a nonexistent magazine or directory, and absconds with the proceeds. Many directory advertising schemes are perpetrated out of storefront operations. A fake (or in some instances, real) directory is presented to the potential victim. The victim contracts for the display or classified advertising, which will appear some months hence. By that time, the fraudster has collected the funds and disappeared.

6.2.3 Property Improvement Schemes

Fly-by-night operators, promising repairs to property at bargain rates, are a particular problem for elderly victims. The typical fraudster is a professional con artist who obtains business primarily from door-to-door solicitations. The tools of the trade are not hammers and saws, but bogus business cards and counterfeited or preprinted contracts involving the payment of up-front money. Note that these property improvement scams are a subset of procurement fraud, which is covered in more depth in chapter 7. Various forms of this scheme include substituting products, charging for false labor or overhead charges, and absconding with retainers and down payments.

Substituting Products

In a product substitution fraud, the fraudster typically promises a property owner a particular product or brand, and charges him or her for it but then substitutes an inferior brand without an appropriate price reduction. Thus the perpetrator reaps a windfall profit through this deception.

Charging for False Labor or Overhead

Many repair contracts call for labor, materials or overhead to be charged at cost, plus a specified contractor's profit as a percentage of that cost. Obviously the more the repairs cost, the more the contractor makes. By fraudulently inflating costs through the addition of bogus labor charges or overbilling of materials, the fraudster not only increases the profit but also can keep the difference between the actual and inflated costs.

Absconding With Retainers and Down Payments

The preferred method that seasoned professionals use is to simply negotiate money in advance, then disappear. This is essentially an advance fee swindle perpetrated specifically in the property-improvement or repair market. This method is advantageous to the perpetrator because it requires the least amount of capital: no storefront, props, or other accoutrements necessary—just “get the money and run.”

6.2.4 Personal Improvement Schemes

The term *personal improvement fraud* covers the many schemes that prey on people's natural tendency to want to improve their job skills, appearance, education, or position in life. Fraudsters in this category primarily use mail order as an integral part of the scheme. Some common forms of personal improvement fraud are described below.

Vanity- and Song-Publishing Schemes

Vanity- and song-publishing schemes are common, and rely on the victim believing that he or she has talent in a particular area, such as art or song writing. These schemes are normally advertised in magazines or by direct mail. They usually offer to evaluate, for free, the victim's talent. Of course the victim is told after the evaluation that he or she is the newest undiscovered artistic genius. And for a hefty fee, the talent company will promote the artist's work. The artist then remits the fee, and the fraudster uses the funds for personal benefit, providing little or no services in the process.

Modeling Schools

Modeling schools appeal to the natural vanity of some people. Typically, the modeling school tells the student that he or she must have a portfolio of portraits to send to potential customers, ostensibly to enhance the victim's potential for getting modeling assignments. The victim is then charged greatly inflated prices for a photographer to take the pictures for the portfolio. Many modeling schools are not legitimate. They sometimes tout connections to famous people, or claim they have placed famous people, when in fact they have not. These schools get most of their business through mail order or newspaper advertising. Once a particular area is fleeced, the *school* pulls up stakes and moves on.

Diploma Mills

For a fee—usually a hefty one—a *diploma* can be granted to those persons who apply. The fraudsters usually claim the heavy fee is for *processing* the application or for verifying the experience necessary to acquire a degree. The hallmark of a diploma mill is the ease with which the *degree* is obtained, and the related cost. Victims usually apply for an advanced degree to enhance their career skills; however, diploma mills are not accredited, and their diplomas are therefore essentially worthless. Given the nature of this kind of business, there is usually some culpability on the part of the so-called *victim*.

Correspondence Schools

Legitimate correspondence schools offering advanced education do exist. However, there are also many correspondence schools with the same *modus operandi* as diploma mills, providing substandard education at superior prices. They are generally not accredited and offer little hope of job advancement.

6.2.5 Insider Trading Schemes

Insider trading involves the use of nonpublic information to make stock trades on a securities or commodities market. It could include purchasing shares prior to a good news release and can also include selling shares prior to a bad news release. The perpetrators of such crimes get rich, while other investors are unable to share in the wealth. Some might

argue that this is a victimless crime, while others would say that the victims are the market as a group, because each and every trade is part of the market.

Criminal charges for insider trading have become the trademark of economic crime enforcement efforts during recent years. These efforts seek to encourage the confidence of investors in the fairness of the markets.

A surge of prosecutions for illegal insider information transactions began in the late 1980s when stock transactions were first subjected to sophisticated computer review, enabling investigators to identify unusual stock movements. Soon afterwards, when some meaningful piece of financial information about a company was released, investigators could quickly determine who had traded the stock heavily before the news release. If, for instance, a firm's president executed a transaction, it seemed likely, (though not assured), that he or she had acted on the information before it was publicly disseminated. The insider trading laws require that specified officers or directors of a corporation must report their trading activities. The fraudster, however, conveniently forgets to file the required information.

Of course, the notable cases of Ivan Boesky and Michael Milken remain the most infamous, and illustrate the staggering sums of money to be made from illegal stock trades. Boesky, the Wall Street arbitrage king, was sentenced to three years in prison and fined \$100 million. In his plea agreement, he gave information that led to the indictments of so-called junk bond king Michael Milken, who eventually pled guilty to insider trading and was fined \$600 million.

6.2.6 Homicide-for-Profit Schemes

Homicide cases are quite different from white-collar crime cases in that the perpetrator is a violent criminal, whereas most fraudsters are not violent. The tools of a murderer are guns, knives, ropes, water (for drowning), fire (for arson) and poison, whereas the tools of a fraudster are documents, books and records, computers, and calculators. The victim in a homicide case loses his or her life, whereas a fraud victim generally only loses some money.

But there is one main similarity, particularly when there is a financial motive for the homicide—the use of forensic accounting in homicide cases is similar to its use in fraud cases and may involve corporate- or personal-financial assessments, or both.

Generally, forensic accounting may be applied in homicide investigations for one or any combination of the following three purposes:

1. To analyze and determine a possible financial motive for murder.
2. To analyze financial documentation for possible investigative aids that may assist in proving murder.
3. To identify possible payments on a contract for murder.

Assessing Financial Motive

In determining a possible financial motive, the investigator must direct the accounting analysis primarily toward establishing and measuring any financial benefit to the accused as a result of that person's association with the murder victim. Benefit may be shown in any one or combination of the following methods:

- Payments by the victim to the accused (extortion).
- Assets such as real estate, collectibles, or antiques transferred to the accused.
- Insurance proceeds paid to the accused as a beneficiary under a policy.
- Other benefits, such as obtaining equity in a business or transferring of a partnership interest to the accused.
- Other motives that don't equate to a direct financial benefit, such as the imminent loss of assets, involvement in drug trafficking, or marital infidelity.

Accounting evidence is not generally as significant as viva voce evidence. It may, however, provide circumstantial evidence of a financial motive.

Assessing Financial Evidence to Assist in Other Ways in the Investigation

When assessing the financial matters of the victim in order to assist in a police investigation, the forensic accountant may seek to determine:

- The victim's business and social relationships and the identity of people with whom he or she had dealings.
- The existence of any debts owed either by or to the victim, and whether evidence exists to suggest the victim or debtor was resisting payment on them.
- The possibility of eliminating financial matters as a direction in which to pursue in the investigation.

Investigators should examine business and personal financial records, as well as financial-related evidence from the local real estate deed-mortgage recording office, lawyers, the will of the deceased, and insurance policies.

Robert Kilbride Case Study

On March 29, 1998, Mary Kilbride, wife of Robert Kilbride, a veteran police officer, was found dead outside her condominium complex. She had fallen from the twentieth floor balcony of their condominium. Eight days later, Robert Kilbride flew to the South Pacific to join Ms. Cathy Smith, whom he later married in May 1999 in Europe.

Ms. Sleuth, a forensic CPA, was called in to assist with the investigation. The police suspected Mary's death was not an accident—there was a \$275,000 life insurance policy on her life that was paid to Robert Kilbride in late September 1998.

By way of background, Ms. Sleuth was told that in July 1997, Kilbride resigned his position from the police force. Friends and acquaintances said that about this time it was evident that Robert and Mary Kilbride were having marital problems.

Ms. Sleuth then worked with the investigating officer to determine all she could about the Kilbrides' life-style. The primary objective of Ms. Sleuth's accounting assistance was to summarize Robert Kilbride's financial activity for a period of approximately one-and-a-half years prior to Mary Kilbride's death, because of the allegation that Robert had murdered his wife Mary for the insurance proceeds. No summary books and records were available, a not uncommon situation in

investigations of personal finances. Therefore, Ms. Sleuth had to reconstruct the financial facts before they could be interpreted.

The volume of financial documents was considerable. Kilbride had numerous credit cards, bank accounts and brokerage accounts in the United States, Canada and Europe. Kilbride was also involved in numerous business deals of varying nature and purpose.

In order to prove Kilbride's financial affairs, Ms. Sleuth completed the following:

1. A summary of Kilbride's financial history.
2. An analysis of Kilbride's estimated net worth as of the end of July 1997 and September 1998, based on bank statements, brokerage statements, correspondence, contracts, appraisals, loan applications and other financial documentation.
3. A source and application of funds analysis of Kilbride's financial activity from March 1997 to December 1998, primarily based on Kilbride's banking documents, credit card statements and brokerage statements.
4. A report on Kilbride's monthly deficiency based on the information in the source and application of funds analysis.
5. Graphs showing the cumulative deficiency from just prior to Mary's death to late September 1998, when the insurance proceeds were received.

These analyses revealed the following, which the investigating officer corroborated by *viva voce* evidence from former coworkers, friends, neighbors and other people who knew the Kilbrides.

1. When he left the force, Kilbride had no known source of steady income.
2. The Kilbrides' combined annual salaries were less than \$60,000, yet they lived in an expensive condominium and had a leased luxury sports car.
3. After leaving the force, Kilbride's net worth declined considerably. He began to borrow heavily and sell off certain assets, including a rental property. He was also involved with various unsuccessful business ventures.
4. By March 1998, substantially all of Kilbride's net worth was represented by assets he owned jointly with his wife. These assets included the equity in their condominium, furniture, furs, jewelry and household effects.
5. Between the time of Mary's death in March and his receiving the life insurance proceeds in September, Kilbride spent more than \$100,000 traveling throughout the United States, Canada and Europe. Although Kilbride had no known employment income, he and Ms. Smith rented a villa on the Mediterranean coast. He had approximately \$15,000 in other income during this period. Kilbride financed his life-style primarily by selling more assets, obtaining further loans and making heavy use of credit cards.
6. In late September 1998, Kilbride received the \$275,000 in life insurance proceeds from Mary's death.
7. Also in September 1998, Kilbride sold the luxury condominium; he and Ms. Smith continued to live in the Mediterranean villa until he returned to the United States in January 1999, when he was arrested.

In summary, the accounting evidence revealed that Kilbride enjoyed a life-style he could not afford. He was living well beyond his means—his expenses so greatly exceeded his income during the months before and after Mary's death that he would have been virtually bankrupt if he had not received the insurance money on Mary's life.

This evidence was very useful in establishing a motive for murder, and weighed heavily at Kilbride's murder trial at which he was found guilty.

6.3 INDIVIDUALS VERSUS THE GOVERNMENT

Fraud against the government is a general term for several kinds of schemes perpetrated against federal, state, and local governments or government agencies. Typically, frauds against the government committed by individuals involve one of the following: income tax fraud and benefit-program fraud. (See chapter 7 for a discussion of frauds against the government committed by corporations.)

6.3.1 Income Tax Fraud

According to some estimates, most taxpayers do one of the following:

1. Fail to disclose all their income
2. Take deductions to which they are not entitled

The most common income tax frauds involve categories of individuals who receive their compensation in cash. These categories include waiters, restaurant owners, bartenders, and bellhops.

For the Internal Revenue Service (IRS) to be successful with a claim for income tax fraud, intent must be proven—it is perfectly legal for taxpayers to manage their affairs to minimize their taxes—it is illegal for them to do so in a deceitful manner.

6.3.2 Benefit-Program Fraud

Another major category of fraud against the government generally involves making false statements of various kinds in order to obtain funds. The United States and other countries with strong social assistance programs are easy targets for fraudsters. The specific programs targeted include:

- Welfare benefits
- Medicare and Medicaid benefits
- Unemployment benefits
- Disability programs
- Student loan programs
- Housing programs

Often, rings of fraudsters apply for government benefits, resulting in very high losses to the government, and ultimately to the taxpayer through increased taxes.

According to a January 2001 report, the U.S. government has taken an increasingly active role in pursuing health care fraudsters. The rate of criminal convictions quadrupled from 1992 to 1999. At the same time, recoveries from civil fraud cases increased by more than 50 percent, and of the \$1.5 billion the government recovered from fraud cases, \$840 million was from health care cases, both public and private.

6.4 INDIVIDUALS VERSUS FINANCIAL INSTITUTIONS

Fraud committed externally against a financial institution can take many forms and can be committed by anyone who deals with such organizations, including individuals and corporations. The most common offenses committed by individuals—and sometimes corporations—are credit fraud, loan fraud, false mortgage security, real estate fraud, money transfer fraud, money laundering, and check fraud. These and other frauds against financial institutions, committed by individuals, are described below.

6.4.1 Financial Institutions and Fraud

Definition of a Financial Institution

For the purposes of this Handbook, a *financial institution* is any organization, whether domestic or international, that is engaged in receiving, collecting, transferring, paying, lending, investing, dealing, exchanging, and servicing money and claims to money. This also includes safe deposit facilities, custodianships, agencies and trusteeships.

Under the broadest concept, the term financial institution may be applied to institutions, such as cooperatives, export-import banks, investment bankers and mortgage bankers.

Legal Aspects of Bank Fraud

In most jurisdictions, financial institutions are insured by an agency of the government and are governed by related criminal statutes. For example, in the United States the broadest of all federal statutes is Title 18, U.S. Code, Section 1344. It covers all assets owned or controlled by a bank, as well as employees and outsiders. It prohibits any action that would defraud the financial institution, such as embezzlement, misapplication, false statements and related fraudulent behavior.

6.4.2 Credit-Card Fraud

Generally, credit-card fraud can be divided into two categories. In some instances, the fraudster uses credit information from one individual to obtain credit for use by another. For example, John R. Fraud, with bad credit, obtains the credit information of John Q. Smith, and applies for a credit card under the name of John Q. Smith, using John R. Fraud's address. John R. Fraud then makes charges on the account. When John Q. Smith protests, the credit-card company attempts to locate the real user of the credit card, John R. Fraud, who has since absconded.

The other common credit-card fraud involves duplicating credit cards and then using them to purchase high-value merchandise, for instance, jewels, furs, and other items that can easily be resold before the credit-card company catches up with the fraudster.

More attention should be paid to credit-card fraud because it is growing in volume and taking on international aspects. No longer is credit-card fraud local; the Internet has opened the door to global possibilities. A merchant extending credit on an Internet transaction has to rely on the honesty of the purchaser and the limited comfort a bank authorization provides. All too often, the merchant is stuck for the shipped merchandise and no payment.

6.4.3 Loan Fraud

Borrowers sometimes provide false information to a lending institution in order to obtain funds to continue business activity, or simply to fraudulently get money that they have no intention of repaying. Some of the most common schemes include loans to nonexistent borrowers, false applications with false credit information, bribery of a loan officer, borrower misapplication of funds, and single family housing loan fraud.

Loans to Nonexistent Borrowers

In a loan-to-a-nonexistent-borrower fraud, the borrower uses a false identity to obtain a loan. This scheme can be carried out individually by the borrower, or with the assistance of an insider, such as a loan officer.

Fraud committed by individuals can be difficult to detect, particularly if the identity documents of the fraudster match his or her details as provided on the loan application. Warning signs include:

- The borrower is unknown to bank personnel.
- No public credit report is available.
- The borrower or loan officer requests unusual loan terms.
- Loan application information does not check out.
- The proposed security has an inflated value.
- The proposed inventory (security) has an unrealistic value.
- There is no CPA associated with the financial statements.
- The loan officer's bonus is based on volume of loans funded.
- The proposed collateral is located outside the bank's market area.
- The loan proceeds are distributed prior to the loan's closing.

False Applications with False Credit Information

False information on the credit application can include overstated assets, nonexistent assets, understated or omitted liabilities, inflated revenue and understated expenses. For example, a borrower with marginal net worth might inflate the asset and income figures on his or her personal financial statements to convince the loan officer of his or her credit worthiness. The loan officer and others involved in the bank loan approval process can often detect these schemes by observing one or more of the following:

- Appraisals-valuations that defy common sense and local knowledge
- Appraisers who are paid on basis of appraisal amount
- Large loans beyond experience and expertise of the loan officer
- Borrowers who default on the first payment

- Numerous payment extensions, or payments that are placed on nonaccrual status
- No audit trail for verifying application information
- Applicant reports receiving loans from many other banks

Bribery of Loan Officers

Statutes (for example, Title 18, U.S. Code, Section 201) prohibit any officer, director, employee, agent or attorney of a bank from knowingly soliciting or receiving things of value in connection with bank transactions. In the usual scheme, a borrower offers an officer an inducement to grant a loan that would not otherwise be made (for instance, because the borrower has little or no credit, or because the borrower is not using his or her real name).

(Text continued on page 15)

Senior loan officers can often detect these schemes by observing one or more of the following:

- The life-style of the originating loan officer is beyond the means provided by normal compensation.
- The loan officer has unreasonably high productivity.
- The loan officer's compensation is based on volume productivity.
- Loan agreements contain terms unreasonably favorable to the borrower.
- There is a pattern of disbursements to particular agents, brokers, appraisers, finders, and so on.
- There are multiple loans to the same borrower with the same agents involved.
- The loan or other bank officer has a financial interest in the customer's project, or stockholdings in a bank subsidiary profiting from the business.

Borrower Misapplication of Funds

Borrower misapplication is most common when the borrower has little or no personal risk in the collateral, for example, real estate. The highest risk real estate loans are those in which the lender provides all the funding on a nonrecourse basis. The most common ways borrowers misapply loan funds are as follows:

- Kickbacks or profit interests in construction activities
- Brokerage or real estate fees
- Property management fees
- Related-party vendors
- Closing-statement prorations of rent, taxes, and other items
- Land flips
- Sale of property rights, such as laundry or cable TV
- Misappropriation of operating proceeds or loan proceeds
- Misappropriation of escrow payments

Single Family Housing Loan Fraud

One variation of the misapplication-of-funds fraud is the borrower who purchases single family housing units, ostensibly for personal use, but in reality as rental property or in some instances for resale. When applying to a financial institution, the fraudster usually misrepresents his or her ability to finance the property and make payments. Usually loan officers uncover these frauds by observing one or more of the following:

- There is an unrealistic change in commuting distance.
- A high-income borrower has little or no personal property.
- New housing expense is 150 percent or more of the previous expense.
- Bank deposits are listed in round amounts on application.
- The borrower reports overlapping dates of current and prior employment.
- The previous employer is listed as out of business.
- A high-income borrower does not use a professional tax preparer.

- The appraisal shows a tenant as the contact person on an owner-occupied house.
- The initial title report shows delinquent taxes.

6.4.4 Real Estate Fraud

Real estate fraud is essentially a specialized form of loan fraud committed either by individuals or corporations. Financial institutions, especially the savings and loan associations in the United States, were badly hit in the 1980s due to fraud committed in the real estate area. These schemes are often perpetrated in concert with the insiders of financial institutions.

Land Flips

A land flip is the practice of buying and selling a parcel of land very quickly, often in a single day or month, at a successively higher price to related parties, until a lender—who believes the transaction is at arm's length—provides financing on an unrealistically inflated loan amount. The key components of the scheme in sequential order are as follows:

1. The same piece of property is sold back and forth between a borrower—the fraudster—and dummy or shell corporations.
2. Each time the land is sold, the price is inflated.
3. To support each sale, the borrower secures an appraisal based on an unrealistic or favorable set of assumptions, or performed by a friendly, incompetent or dishonest appraiser.
4. The borrower goes to a financial institution—the victim—and mortgages the property for its *appraised* value, keeping the grossly inflated loan proceeds.
5. The fraudster defaults on the loan.

False Appraisals

Fraud perpetrators use false and inflated appraisals to support loans larger than the true value of the property. Appraisers are either parties to the fraud or paid off, or they are merely unqualified—that is, easily fooled by bogus transactions like land flips—to perform the appraisal.

Nominee Loans

Nominee loans are those made in the name of a *straw* (dummy) borrower or agent—that is, a borrower having no substance—while the identity of the real borrower is undisclosed to the lender.

Double Pledging Collateral

This scheme involves fraudulently pledging the same collateral with different lenders, before the related liens are recorded and registered. This obviously hinders the lender's ability to look to the collateral as a source of recovery when the borrower defaults.

Real Estate Fraud Detection

Lenders or other interested parties can often detect real estate fraud by observing one or more of the following warning signs:

- A single borrower has received multiple loans.
- The same appraiser has appraised two or more different properties for the same borrower within a short period of time.
- The same appraiser has made successive appraisals of the same property at high values in a short period of time.
- The property was bought or sold many times in a short period.
- The borrower is a *shell* with no real substance or a holding company whose substance lies hidden in its numerous subsidiaries.
- The buyer is obviously shopping for a loan instead of a long-term banking relationship.
- The seller of the property is another bank.
- The borrower has a prior default history.
- The borrower has a history of loan payoffs by obtaining other, larger loans.
- The loan application contains requests for several loans to different persons on the same property.
- The borrower requires the loan as a condition before delivering large deposits to the bank, with the loan being the inducement for establishing a continuing banking relationship.

6.4.5 Money Transfer Fraud

Wires totaling two to three times a bank's assets may be processed every business day. It is rare that wires do not at least equal a bank's total assets, and they can sometimes be ten times the assets for banks that have a large correspondent network. The process is highly automated at most banks.

In the most common money transfer fraud, an outsider or bank employee with access to the correct identification numbers needed to wire transfer funds, steals the funds. In one case in Chicago, a bank insider with knowledge of the wire transfer codes and procedures conspired with his friends to wire nearly \$70 million out of the country. The scheme was detected (early enough to avoid a loss to the bank) when the transfer was made from a customer's account, thereby overdrawing the account balance.

Warning signs for this kind of fraud include:

- Clerks rather than more senior personnel perform actual processing.
- Managerial personnel conduct frequent overrides of the established approval authority controls.
- There is evidence of wires to and from offshore banks in countries known for their bank secrecy laws.
- There are routine high volume, high dollar transfers.
- There are frequent wires for persons with no account at the bank.
- Access to the wire room is often not properly restricted.
- Employees become very comfortable with the routine of the job and with their coworkers.

Variations of these schemes involve misrepresenting the customer's identity. The fraudster will use pretext telephone calls to obtain correct account information from the bank. Then the fraudster obtains the codes from an insider. Thereafter, the fraudster makes a telephone call to transfer the funds out of the bank.

6.4.6 Money Laundering

Money laundering refers to the process of turning *dirty* money into *clean* money. The primary objective is to conceal the existence, source or use of illicit money and thus the underlying offence—whether the offence is trade in illegal narcotics, robbery, fraud, illegal political contributions, tax evasion, prostitution or any other criminal activity. Money launderers may also want to obstruct investigative efforts, preserve assets from forfeiture, and evade taxes.

Perpetrators may launder money in the country in which the crime is committed or where the funds originated; more often, however, they send the money across an international border. Usually they deposit the money in a bank or other institution in a tax haven and it comes back *clean* in the form of salaries, loans, fees or services.

Money Laundering Methods

There are three main methods for laundering money:

1. Through legitimate *fronts*
2. Through couriers and smurfs
3. Through the cooperation of a bank insider who ignores the reporting guidelines

Each of these methods has certain unique characteristics; however, they also have some common characteristics:

1. Large cash shipments
2. Large volume of wire transfers to and from offshore banks (However, not all offshore wire transfers involve money laundering—see below.)

Legitimate Fronts. Many money launderers open a legitimate front business that handles a great deal of cash—for instance, a casino, restaurant, parking lot, vending machine company, or pawnshop—and then deposit the ill-gotten gain along with the legitimate income of the business. Perpetrators then commingle the illegal cash with the legitimate receipts thereby disguising any illegal sources. They then withdraw the *cleaned* money or wire-transfer it to a final destination.

Interested parties, for example a bank or bonding company, can usually detect this kind of fraud by observing one or more of the following warning signs:

- Accounts accumulate deposits that are subsequently transferred out.
- Cash deposits from sources are not identified as customers of the business.
- There is a sudden and unexplained increase in the volume of cash deposits.

Money launderers can use gambling casinos. The ill-gotten cash is used to purchase chips. Later the launderers exchange the chips remaining at the end of a controlled (carefully limiting losses) gambling session for money and receive the proceeds in the form of a check from the casino, thereby creating a seemingly legitimate paper trail.

Smurfing. One variation of the money laundering scheme is to use special couriers, called *smurfs*, to make relatively small deposits and withdrawals. For example, cash deposits of \$10,000 or more must be reported to the Internal Revenue Service (IRS) on a special form called a Currency Transaction Report (CTR). To avoid this reporting requirement, smurfs make deposits or withdrawals just below this threshold amount.

Banks and other interested parties can usually detect this kind of fraud by observing one or more of the following warning signs:

- Withdrawals made in numerous transactions just under \$10,000.
- Customers who are not account holders exchanging large amounts of small bills for large denomination bills.
- Inquiries as to policies of the bank regarding reporting currency transactions.
- Large dollar volume of cashier's checks and money orders sold for cash to customers who are not account holders.
- Persons shown as unemployed and self-employed on a CTR.

Breaches of the Reporting Guidelines. In still another variation, the money launderer conspires with a bank insider, who agrees to make deposits for the money launderer and forego the reporting mechanisms. The bank gets free use of the deposited funds, and in some instances, the bank officer is compromised through a bribe or kickback. Banks can usually detect this kind of fraud by observing one or more of the following warning signs:

- An account with many different individuals making deposits, and only a few making large withdrawals.
- Accounts with accumulated deposits that are subsequently transferred out.
- High dollar limits and large numbers of bank customers exempted from CTR requirements.
- An incorrect or incomplete CTR.

Money Laundering Mechanics

Although laundering and offshore banking conjure up images of financial wizardry and international tax lawyers and accountants, most illegal activity involves the simple addition of some layers to the basics common to ordinary business transactions. In essence, laundering works like this.

Party A, who has come by the dirty money (or legitimate money that needs to be laundered) gives it to Party B, who is the laundryman. Party B sends the money offshore where it is deposited and funds are subsequently disbursed or laundered and then returned to Party A for use.

During the laundering, Party B, having received the money from Party A, sets about concealing it. Having the money in currency upon receipt makes the job easier. If the money is in paper (checks, and so on), Party B may have to first start the laundering process by converting it to local currency. Party B has, or sets up, one or more local companies, of which he or she is the owner, manager or employee, depending on the relationship to Party A.

Now the offshore part of the process begins. Party B goes to a tax haven lawyer and establishes an offshore company: loan companies, finance companies, or trusts are preferable. Party B's name does not appear anywhere in the legal documents.

The company in the tax haven opens an offshore bank account. Party B travels to the haven with the currency, and Party B or the lawyer buys a cashier's check at the bank with the tax haven company as remitter. The lawyer then draws up the necessary loan documents to show a loan from the haven company to Party B's local company. Party B then returns home with the cashier's check. Thus, the money is brought back home as a loan (which being capital, not revenue, is not taxable) and is *clean*.

Party A on his own, or through Party B, now makes use of the laundered funds by drawing out salaries, obtaining loans from Party B's local company, paying dividends, opening a corporate expense account, using a company car, and so on.

Party B's local company files appropriate tax returns and makes note of payments, or at least interest payments. Interest is deducted on the company's tax return. If the company loses money, it has a tax offset. Party B does nothing illegal in the local country and, of course, makes interest payments on the loan payable to the offshore company, allowing further funds to be moved.

If a law enforcement agency questions the loans, the company will obtain full documentation from Party B's attorney in the tax haven. Inquiries beyond documents will be blocked by the haven's secrecy requirements.

Offshore Banks and Tax Havens

There are many reasons, some legitimate and some not, why money launderers transfer money and other valuable securities from one jurisdiction to another jurisdiction that has secret banking privileges. These foreign jurisdictions are commonly referred to as tax havens because, in addition to bank secrecy laws, they had no income taxes so people or companies first used them to (legally) minimize or to (illegally) evade taxes.

Tax haven is now a misnomer, since funds may be deposited for reasons other than escaping tax. Tax havens have grown in popularity in recent times as one of the few means of placing funds beyond the reach of creditors or other investigators. It did not take long for criminal organizations and individuals to exploit the sanctuary of the tax haven. With the development of multinational banking systems and international business and commerce, it became easy to put together sophisticated laundering schemes to move the proceeds of crime to foreign banks protected from intrusion by law enforcement officials.

The World's Tax Havens. Switzerland has a long history as an international tax haven, imposing little financial regulation and strict secrecy laws. Many other countries have jumped aboard the bandwagon. The key tax havens include—

- Bermuda and the Caribbean: Antigua, Bahamas, Caymans, Montserrat, Netherlands Antilles, St. Vincent, and Turks and Caicos.
- Central America: Panama and Costa Rica.
- Channel Islands: Guernsey and Jersey.
- Pacific: Hong Kong, Singapore, and Vanuatu.
- Other locations: Liberia, Bahrain, Liechtenstein, Switzerland, and Cyprus.

Offshore Facilities. Typically, the tax haven's biggest domestic industries are banks, financial institutions, companies, trusts, agents, accountants and attorneys who collectively constitute offshore facilities. Facilities that are available in tax havens include—

- *Banks.* There are two classes of banks. Class A banks conduct local business transactions in the tax haven. Class B banks exist on paper only, as they conduct no local business transactions.
- *Companies and trusts.* Companies can be incorporated in the tax haven; trusts (such as family, estate, or other kinds) can be set up.
- *Offshore agents, accountants and attorneys.* These are an essential element of the offshore facilities in a tax haven.

The Tax Haven's Rationale. Tax havens encourage offshore facilities for economic, political and social reasons, all of which benefit their residents. For example, offshore facilities generate up to 20 percent of the Caymans' revenues, balance the budget in Montserrat (through licensing fees) and have a huge impact on local economies, particularly those of economically emerging countries.

For example, in 1964 the Caymans had one or two multinational banks and virtually no companies. By 1981 they had thirty multinational banks, 300 Class B banks, and about 13,600 companies, the latter handled by a small number of lawyers, accountants and agents. The Caymans' total population in 1981 was about 15,000.

Many havens claim that the United States blames them for problems that it is unable to solve domestically. Furthermore, offshore competition is so stiff that it is estimated that if one country were to cease being a tax haven three more would start. (When Switzerland relaxed its secrecy laws, Bahamian and Caymanian business grew at a rapid rate.) Also, bank brokers move from island to island as laws tighten or loosen.

A local Bahamian bank executive summed it up when he said

The Bahamas must do things which are not allowed in the United States because to do things which are allowed in the United States is noncompetitive, since in every instance the United States does it better than the Bahamas do. The Bahamas are therefore compelled in banking and trust operations to appeal to unallowable activities and by inference to appeal to activities disallowed in the United States.

Secrecy. The vital characteristic of a tax haven is that it allows offshore facilities to conduct their affairs behind a veil of secrecy. Tax havens offer not only secret, numbered bank accounts but also corporate laws and secrecy provisions that prevent law enforcement officials from intruding. In addition, lawyers from tax havens offer a further level of secrecy because they too are shielded by the haven's secrecy laws, they maintain attorney-client privilege, they sometimes do not know who their clients are, or they may be coconspirators, or any combination thereof.

Tax havens view secrecy as a necessity for keeping offshore business. Business people from various parts of the world (the Middle East and South America, for example) consider secrecy to be a normal characteristic of business affairs. Flight capital (money being sent out of politically unstable countries) has to be transferred secretly. Thus, it is not only criminals but also politicians and governments to whom secrecy is attractive.

Civil secrecy exists in common law as the result of a British case, *Union v. Tournier* (1907). This case established that a banker had a duty to treat his customer's affairs as confidential. Many havens follow this law. Some jurisdictions have passed stringent, criminal laws to buttress *Tournier*—for example, the Bahamas and the Caymans. Corporate laws in the havens also aid secrecy by permitting nominee owners and bearer shares, prohibiting disclosure of the beneficial owner, not requiring financial statements and audits, and allowing the purchase of companies off the shelf.

Quite apart from the law, secrecy prevails in some tax havens by virtue of inadequate records, unskilled administrators and corruption.

Vehicles Used to Transfer Funds to Tax Havens. Individuals or businesses can use several kinds of institutions to transfer funds to tax havens. These include banks with international branches or facilities, smaller trust companies and banking institutions, shipping companies, real estate companies, travel agencies, money changers, insurance companies, finance companies, brokerage and investment companies, international trading companies, holding companies, and multinational corporations. The transfers themselves may be legal or illegal. The transfer can be accomplished by means of letters of credit to a bank in a tax haven, a bank draft, a wire transfer, or the transport of cash itself.

File Folders. Money launderers can purchase a set of legal papers in tax havens—for example, legal documents, financial statements, and banking documents dated some years before they are purchased. These documents make it appear that the company has been in business for several years. In reality, of course, it never previously existed. These companies have no substance.

Tax Havens and Law Enforcement. The combination of offshore corporate entities and secret bank accounts in tax havens permits entities to construct a maze of financial transactions. The tracing of assets becomes a very complex task. The transferring of questionable funds from one tax haven jurisdiction to another greatly compounds the complexity.

Enforcement problems are pervasive, affecting not only criminal but also civil actions (such as divorces, bankruptcies, and so on). Investigating cases takes a tremendous effort, and conviction is by no means certain. There is no central clearing house to handle offshore inquiries.

Investigations into Narcotics Trafficking

Narcotics trafficking is currently the primary source of laundered funds. The sophistication and complexity of laundering schemes are virtually infinite and are limited only by the creativity and expertise of the criminal entrepreneurs who devise the schemes. Organized crime uses banks and other financial institutions in the course of laundering as routinely, if not as frequently, as legitimate businesses use banks for legitimate purposes.

Previously, much of the investigation into narcotics trafficking occurred on the street in which the drugs were followed to identify the dealers. Although this led to many successful prosecutions, it seldom exposed the leaders of the organizations. The problem with a street investigation is that the authorities generally cannot make a buy from, or a sale to, the top person in the organization without the use of an informant, who is generally unreliable. Furthermore, because the sentences received by drug traffickers were often so light,

perpetrators considered the risk worth taking—and the leaders of the organizations continued to be insulated.

Currently, law enforcement authorities obtain financial documentation during seizures in order to establish that certain individuals possess goods that far exceed their known sources of income. This technique has made possible the successful prosecution of the leaders in drug trafficking schemes. Generally investigators use two methods to prove the flow of funds obtained from narcotics trafficking:

1. Net worth analyses
2. Sources and uses of funds

6.4.7 Check Fraud

Check fraud is a general term for the attempted negotiation of bad checks at a financial institution. Typically con artists prey on banks in an attempt to negotiate fraudulent or fictitious instruments. Common kinds of check fraud include forged, altered, and stolen checks; new account fraud; and check kiting.

Forged, Altered, and Stolen Checks

Most attempts to defraud banks involve one or more of the following:

1. Checks bearing the forged names of makers, endorsers or payees.
2. Altered checks showing increased amounts.
3. Counterfeit checks.
4. Stolen checks passed by others.

Bank officers and other investigators can detect this kind of fraud by observing one or more of the following warning signs:

- Obvious written alterations on checks
- Illegible maker, endorser or officer signatures
- Checks imprinted with a maximum amount, or the term *void*, or *nonnegotiable*
- Unprofessional printing
- Business checks presented for cash instead of deposit

New Account Fraud

Check fraud is much more likely to occur in new accounts than in established accounts. Bank employees must make special efforts to properly identify the potential new customer, without offending existing customers. Banks should establish screening criteria that must be enforced by everyone handling new accounts. These employees must take prompt, decisive action to manage or close (or both) apparent problem accounts.

Most perpetrators of new account fraud use false identification. Examples include fraudulent birth certificates, fraudulent passports, duplicate social security numbers, fraudulent voter registration cards, stolen credit cards, stolen driver's licenses, stolen paychecks, front (shell) businesses, fraudulent student-identification cards, and disguised identities (including post office box mail address, lock box rental, mail forwarding, telephone answering service, and rented office space).

New-account criminals are professionals. They use false identification to open new accounts and steal money before the bank collects the funds. Bank officers can normally detect new-account fraud by observing one or more of the following warning signs:

1. The customer resides outside the bank's normal trade area.
2. The customer rushes to open an account and obtain a loan.
3. The customer's dress or actions, or both, are inappropriate for his or her stated age, occupation or income level.

To help prevent this kind of fraud, banks should consider adopting the following procedures:

1. Implement well-defined procedures for increasing employee awareness of new-account fraud.
2. Establish specific guidance about acceptable identification and its reporting.
3. Require detailed verification of customer's information, including—
 - Previous checking account history (internal and external investigation).
 - Credit reports and credit scoring systems.
 - Dun & Bradstreet reports.
 - Better Business Bureau reports.
 - Special requests for no mail contact.
 - Post office box or hotel address.

Check Kiting

Check kiting is a term for building up large apparent balances in one or more bank accounts, based on uncollected or floated checks drawn against similar accounts in other banks. As banks decrease the amount of time taken to clear checks, this kind of fraud is becoming less common. Although many individuals engage to some degree in kiting, a commercial customer can perpetrate this scheme by using several bank accounts to increase available cash reserves.

The brokerage firm, E.F. Hutton, committed one of the most significant check-kiting schemes perpetrated in the United States. They engaged in a \$20-million kiting scheme to decrease the cost of their funds during the late 1980s. The resultant bad publicity eventually led to the company's demise.

Check Kiting, Illustrated. In commercial bank accounts established over a period of time to avoid suspicion, a fraudster starts with little or no money in Bank A and Bank B, and writes \$5,000 in checks on each for deposit in the other:

| | Bank A | Bank B | Total |
|-------------------|---------------|---------------|--------------|
| Apparent Balances | \$5,000 | \$5,000 | \$10,000 |
| Actual Balances | -0- | -0- | -0- |

Chapter Six: External Fraud for Personal Gain

The process is quickly repeated (for example, the next day) with \$8,000 in deposited checks:

| | Bank A | Bank B | Total |
|-------------------|---------------|---------------|--------------|
| Apparent Balances | \$13,000 | \$13,000 | \$26,000 |
| Actual Balances | -0- | -0- | -0- |

A \$6,000 down payment is made on a Mercedes from a check written from Bank A.

| | Bank A | Bank B | Total |
|-------------------|---------------|---------------|--------------|
| Apparent Balances | \$7,000 | \$13,000 | \$20,000 |
| Actual Balances | (\$6,000) | -0- | (\$6,000) |

The next day additional checks for \$4,000 each are written and deposited into each account:

| | Bank A | Bank B | Total |
|-------------------|---------------|---------------|--------------|
| Apparent Balances | \$11,000 | \$17,000 | \$28,000 |
| Actual Balances | (\$6,000) | -0- | (\$6,000) |

The balances are then paid to a travel agent, and the fraudster takes a long trip:

| | Bank A | Bank B | Total |
|-------------------|---------------|---------------|--------------|
| Apparent Balances | -0- | -0- | -0- |
| Actual Balances | (\$17,000) | (\$17,000) | (\$34,000) |

Check Kiting Characteristics. Bank personnel usually uncover check-kiting schemes by observing one or more of the following warning signs:

- Frequent deposits and checks in same amounts.
- Frequent deposits and checks in round amounts.

- Frequent deposits of checks written on the same paying bank, which is not the deposit bank.
- Little time lag between deposits and withdrawals.
- Frequent Automatic Teller Machine (ATM) account balance inquiries.
- Many large deposits made on Thursday or Friday to take advantage of the weekend.
- Large periodic balances in individual accounts with no apparent business explanation.
- Low average balance compared to high level of deposits.
- Many checks made payable to other banks.
- Bank willingness to pay against uncollected funds (note that not all payments against uncollected funds are check kites, but all check kites require payments against uncollected funds).
- Cash withdrawals with deposit checks drawn on another bank.
- Checks drawn on foreign banks with lax banking laws and regulations.

Slowing the Bank-Clearing Process. Before the days of sophisticated computer systems, a check-kiting scheme could develop using less paper, fewer financial institutions, and smaller amounts than are commonly used today. Banks can still be hit with large losses when a fraudster slows down the bank clearing process. Typical fraudsters' procedures include—

- Using counter checks without any computer or Magnetic Ink Character Recognition (MICR) coding.
- Providing insufficient information on checks (for example, using an incomplete name of a bank and branch, leaving out the account number, giving an illegible signature).
- Making errors on the face of checks such as date and figures.
- Defacing the check (for example, by using staples).
- Placing stop payments on certain documents.
- Having accounts in institutions other than chartered banks (that is, trust companies and credit unions).

New Techniques. It is now very difficult to effect a check-kiting scheme employing the same procedures as in the past. Banks are reluctant to accept counter checks; more significantly, checks usually take only one day to clear. This is true even for checks issued on out-of-town or out-of-state banks. The financial institutions claim that, in the near future, checks will clear instantaneously. To counteract the tightening of bank procedures, the fraudster has had to increase the number of financial institutions used, the dollar amounts, and frequency of checks issued.

Check-Kiting Scheme Investigations. The main issues to be addressed when investigating a check-kiting scheme are as follows:

1. The loss does not necessarily occur at the time of detection. Banks are usually put at increasing financial risk over a period of time.
2. Accounting evidence must show that—
 - a. Control was exerted over a number of accounts.
 - b. A loss did occur.

- c. Economic risk has increased as shown by day-by-day analysis.
 - d. Every time the perpetrator withdraws money from the system of accounts (in excess of the deposits put into the system), the bank incurs a loss or risk of loss.
 - e. The volume of inter-account checks is high.
3. The bank must determine whether it gave implied credit to the accused through *daylight overdraft* privileges, which allow an overdraft balance at the end of a business day to be cleared up before the close of the next business day to cover the previous day's overdraft.
 4. The timing of the investigation and the availability of legible microfilm documentation are important.
 5. Documentation of the *modus operandi* needs liberal use of visual aids.

Accounting Assistance. When investigating check-kiting, the CPA should—

- Identify the fraudster-controlled accounts because the financial institutions where they are maintained risk suffering economic losses.
- Identify and demonstrate the loss. This task is difficult because there is a mistaken tendency to regard loss as occurring at the termination of the check-kiting scheme. In fact, however, the risk of loss usually builds up day by day, over a period of several months. Recognition of the economic loss occurs when the perpetrator abandons the fraudulent activity for whatever reasons (this is equivalent to the game of musical chairs—the loss isn't recognized until the music stops).
- Perform a day-by-day analysis to show both the buildup of the loss and the increase in economic risk to the financial institutions.
- Recognize that a check-kiting scheme could take place over an extended period of time without the knowledge of the bank. This is an issue that is frequently raised in court. This component is an educational aspect for many: lawyers, police, bank officials, laymen, and even CPAs find check kiting difficult to understand.
- Try to accomplish the difficult task of demonstrating to a court of law that this case was not merely an unbroken circle of checks and that this *shell game*, which was apparently tolerated by the financial institutions, resulted in economic loss to them.

Mr. I.M. Kiter Case Study

Recently, between January and the middle of March, an extremely busy, well-respected professional, Mr. I.M. Kiter, operated a massive check-kiting scheme that employed at least eight bank accounts at three separate financial institutions. For two-and-a-half months he was able to falsely inflate the value of his accounts by issuing checks to or from his various accounts.

About four weeks before the scheme was uncovered, one of the financial institutions was sufficiently concerned about the status of Mr. Kiter's accounts that it would only accept certified checks for deposit. This had the effect of reducing the clearing time to zero days or in certain instances to minus one day (the check was certified

the day before it was deposited). Despite these restrictions, Mr. I.M. Kiter was able to continue his check-kiting scheme for the following reasons:

1. The other financial institutions did not require deposited checks to be certified.
2. Some overdraft privileges were permitted.
3. Mr. Kiter spoke with the financial institutions daily and explained away his suspicious conduct.
4. Checks were not return marked *not sufficient funds* (NSF), as required by bank policy, because the bank's normal policies were changed for Mr. Kiter, a *good* customer.
5. The bank permitted daily daylight overdraft privileges.

Forensic accountants performed an analysis of the deposit and disbursement activity in the various bank accounts. With the exception of the closing bank overdraft, the deposits totaled about \$87.5 million, of which more than \$85 million represented money circulated among the eight accounts controlled by Mr. Kiter. The total amount of actual deposits from noncontrolled accounts only amounted to about \$2.5 million. The ending balance in one of Mr. Kiter's accounts at Anytown Bank was a negative \$1.7 million. This overdraft balance resulted in a loss that was fully absorbed by Anytown Bank. Forensic accountants also performed an analysis of an account maintained by Mr. Kiter at Bigtown Bank for the period March 1 to March 10. This analysis indicated that Bigtown Bank permitted ongoing overdraft privileges to Mr. Kiter in amounts up to almost \$1 million. Closer inspection revealed the extent of Mr. Kiter's abuse of the daylight overdraft privileges.

This practice was confirmed by the review of Bigtown Bank's credit correspondence, and demonstrated that the departure from Bigtown Bank's policy allowed Mr. Kiter to continue the check-kiting scheme in an uninterrupted fashion. In fact, when the kiting scheme fell apart, it provided Mr. Kiter with a defensible position for court purposes (that is, his conduct was condoned or *blessed* by Bigtown Bank).

The practices of Bigtown Bank also raised the questions as to whether the economic loss suffered by Anytown Bank was because of the check-kiting scheme, or because of the conduct of Bigtown Bank. Evidence introduced during the trial did not establish that the banks were aware of the kiting scheme. However, there was evidence that Bigtown Bank knew that Mr. Kiter was having some cash flow difficulties pertaining to closing a number of real estate deals. Handwritten comments from the Bigtown Bank branch manager to his credit department indicated that—

1. The bank closely monitored Mr. Kiter's account.
2. The bank allowed certified checks to cover the overdraft daily.
3. The bank tolerated daily overdraft amounts of approximately \$ 1 million.
4. The bank received substantial revenues via overdraft and service charges (an example of the bank greed factor).
5. The bank indicated at a meeting held with Mr. Kiter on February 25th that it would permit the overdraft arrangement to continue for another sixty days.

6. Mr. Kiter had social connections and was a source of business for the bank.

Although Mr. Kiter was found guilty, the judge's ruling implied that prior knowledge of the check-kiting scheme on the part of one of the banks weakened the prosecution's case.

6.5 INDIVIDUALS VERSUS INSURANCE COMPANIES

Insurance fraud generally consists of a presentation to an insurance company of a materially false or misleading written statement relating to either an application or claim for insurance. Fraud occurs not only when there is an actual loss (that is, a claim is made based on bogus information), but also when there is a risk of loss. This distinction is important for insurance fraud because insurance policies relate to risks. Accordingly, if an insurance policy based on a material misstatement is placed, the insurance company is the victim of a fraud because there was the risk of a claim, even if no claims are made on the policy.

Some insurance policies relate to risks faced by individuals, whereas others relate to risks faced by corporations. This section deals with both kinds.

Computers have become an important tool in discovering insurance fraud. The most common use is to let the computer discover clusters or interrelated data; for example, an unusual number of claims filed from the same address. This kind of screening is effective in insurance scams because the fraudsters often work in consort, for example, with doctors or auto repair shops, to file inflated claims that a search engine seeking commonality can discover.

6.5.1 Life Insurance Fraud

Life insurance is a policy that pays the insured's beneficiary a predetermined amount of money in the event of the insured's death. Common life insurance frauds include homicide fraud, staged-death fraud, preexisting health condition fraud, and double-indemnity fraud.

Homicide Fraud

A beneficiary of a life insurance policy may commit homicide to collect benefits. In these cases, there are actually two victims—the person who has been murdered (see section 6.2.6), and the insurance company, which is required to make a payment on the policy.

Staged Death Fraud

An insured might fake his or her death in order to collect benefits. A variation of this scheme occurs when a policy is taken out on an insured who is already dead.

Preexisting Health Condition Fraud

An otherwise uninsurable person obtains a life insurance policy through false health statements on the application describing preexisting health conditions. The normal, minimal medical examination would not be sufficient to expose the condition. The insured hopes to die of causes unrelated to the *feared* condition—that is, a condition that would

otherwise prevent the policy from being issued—and without an autopsy being performed, so that the insurer will pay the policy benefits.

Double Indemnity

In some cases, a beneficiary of a life insurance policy will report the death as having been accidental in order to obtain twice the face value of the policy. A variation of this scheme occurs when a beneficiary attempts to make a suicide appear to have been accidental.

6.5.2 Casualty Insurance Fraud

Casualty insurance covers the personal injuries and property damage that result from an accident or other covered occurrence. While accidents can occur anywhere and at any time, a large number of casualty claims involve injuries sustained in traffic accidents. The following are the common casualty insurance frauds:

- Staged accidents
- Mortgage insurance fraud
- Legitimate accidents with false claims
- Personal injury insurance fraud
- Fraudulent claims

Staged Accidents

A staged accident is one in which, for example, an individual will purposely pull out into the path of an oncoming vehicle or will allow themselves to be rear-ended in order to cause a collision. A fraudulent claim is then made for nonexistent personal injuries or a falsely inflated claim is made for real injury. These kinds of insurance fraud usually involve *rings* of individuals, including unscrupulous doctors, attorneys and claim adjusters.

Mortgage Insurance Fraud

Mortgage insurance is a policy that guarantees mortgage payments to the lender if the purchaser of the property defaults on those payments because of death or disability. A typical mortgage insurance fraud is a variation on a staged accident fraud—for example, an employee who is laid off from work claims that he is disabled, so his mortgage is paid via his mortgage insurance policy.

Legitimate Accidents with False Claims

In many cases, an individual is involved in a legitimate accident and later exaggerates his or her personal injuries (usually soft-tissue injuries) to bilk the insurance company.

Personal Injury Insurance Fraud

Personal injury insurance fraud usually involves lying about the circumstances of the cause of an injury so as to bring it within the insurance coverage. For example, a worker covered by workers compensation insurance injures his back while working at home but reports it as a job-related injury to come within the workers compensation insurance coverage.

Fraudulent Claims

A fraudulent claim is one in which, for example, an insured's auto is brought into a body shop for repair after a legitimate accident. The body shop inflates the claim, typically to

cover the deductible. The body shop may then pay a cash bribe to the claims adjuster or intentionally cause additional damage to the car to maximize its profit.

In another example, an insured seeks the cooperation of a scrap yard that has the capability to crush autos. The insured has his auto crushed and files a theft claim. If the auto is not recovered within a reasonable span of time, the claim is paid. The insured then pays the scrap yard for destroying the vehicle without a trace.

In still another variation, a wrecked vehicle is located and insured. A bogus accident is concocted and a fraudulent claim is filed. Using the same vehicle, this scheme is often repeated with different insurance companies.

6.5.3 Health Insurance Fraud

Health insurance is a policy that covers someone's health in the event that the person is injured or becomes ill. Common health insurance schemes include mobile labs, bundling and unbundling claims, and collusion between an insured and a provider.

An insurance industry representative reported, in January 2001, that fraud claims in both the public and private sector reach about \$53.9 billion annually. The U.S. government has increased the funding of law enforcement agencies in the health-care fraud area, with some U.S. attorneys offices setting up special health-care fraud units. According to one U.S. attorney, health-care fraud is the most active area of white-collar crime, which includes going after clinical labs and individual doctors, among others.

A growing fraud related to credit-card fraud is debit-card fraud. Many banks are now issuing a combination ATM/debit card/credit card rather than three separate pieces of plastic. Although merchants, generally, cannot check whether there are funds in the bank supporting a debit card purchase, they can check a credit card with a phone call. No doubt as the problem grows, protective steps will be installed to stop the fraudsters. Until the preventive measures catch up, prosecuting and publicizing the fraud will help slow the growth of this new threat.

Mobile Labs

In the usual mobile lab scam, a group of people set up a *lab* in a storefront located in a blue-collar, low income area, often where English is the second language. They then pass out fliers in the parking lot of a minimum wage manufacturing firm, offering *free* physicals to people who have medical insurance. After filling out a family history, the insured is subjected to extensive tests for a variety of maladies, and the average physical ends up costing the insurer three to four thousands dollars. When the insured returns for the results of the tests, the lab is gone.

Bundling and Unbundling Claims

Bundling and unbundling claims is the practice of physicians or clinics billing separately for medical services performed at the same time. For example, an insured woman has a hysterectomy performed and at the same time she also has her appendix removed. The physician, however, bills the insurance company as if the appendectomy was a completely separate procedure.

Insured-Provider Collusion

In collusion between an insured and a provider, the provider furnishes the insured with a bill for services not actually rendered. The insured makes an application for reimbursement to the insurance company, and the proceeds are divided between the insured and the provider.

6.5.4 Property Insurance Fraud

Property insurance is a policy that covers an individual or corporation's property from loss (whether stolen or destroyed), up to a predetermined amount of money. Common property insurance schemes include: staged false theft, repossessed household goods, pawned personal property, and arson.

Staged False Theft

In staged false theft, an insured secretes property he or she owns and reports it stolen, or alternatively reports property stolen that he or she never owned.

In a recent case involving Michael Jackson CDs, a music distributor had misjudged the demand for the CD and had excess inventory on hand. A theft was then staged in order to offload the excess stock, which was then destroyed. When forensic accountants revealed the lack of demand and the excess inventory, the distributor dropped his claim.

Repossessed Household Goods

Repossessed household goods fraud occurs when, for example, household items (furniture, appliances, and so on) are repossessed, and the insured reports the property was stolen.

Pawned Personal Property

When pawning personal property, a fraudster may inflate the value of his or her personal belongings, insure them, and then pawn them for a lesser amount of cash. The fraudster then reports them stolen and files a claim. Once the insurance payment is received, the fraudster then redeems the items from the pawnshop with a portion of the insurance payment, and pockets the difference. These schemes can be risky to the perpetrator, however, because in most states pawnshops are required to check customer identification and keep records of their transactions, in order to facilitate police investigations of reported thefts.

Arson

Arson is the purposeful destruction of property by fires, sometimes for profit. For example, an insured may be about to lose his or her house, car, or business due to an inability to make loan payments. The insured sets fire to the property to collect the insurance proceeds. Alternatively, an insured may replace an item with something less expensive when he or she remodels after the fire.

Arson can also be committed by companies, which then file claims under their property insurance policies as well as their business interruption policies. This is covered in chapter 7.

CHAPTER 7:

Commercial Crime

- 7.1 Overview..... 3
 - 7.1.1 Definitions..... 3
 - 7.1.2 Victims of Commercial Crime..... 4
 - 7.1.3 Extent of Commercial Crime..... 4
 - 7.1.4 Responsibility for Commercial Crime 4
 - 7.1.5 Characteristics of Commercial Crime..... 5
 - 7.1.6 Investigation and Prosecution of Commercial Crime 6
 - 7.1.7 Causes of Commercial Crime..... 6
- 7.2 Forms of Commercial Crime 7
 - 7.2.1 Corporate Shams..... 7
 - 7.2.2 Investor Frauds.....12
 - 7.2.3 Finance Fraud.....14
 - 7.2.4 Arson for Profit.....20
 - 7.2.5 Procurement Fraud23
 - 7.2.6 Organizational Bribe Giving.....26
 - 7.2.7 Industrial Espionage27
 - 7.2.8 Securities Fraud29
 - 7.2.9 Environmental Abuse39
 - 7.2.10 Economic Extortion.....43
 - 7.2.11 Customs Duty Fraud.....44
 - 7.2.12 Health Care Fraud46
 - 7.2.13 Possession of Property Obtained by Crime.....46
 - 7.2.14 Coupon Redemption Fraud48



| | | |
|-------|--------------------------------------|----|
| 7.3 | Prevention of Commercial Crime | 48 |
| 7.3.1 | Increased Awareness | 49 |
| 7.3.2 | Formal Deterrence | 49 |
| 7.3.3 | Informal Deterrence | 50 |
| 7.3.4 | Ethics | 50 |

CHAPTER 7:

Commercial Crime

7.1 OVERVIEW

7.1.1 Definitions

The terms *white-collar crime*, *economic crime*, and *commercial crime* are not legal ones and are often used interchangeably. This chapter covers the distinctions between these terms.

White-Collar and Economic Crimes

Although scholars differ widely in their definition of white-collar crime, the *Dictionary of Criminal Justice Data Terminology*, published by the U.S. Bureau of Justice Statistics, defines white-collar crime as: “non-violent crime for financial gain committed by means of deception by persons whose occupational status is entrepreneurial, professional or semi-professional and utilizing their special occupational skills and opportunities; also non-violent crime for financial gain utilizing deception and committed by anyone having special technical and professional knowledge of business and government, irrespective of the person’s occupation.” This definition includes most if not all of the crimes and behaviors described in this Handbook.

Economic crime has a similar definition regarding its objective and methodology, that is, crime committed for economic gain by means of deception; however, economic crime is broader in its scope than white-collar crime: it could also include violent crimes committed by people without any particular occupational status—for example, armed robbery.

Commercial Crime

The term commercial crime is frequently used as a substitute for the terms white-collar crime and economic crime. However, for purposes of this Handbook, a more restrictive definition is adopted: that is, commercial crime is white-collar crime committed by an individual or a group of individuals in a company for the benefit of that company and, indirectly, themselves.

This distinction, that is, between fraud committed *against* a business or commercial entity, and commercial crime committed *by* a business or commercial entity—is a useful one. Historically, our legal system, institutions, and even the procedures adopted by auditors have tended to focus more on conventional fraud committed purely for personal gain. In recent years, however, awareness has been heightened to the possibility of the business or commercial entity itself being the perpetrator.

Frauds against investors and environmental crime are two examples that have received increasing media attention.

7.1.2 Victims of Commercial Crime

Victims of commercial crime can include—

- Customers—for example, through false advertising and price fixing.
- Competitors—for example, through industrial espionage and intentional copyright infringement.
- Creditors—for example, through a planned bankruptcy.
- Investors—for example, through false financial statements and other securities fraud.
- The general public—for example, through environmental abuse.

In addition, the practice of organizational bribe giving may victimize any one of the above groups—for example, the general public when a bribe is given in the awarding of a government contract.

7.1.3 Extent of Commercial Crime

Two decades ago commercial crime received much less media attention than today, largely being confined to a short paragraph or two in the business section of the nation's newspapers, if it was mentioned at all. Today's front-page stories are a testimony to the current widespread public interest in and concern about commercial crime. Scholars attribute this growing emphasis to, among other things, a greater skepticism about the behavior of persons in authority. The alleged crimes of Whitewater involving President Clinton and his associates only deepen the mood of distrust of those in prominent places.

Statistics suggest that there is some reason for distrust. For instance, KPMG Peat Marwick's 1998 Fraud Survey reported that false financial statements caused losses of \$1 million or more in 42 percent of the reported instances, whereas in the 1994 survey, losses of this magnitude represented only 24 percent of the total losses.

While it is true that surveys only deal with reported crime, what is clear is that the extent and value of reported commercial crime is on the increase. Many experts believe that many frauds go unreported and that the extent of unreported commercial crime is also on the increase.

7.1.4 Responsibility for Commercial Crime

Some scholars debate whether individuals should be held responsible for crimes committed on behalf of their organizations. Although some direct benefit accrues to the perpetrator, far more benefit accrues to the organization.

Regardless of whether the organization is held liable, the frauds are a direct result of some human action or interaction: if a business is like a dynamite charge, someone must push the plunger.

Most criminal statutes require that the guilty person have the required criminal intent. However, an organization can be held liable even if it were unaware of or did not participate in the fraud. The law recognizes two theories of organizational responsibility:

1. *The identification theory.* The organization is held liable when the employees and organizations can be viewed as one and the same, for example, a small business owner who has incorporated.
2. *The imputation theory.* The organization is held responsible for the actions of its employees through the doctrine of *respondeat superior*, a seventeenth century doctrine that means “let the superior respond.” The legal theory was developed from civil lawsuits to prevent employers from denying financial responsibility for the acts of their employees.

7.1.5 Characteristics of Commercial Crime

While commercial crime can take many forms, often it is distinguished by one or more of these characteristics: tolerance, diffusion of harm, and rationalization.

Tolerance

While awareness of commercial crime has increased in recent years, there still remains a somewhat greater tolerance for this form of crime as compared to violent crimes such as armed robbery, or those involving drugs. This greater tolerance may stem not so much from the nature of the crime itself, but rather from the perception of the perpetrator as being somehow more *civilized*. Anybody with strength, decent aim, or access to poison, can commit murder, but only a limited number of *respectable* corporate executives or directors are in a position to violate antitrust legislation.

Diffusion of Harm

Another notable characteristic of most kinds of commercial crime is that there are often numerous victims who are frequently unaware that they have been harmed. Death from smog or asbestos poisoning is very likely to be slow and insidious, and its victims will be hard-pressed to relate their terminal illness to its precise cause, given the complicated nature of other possible contributing factors. A factory worker with cancer is not likely to be certain whether it was the toxic chemicals that he handled for fifteen years, the fact that he smoked too many cigarettes, or bad genes or bad luck that will shorten his life.

In many other cases of commercial crime, the harm tends to be widely diffused and, for each person, rather insignificant. But these can still be significant crimes. Companies can earn millions over the course of a year by charging higher prices for products that do not meet the standards they are alleged to attain. Few people who pay for a package of one-hundred thumb tacks will take the time and energy to count the contents of the package to be certain that they have gotten their money’s worth; it would be an easy and safe venture to put ninety-two tacks in each package, and some merchandisers find the temptation irresistible. Similarly, a customer will most likely remain unaware that the gasoline pumps at a service station are calibrated so that they get fewer gallons than those for which they are charged. Even if they come to know about these kinds of issues, most customers would shrug them off as not worth the trouble it would take to do something to remedy the situation; at most, they might take their business elsewhere.

Rationalization

Perpetrators of white-collar crime are known for providing elaborate excuses for their crimes, and the nature of such explanations may be a major distinguishing mark between them and street offenders. It has been posited that embezzlers typically claim that they are only borrowing the money; they intended to repay it once they had covered the bills and other financial demands vexing them. Commercial criminals will similarly rationalize their behavior; for example, antitrust violators usually maintain that they are seeking to stabilize an out-of-control price situation when they conspire with others to fix prices, and they are likely to insist that power-hungry prosecutors and investigators are singling them out.

7.1.6 Investigation and Prosecution of Commercial Crime

The diffuse nature of most commercial crime poses a particular law enforcement dilemma. Without complaining witnesses, policing has to be proactive instead of reactive; that is, the enforcement officials themselves have to decide where the offenses are being committed and how to go about stopping them. Enforcers obviously cannot cope with all the violations and must decide on rules to guide their efforts. Should they go after the behaviors that cause the most harm? Should they take on the bigger offenders, or concentrate on the *smaller fry*, where their chances of success are much better? They can readily accumulate ten convictions in a year against ten insignificant companies, whereas it might take three years to win a victory over one huge corporation. Besides, the resources of the large organization might allow it to win its case, regardless of the lawless nature of its behavior.

7.1.7 Causes of Commercial Crime

Because businesses are bottom-line driven, it has been posited that they are inherently prone to committing crime, yet not necessarily criminal. Without necessarily meaning to, organizations inherently invite commercial crime as a means of obtaining goals. For example, a department manager's concern with reaching assigned goals, may lead the manager to maximize his or her department's own interests to the detriment of the organization, or to the detriment of society as a whole.

Organizations can also be criminogenic—prone to producing crime—because they encourage loyalty. Accordingly, this is because—

1. The organization tends to recruit and attract similar individuals.
2. Rewards are given out to those who display characteristics of *a team player*.
3. Long-term loyalty is encouraged through company retirement and benefits.
4. Loyalty is encouraged through social interaction such as company parties and social functions.
5. Frequent transfers and long working hours encourage isolation from other groups.
6. Specialized job skills may discourage company personnel from seeking employment elsewhere.

These reasons in turn cause company personnel to sometimes perceive that the organization might be worth committing crime for.

Another aspect that makes companies criminogenic is their compensation structures, particularly for corporate executives who are most likely to be the perpetrators of commercial crime. Compensation packages for senior personnel usually include a component based on the results of their company or department, either through stock options or bonuses. Typically, senior executives have a greater amount of compensation tied to results than do other employees. Because commercial crime is so diffuse, and the likelihood of being caught is low, senior executives may perceive that the incentives to “enhance the success of their organization” through commercial crime will outweigh the risks.

7.2 FORMS OF COMMERCIAL CRIME

Today, the realm of commercial crime can be said to primarily involve offenses against laws that regulate either one or both of the following: the marketplace or the established standards of conduct for professional and political life. Some of the most common forms of commercial crime are described in this section, along with Case Studies and other examples that illustrate the salient features of such crimes.

The first two cover *shams*, which Webster’s Dictionary defines as “. . . an imitation or counterfeit purporting to be genuine [*noun*] . . .” and “to act intentionally so as to give a false impression [*verb*].”¹ Shams are the result of the activities of a confidence trickster or con artist who has been able to obtain money from the public by various means. Generally, there are two kinds of shams: corporate shams and investor fraud.

Although these shams are discussed separately in this chapter (due to the size of each section), in many cases the perpetrator (the corporate con artist) and the victim (individuals) of the shams have similar characteristics, as does the way in which the sham is operated. However, they have two major distinctions:

1. In the corporate sham a corporation exists from which the pitch is made. This is in contrast to an unincorporated individual making a pitch, not on a corporation’s behalf, but on his or her personal behalf.
2. In investor sham the nature of what is being *sold* to the victim differs. For example, an investor sham typically involves making a speculative investment, whereas a corporate sham typically involves the purchase of something tangible.

The remaining sections of this chapter include the following kinds of fraud as committed by companies: procurement fraud, industrial espionage, finance fraud, securities fraud, environmental abuse, economic extortion, health care fraud, and possession of property obtained by crime.

7.2.1 Corporate Shams

Corporate shams generally involve something counterfeit or false. In this case the corporate sales pitch appears to offer something genuine, yet there is no underlying substance. The perpetrator of the crime is often a con artist acting through a corporate entity. In fact, by using the *corporate veil* as a shield from the public, the con artist gains an appearance of

¹Merriam Webster’s Collegiate Dictionary, Tenth Edition, 1993.

respectability and substance that he or she would otherwise lack. The con artist's wares may consist of one or more of the following:

- Products oriented to individual consumers (as opposed to products that companies would buy) that are sold by false advertising.
- Franchises or distributorships that the victim purchases in order to run a business.
- Solicitation of money donations towards a charitable or religious cause.

Generally, shams that are carried on through an incorporated business involve pyramid sales schemes, mail order sales, advertising to be placed in charitable programs or flyers, or donations to charitable organizations. Newer forms of corporate shams that are becoming more common are the selling of franchises, and other get-rich-quick schemes, such as the selling of vending or arcade game machines: the purchasers then set up their own business using the franchise or the equipment bought.

When a con artist hides behind a corporate veil, some or all of the following characteristics may apply:

1. The con artist uses expensive letterhead, emblazoned with a worldly name and a classy address, to impress potential victims.
2. The company has a very informal corporate structure, and a very short life span.
3. The company's accounting systems are primitive or nonexistent.
4. The company conducts an extensive and appealing advertising campaign.
5. If a product is offered, the product itself may be of questionable value, and there is seldom, if any, post sale servicing.
6. The customer is expected to pay for the product via cash or readily negotiable checks on (or before) delivery.
7. Once received, the cash is quickly removed from the company through the payment of commission expenses, salaries, bonuses or management fees, so that the con artist can reap the immediate benefits of the scheme.

The key to the corporate sham, as with any sham, is the effectiveness and the speed with which the sales pitch brings results. The method of delivering the sales pitch may range from telephone solicitation (via a boiler room operation), to either cold calls, or advertising in local newspapers, or both.

Possible red flags for a corporate sham include elaborate representations that demonstrate the quality of the product, proposed earnings that are excessively high for the franchise, or an apparently hard-sell pitch to raise money for a purported charitable purpose.

Finally, you should be aware of the arguments put forward by defense counsel in corporate sham cases. Some of the issues defense counsel might raise include:

- *Caveat emptor*—let the buyer beware.
- Some of the money received was in fact directed to the promoted charitable purpose.
- The investor is at fault: that is, for not working hard enough at a franchise operation to make it succeed, or for not waiting long enough to receive the goods that would have eventually been shipped, and so on.

Merchandise Swindles or False Advertising

Merchandising frauds include all frauds perpetrated against purchasers of merchandise and services. If you have ever paid for an item and received something less than advertised, you have been the victim of a merchandising swindle or false advertising.

These frauds generally fall into one of the following four categories:

1. Representations that the purchase is a bargain when in fact it is not—for example, department stores raise the price of a product significantly one day and then the next day drop it back to where it had been, maintaining in their advertising that it now is *on sale*.
2. Collection of money for one product and substitution of another of lesser quality or cost—for example, claims have been made that shoes are alligator when in fact they were made of plastic.
3. Misrepresentations regarding the quality of the product—for example, a company selling glass *demonstrated* in television commercials that its car window product was so perfect that when you looked through it you could hardly believe there was anything between you and the outside scene; it was later proved that the ads were filmed from inside a car with the window rolled down.
4. Failure to deliver the product or service—for example, in bait and switch tactics, stores advertise a specific product at a strikingly low price, but then, when the customer tries to buy the item, it is no longer available. It is the customer's presence and attention they want to attract—once they have him or her listening, they assume that slick sales tactics can accomplish the rest of the deceit.

Defraud You in Writing Case Study

Between September 1997 and June 1998, Smith and Jones, partners of Defraud You in Writing Inc. committed fraud by obtaining funds from the public for goods they did not intend to supply.

Smith and Jones operated the business through telephone solicitation whereby books were offered for sale, and customers' names were entered into a drawing for a trip to the Caribbean via Acme Tours. Door-to-door sales people would follow up on the calls and try to obtain orders for the books. The orders set forth the terms, the method of payment, the time and method of delivery, and an announcement for a drawing on a certain date. The drawing date was inserted in a blank on the order form, the first draw being December 31, 1997.

From the evidence of Mr. Sleuth, forensic accountant, during the period between October 1997 and May 1998, the actual net cash receipts from orders by members of the public totaled \$75,291 (after allowances for returned checks) on 1,867 orders.

Defraud You in Writing's suppliers were not paid during this period, so the total number of orders filled was 311. In fact, during the three months with the largest sales, (December, February and March) no books were ordered from Defraud You's

suppliers. Instead, substantial effort was being made to increase the sales force (and thus the revenue), and new premises were being sought.

The judge in this case believed that Defraud You in Writing used the 311 orders to create a camouflage for the business' real activity: to obtain funds for orders they never intended to fulfill.

As for the drawing, no arrangements had been made with Acme Tours to enable the winner to take the trip.

Franchise and Distributorship Frauds

Both franchise and distributorship frauds are characterized by a *get-rich-quick* business opportunity that involves a large up-front purchase of equipment, supplies, and promotional materials. Many such schemes are part of a pyramid scam.

CookieVend & Run Inc. Case Study

CookieVend & Run Inc. was incorporated in March 1997 to sell cookie vending machines. CookieVend's headquarters were located in New York City. Its office staff generally consisted of the president, general office manager, secretary-treasurer, bookkeeper, and three typists.

Shortly after CookieVend's incorporation, a series of ads were placed in newspapers across the country. These ads offered a substantial guaranteed income, which could be earned for an investment of \$3,000 to \$9,000. Although the ads differed somewhat from paper to paper, they all offered a part-time job that could net the right person an income of \$2,000 per month or more.

In addition to the office staff, CookieVend employed a sales staff of approximately ten people to interview the respondents to the ads. These sales reps traveled independently of each other and were provided with a corporate brochure and other material that instructed them on what to promise the new distributors.

Some 180 people purchased these distributorships for an investment of between \$3,000 and \$9,000 each, depending on the number of vending machines purchased. Supplies of cookies and insurance were also purchased. CookieVend's total sales from April to December 1997 were approximately \$1.2 million.

In the ensuing year, not one distributor was successful in his or her business. The complaints were generally as follows:

1. The quality of the vending machines was very poor.
2. Three distributors never received their vending machines (twenty-three machines in all).
3. Cookies were stale when received by the distributor.
4. The price of cookies increased from fourteen cents to twenty cents each soon after the distributors purchased their machines.

5. The company did not honor claims of damage to machines in accordance with the insurance protection policy on the agreement.
6. The company did not honor its three-year repair warranty on vending machines.
7. The company did not attempt to address any reasonable complaints.

Evidence of Fraud. All of CookieVend's management personnel were found guilty of fraud and received jail sentences. The evidence that formed the basis for the case against them was as follows:

1. CookieVend's revenues and expenses showed that its level of profitability was directly attributable to the sale of machines. This also showed that the sale of cookies resulted in losses, thus CookieVend had a motive to sell machines rather than cookies.
2. CookieVend's primary disbursements were for commissions, advertising, travel, and business promotion. These expenditures occurred during a period when the distributors' complaints about product quality fell on deaf ears.
3. The profit-loss experience of the distributors was much worse than the profit-loss statements represented in the newspaper advertisements. One of the highest performing distributors realized a gross profit, assuming all cookies were sold, of \$375, on an investment of \$7,941 over a period of eighteen months.
4. CookieVend never purchased a liability policy although the distributors' purchase agreements represented that a policy did in fact exist.
5. The distributor agreement set out a nonrescission clause specifically stating, "The distributor is not relying on any oral or written expressions, promises or warranties made by anyone to consummate this transaction."

Charity and Religious Fraud

Jim Bakker, former head of the defunct PTL (Praise the Lord Club) has brought international attention to religious fraud. The essence of his scheme was to sell "lifetime partnerships" in a luxury hotel, which his followers could use for life. Prosecutors were able to show that Bakker's plan was completely unworkable, because many more partnerships were sold than could ever be accommodated. Bakker used the money to pay himself and his lieutenants millions of dollars in salaries and bonuses. He was convicted under federal mail fraud statutes.

Other kinds of charity and religious groups resort to fraud as a way of obtaining *contributions*. In the most common of the schemes, fraudsters operating in boiler rooms call unsuspecting victims and raise funds for allegedly good causes or for worthwhile organizations. The funds collected are not used for their intended purpose, or the fraudsters fail to disclose that they keep the majority of the funds raised for administration costs and give the sponsoring charity or religion only a small portion of the money collected.

Rob M. Blind Case Study

Between January 1997 and July 1998, Rob M. Blind and I. Swindle committed fraud by developing a scheme through the medium of telephone solicitations that induced the public to contribute funds allegedly for charitable purposes—to benefit the blind.

The operation, *Help the Sightless Associates*, carried on by Rob and his associates, was reasonably simple. They hired three or four blind musicians, who joined other sighted employees for a tour of several cities. In each city they planned to visit, they conducted a telephone solicitation campaign: literally by going through the yellow pages and calling every business listed. The firms solicited were asked to buy an ad in a program, which was to be distributed at a concert to be held in that city.

If the firm refused to advertise, it would be asked to buy tickets to the concert that it could use, give away, or allow to be given away on its behalf.

The *Help the Sightless Associates* was not a charitable organization and never applied for registration as such. There is no record of them donating anything to the blind other than paying the musicians who gave the concerts.

As for the dollar amount of the fraud, according to Mr. Sleuth, forensic accountant, the total gross receipts for 1997 and part of 1998 were \$252,327. These funds were used in the following manner:

| | |
|---------------------------------|-------------|
| Payments to the blind musicians | -50 percent |
| Payments unaccounted for | -48 percent |
| Expenses | -2 percent |
| Total | 100 percent |

7.2.2 Investor Frauds

Like corporate shams, investor frauds use techniques designed to produce a quick return or benefit to the company that is the subject of the con. The techniques generally used are telephone solicitation, personal cold calls, or spreading the sales pitch by word of mouth among a particular group of individuals, such as doctors or dentists—who typically have high incomes or high net worth, or both, but possess limited financial or investment expertise. The con artist may succeed in persuading a member of the group to introduce him or her to other members, thus creating confidence in both the scheme and him- or herself. The investors are actively encouraged to spread the word to their close friends about this opportunity for an investment. These activities are often perpetrated through a pyramid or *Ponzi* scheme—both of which are described below.

The key to the con is generally a direct pitch to the investors' greed—that is, promises of high returns within a short period. The scheme may entail investment in precious metals or precious or semiprecious gems, and has been known to embrace items, such as antique coins and commodity futures. Investor frauds have even extended to what is commonly known as flips of real estate.

Although many of the characteristics of a corporate sham discussed in section 7.2.1 apply equally to investor frauds, there are two characteristics that are unique to investor frauds:

1. An extensive and appealing get-rich-quick advertising campaign is conducted, suggesting to the victims that easy money can be made with very little effort.
2. Investors, once the investment is determined to be a con, do not want any publicity that would expose the foolishness of their investment.

Chain Referral (Pyramid versus Ponzi) Schemes

Chain referral schemes are based on the same idea as the well-known chain letter. This is a particular kind of sham, which could involve products, or may involve only investments. In one example of a chain letter, the con artist starts the chain letter by sending a letter to five or more people requesting (on some pretext—often preying on people's superstitions) the recipients to mail money to the con artist. The letter also instructs each recipient to send the letter to a further five people with the request that money be sent to the names in the first two tiers of the pyramid. The third tier recipients in turn repeat the process of mailing the request for money and adding themselves to the bottom of the pyramid. Often there is an instruction that only four or five tiers should receive the money; the top name dropping out with the addition of a new name(s) at the bottom. By the time the chain reaches the seventh or eighth level (if the chain continues that long), the multiplier effect creates enormous wealth to those higher up in the chain, because they receive money from the geometrically growing lower tiers.

Of course, things other than money can be the objects of chain letters. Some involve recipes, Christmas cards, and other harmless items. However, chain letters don't work indefinitely. That is because someone in the lower level inevitably fails to mail out his or her five letters, and the chain is then broken; usually only those in the upper levels profit.

Chain referral schemes, also called pyramids or Ponzi Schemes (after the notorious Charles Ponzi who successfully employed the scheme in the early twentieth century), are based largely on the same principal. The difference is that some are legitimate and some are not. Pyramid sales structures are generally legitimate, and Ponzi schemes are usually illegitimate.

For example, many products sold exclusively in the home, such as Amway merchandise, can be legitimate forms of pyramids. Individuals are recruited to sell merchandise. They in turn recruit their friends and colleagues to sell, and get a cut of their commissions. This recruitment continues on down, with those in the upper levels receiving a portion of the commissions from several different layers of sales personnel. However, because of the turnover in sales personnel, most people fail to achieve a sufficient level in the chain or pyramid to make the touted commissions. They often get discouraged and quit, further depressing the chain.

Illegal pyramids (Ponzi Schemes) exist as well. One common variation is for a fraudster to place mail order ads promising wealth to individuals for performing work in their homes for services such as stuffing envelopes. When the victim responds to the ad, they are informed that the *opportunity* requires sending in money. In return, he or she receives a letter suggesting the victim place a similar ad and collect money in the same way, using the same letter. In other words, the fraudster is telling the victims in effect, "do the same thing to others that I just did to you."

Another typical Ponzi scheme involves the diversion of investment funds. This fraud works as follows: A company will open its doors as an investment firm, promising better than average returns on its investment. When the company receives money from investors A through G, the money is diverted to the personal benefit of the principals. When additional money is received from investors H through L, those funds are used to pay off investors A through G. When funds are received from investors M through Z, this money is used to pay off investors H through L, or at least to pay interest, and so on. The money paid out to the early investors, therefore, is not from returns achieved on investments, but rather a diversion of new investments. This pyramid continues until the scheme collapses.

Many operators simply set up a mail or telephone operation, collect funds, then close the operation and move, only to reestablish a similar operation and repeat the scheme. Law enforcement officials acknowledge a significant problem with chain referral schemes, but readily admit that they are incapable of adequately controlling the problem.

These schemes, or variations of them, cannot go on indefinitely because they require a constant stream of money to cover the diverted funds. When the flow of new investments fall below that level, there is insufficient cash to pay off old investors, and the scheme collapses. The chain referral schemes are not dependent on a particular product or service, but rather on the method of diverting funds. Common chain investment schemes include franchising, sales distributorships, investment and securities of various kinds, and merchandise.

Finally, it should be noted that many chain referral schemes involve small amounts of money that are taken from many victims. Because victims typically feel foolish about being fleeced, they frequently do not file charges. And even when complaints are made, the police do not give these crimes priority because of staffing and budgetary commitments. As a result, many chain referral operators stay around a long time.

7.2.3 Finance Fraud

False Mortgage Security

False mortgage security is a term used to refer to security that turns out to be nonexistent or to have a value far lower than was represented. This is a kind of loan fraud whereby the perpetrator is usually an individual acting through a sham corporation, and the victim could be a bank, but is more likely an individual or another corporation.

The usual characteristics of false mortgage security fraud are as follows:

- An investor is persuaded to make a loan or invest funds on the assurance that repayment of the loan or investment will be fully protected and secured in some way.

- When the touted investment fails to materialize, the investor discovers that the assets supposedly securing the investment do not exist, are worth much less than the investor had been led to believe, or were pledged to numerous other investors rendering them virtually worthless.
- The investor is often a financially unsophisticated individual who does not review the transaction papers in detail and may not understand them but is persuaded to invest by the prospect of a high return (for example, a well above average interest rate).
- The investor usually relies on the promises of the perpetrator or the apparent protection afforded by the security.

It should be noted that some assets pledged as security (that is, land or stock) may lose value for legitimate reasons such as fluctuations in their market values. In cases of false security, however, there is intent to deceive on the part of the person soliciting the funds.

Accounting evidence in most cases can establish and document the funds' flow in situations of this nature. It is more likely that evidence establishing the intent to deceive will be obtained by conducting interviews (*viva voce evidence*) than through the analysis of the accounting records. It is often through the interview process that the true nature and intent of the transactions are revealed. The nature of the documentary evidence required to establish the economic benefit to the fraud perpetrator, and to trace the flow of funds are dictated by the nature of the fraud scheme.

Trust Our Paper Inc. Case Study

Trust Our Paper Inc. commenced its syndicated mortgage program in 1995. The program expanded rapidly, particularly during 1998, to include loans for property development in Plainville. The company solicited—in appropriate private offerings—funds from the public for investment in specific mortgages, with certain representations made about the nature of each loan and the mortgaged property. Unbeknownst to the investors, the mortgaged property was not as marketable or valuable as had been represented because it did not have the necessary local governmental approval for development.

During 1998, the period of its most rapid expansion, Trust Our Paper experienced an increasingly severe negative cash flow from operations. This condition persisted until March 1999, when Trust Our Paper went into receivership primarily as a result of—

1. The apparent inability of the mortgagors (borrowers) to make interest payments.
2. The apparent inability of the mortgagors to pay principal amounts upon maturity.

In reality, the face amount of the mortgages were much higher than the underlying value of the property secured by the mortgages.

The problems in this case are best illustrated by a transaction that commenced in the summer of 1998, when Trust Our Paper purchased land in Plainville at a price of \$400,000. It planned to build a 300-suite apartment complex on the land. Before

the closing of the transaction, Trust Our Paper had been unsuccessful in obtaining mortgage financing through normal channels because of an inability to get zoning approval for its plans. The location of the land and environmental concerns proved to be insurmountable obstacles.

Trust Our Paper then provided a loan of \$1 million to ABC Developments Ltd., the developer of the property, secured by a first mortgage on the property. Funds were solicited from the public—in a properly registered offering—for investment in this mortgage. Trust Our Paper represented to the investors that it had used the mortgage proceeds for interim construction of a 300-unit residential complex.

However, an examination of the mortgage proceeds revealed a different story. Out of the proceeds, \$400,000 was used to reimburse Trust Our Paper for the cost of the property. Thus, the purchase was financed entirely by the investors through their loan to Trust Our Paper. Of the remaining funds, \$115,000 was disbursed in November 1998 to Green Investments Inc., a troubled company with a deficit of \$296,000. The balance of \$485,000 was disbursed in a similar manner.

The underlying security given to the Trust Our Paper investors was highly questionable in light of the following:

1. The mortgage for \$1 million was on land purchased for \$400,000.
2. The mortgage guarantor advised that the property was unsuitable for financing.
3. The property remained undeveloped.
4. The developers were unable to obtain alternate mortgage financing.
5. The mortgage proceeds were not used as purported.

Thus, the proceeds raised from the public offering were diverted from their intended use, that is, to develop the property. This diversion diluted the value of the security and jeopardized the achievement of the appraised potential that was offered as security.

Advance Fee Fraud

Generally, advance fee schemes involve paying bogus corporations an up-front finder's fee in exchange for a promise to receive an advance on a loan. The victims of these kinds of schemes can be both individuals and corporations. Often if an individual is seeking loan funds but for whatever reason cannot obtain funding from traditional sources, he or she will turn in desperation to these fraudsters.

Once the fee is paid, the perpetrator disappears. In some cases, desperate institutions are offered access to illegal money, and they typically do not report the loss of the advance fee when the deal falls through. General characteristics of these schemes include one or more of the following:

- Deals too good to be true often are not true.
- The agent requests documents on bank stationery, or signatures of officers, or both.
- The bank is asked to give nondisclosure agreements to protect the agent or other parties.

- The agent asks for an irrevocable agreement to pay commissions, expenses, and a fee.
- There are several complex layers of agents, brokers, and other intermediaries.
- The perpetrators often describe the offerings as special *one of a kind* offers and state that the deal will be *killed* if anyone is contacted to verify the deal.
- The deal often involves foreign agents, banks, and other sources, such as an unnamed wealthy person or government.

Debt Consolidation Schemes

People who find themselves hopelessly in debt frequently turn to debt consolidation agencies out of desperation. Debt consolidation agencies do not advance loans, but rather act as an intermediary between the debtor and creditor. Some are legitimate, but many are not. Bona fide debt consolidation agencies make money by organizing the debtor's affairs and collecting a percentage of the money handled on the debtor's behalf.

In the typical scenario, the debtor contacts the consolidation agency, and provides a complete list of their creditors and the amount of monthly payments currently owed. The agency then usually writes letters to the creditors, requesting a debt work-out plan providing for lower monthly payments spread out over longer periods of time. The creditors are often motivated to accept the arrangement provided they think that the entire debt, or the major portion of it, will be repaid or that the debt consolidation plan will prevent a bankruptcy filing or default by the debtor. The debtor then makes a lump sum monthly payment to the consolidation agency, which then distributes the money to the creditors.

Unscrupulous debt consolidation schemes are perpetrated when the agency collects money from the debtor but does not forward it to the creditor. In some instances, it is months before the debtor finds out that the money has been misappropriated. The victim debtor has not only lost money to the unscrupulous agency, but still owes the original debt.

Bankruptcy Fraud

Bankruptcy is designed to give every corporation or individual encumbered by mountains of debt a *fresh start*. In a liquidation or Chapter 7 bankruptcy, all assets and liabilities are to be listed on the bankruptcy petition and a trustee is appointed by the U.S. Bankruptcy Trustee's Office in the district where the petition was filed. The role of the trustee is to liquidate the assets of the estate and distribute the funds to the creditors pursuant to the Bankruptcy Code.

Generally there are three common kinds of fraud committed by companies or individuals filing for bankruptcy; they are:

1. *Fraudulent conveyances*. Prior to the filing of the bankruptcy petition, cash or other assets are transferred to friends, relatives or business associates. Once the bankruptcy court has discharged the debtor's debts, these assets are then transferred back to the debtor. This kind of transfer is often referred to as *parking assets*. These prepetition transfers are often disguised to appear as bona fide business transactions.

2. *Concealing assets or asset stripping.* The debtor could: convert assets to his or her own benefit, simply fail to disclose certain assets in the bankruptcy schedules, or deny the existence of such assets when meeting with the trustee or at hearings before a bankruptcy judge.
3. *Planned bankruptcy.* The debtor's affairs are structured in a way that gives the appearance of a failing business, but is actually a lucrative business that needs to avoid the circumstances of a particular obligation, litigation, or labor dispute. This is often accomplished through the use of transfer pricing or management fees from related companies, which may or may not be disclosed to the trustee.

Planned Bankruptcy. Bankruptcy can be attributed primarily to one or a combination of the following causes:

- Incompetence of management
- Lack of managerial experience
- Neglect
- Severe economic recession or depression (macro or market sector)
- Disaster
- Fraud

Fraud is *not* the cause of most business failures.

The victims, regardless of the cause of a business failure, are customers and creditors: customers who have ordered or paid for goods that are undelivered at the time the business *goes belly up*, and the various creditors of the business that remain unpaid at that time. On many occasions the employees are also victimized because they lose their jobs or are unable to collect unpaid wages or both.

A business experiencing financial difficulties can pursue several remedies either to rectify the situation or to conclude the operation of the business. The owner may cease business voluntarily, or an unpaid creditor may precipitate the closing down of the business through the initiation of involuntary bankruptcy proceedings.

Ask the following questions when considering whether a bankruptcy was planned:

1. When did the company realize it would fail? A business failure may appear to be the result of management incompetence, inexperience and neglect. Notwithstanding the reasons for the financial difficulties, it is crucial to establish whether management carried on the business after a point in time when they knew, suspected or should have known that business failure was imminent. In that case, the fraud occurs when they solicit funds from the public, including creditors, in spite of knowing or suspecting that the company might be unable to fulfill the representations and commitments made. The business, however, may have continued in the honest belief that it would turn around (the *rainbow syndrome*).

Establishing the point in time at which management knew, should have known, or suspected that business failure was imminent requires a detailed review and analysis of the financial position of the business. Financial statements, accounting records and banking records have to be scrutinized. (See Chapter 10 for further information on financial statement fraud.) The examination would disclose not only the financial position and any deterioration in it, but also the level of management's

knowledge about the situation. Correspondence and other documents from customers and creditors, expressing concern or demanding delivery or repayment, together with viva voce evidence may also be useful.

2. Did the company pursue remedies? In determining whether fraud exists, the forensic accountant must consider whether the remedies available to the business in financial difficulty, as noted above, were pursued. In addition, the accountant must ask if honest attempts were made to resolve the difficulties or merely to give the impending business failure the appearance of legitimacy.
3. Has the business committed an act of bankruptcy? Bankruptcy law defines specific activities on the part of a debtor as constituting an act of bankruptcy. These activities include one or more of the following:
 - The transfer of assets to a trustee or other third party for the benefit of creditors
 - A payment to one creditor in preference over another
 - The fraudulent conveyance or transfer of property
 - An attempt by the debtor to abscond without paying debts
 - A failure to redeem goods seized under an execution order issued against the debtor
 - The presentation at a meeting of creditors of a statement of assets and liabilities indicating insolvency, or a written admission of the debtor's inability to pay his or her debts (the filing of a bankruptcy petition), or both
 - An attempt to move or hide any of the debtor's property
 - Notice to any creditors that the debtor is suspending payment of his or her debts
 - A failure to meet liabilities, generally, as they become due
 - Default in a proposal made as part of the bankruptcy proceedings
4. Was the business failure planned? A planned business failure occurs where management has converted the assets of the business to its own, that is, personal benefit and then tries to conceal the conversion through formal bankruptcy proceedings. In addition, the debtor induces vendors to sell goods on credit when the debtor knows that it has neither the intent nor the capacity to pay the creditors. Characteristics of a planned failure include one or more of the following:
 - The business has developed a reputation for trustworthiness in the business community. This reputation may have a short history, and may have been established for the express purpose of inducing companies to sell goods to the business on credit.
 - The business sells tangible and highly marketable products.
 - The business seeks to sell, or convert the goods to cash as quickly as possible with little care about the selling price because they have no intention of paying the suppliers for the goods.
 - The proceeds from operations are moved out of the business so as not to be identified as an asset of the business at the time of the filing of the bankruptcy petition.

- The business has little net worth.
- The business has not been a financial success.
- The business departs from its normal business practices with regard to purchasing, payments to suppliers, sales, and the granting of credit to customers.

The typical changes in business conduct of a planned failure include:

- The volume of inventory ordered from existing suppliers increases significantly. The suppliers will probably extend credit up to sixty days, largely as a result of their wish to retain the customer and the established reputation of the company.
- The unsuspecting suppliers will receive little or no payment. They may receive payment for the initial order but not for subsequent shipments. The scam will probably be completed within sixty days of the date of purchase of the inventory. After that time, the suppliers are likely to become suspicious and might take action of some kind.
- The company will refuse to sell the inventory to its customers on credit; that is, it will sell on a cash-on-delivery (COD) or other cash-up-front basis only. To get customers to pay cash, the selling price per unit is commonly at or below the company's cost price per unit, as shown on the supplier's invoice.
- If inventory still remains after the company has approached its usual customers, the inventory may then be offered to new customers. These sales tend to be non-arm's length and may be in cash. Although the sales invoices may indicate the payment was made in cash, the deposit of the cash into the business' bank account does not necessarily follow.
- If, after all these efforts to sell, inventory is still left at the site, it can be physically removed. The trail will be covered to prevent obvious detection.

A planned bankruptcy is designed, of course, to benefit those in control of the debtor entity. The fraudster will make every effort to ensure that no trail is left behind to enable the trustee in bankruptcy to retrieve the proceeds of the fraud and return those proceeds to the creditors. The techniques employed to block the path of the trustee are limited only by the perpetrator's imagination and will vary according to the circumstances.

7.2.4 Arson for Profit

Arson and a planned bankruptcy share some similar characteristics. In both situations, business problems exist and are acknowledged to exist by management. Arson, like planned bankruptcy, can become the means of a criminal making the best of a bad situation. The perpetrator will, of course, seek to commit the crime without leaving a trail of criminal conduct.

The following are the chief characteristics of cases of arson:

1. The fire is of an incendiary nature.
2. An insurance policy is in force.
3. There is a financial or other business-related motive.
4. The financial motive may not be readily apparent.
5. Exclusive opportunity to commit arson may or may not be evident.

6. The prosecution's case will often be based on circumstantial evidence.
7. Efforts may have been made to destroy some or all of the accounting and business records.

Without a confession or an eyewitness, the evidence in a case of arson is almost always circumstantial in nature. The prosecutor usually must depend on circumstantial evidence, which must be sufficient to rebut every reasonable hypothesis other than a willful and intentional burning. However, evidence supporting the incendiary origin of a fire is often interwoven with other evidence that tends to connect the accused with the crime. The connection to the accused is often the presence of a motive and the opportunity of the accused to perform the act.

Historically, insurance companies have been reluctant to challenge the veracity of loss claims arising from major fires that have damaged or destroyed commercial, industrial, recreational or residential establishments. The reasons given for this reluctance include the following:

- Court proceedings are protracted and expensive, and the ultimate decision is often favorable to the insured.
- The insurance company (like a bank) is often perceived as the *big, bad guy*, thus, the insured sometimes gets the benefit of reasonable doubt because they are perceived as the *little guy*.
- The punitive damages awarded to a claimant often far exceed the loss claim if the courts feel that there has been an unreasonable delay.
- The only evidence is circumstantial.
- The alleged arsonist has been acquitted in a related criminal proceeding.

Accounting Issues and Evidence

The forensic accountant in arson-related matters should differentiate the business position of the company and its owners from the financial position. Although the financial position may have a considerable bearing on motive, motive is better understood in the context of the business itself and the owners, through an overview of all aspects of the operations and ownership of the business.

Ultimately, the financial analysis is designed to determine the *mindset* of the company, the *money* of the company, and the *worker* in the company. Accordingly, it is usually appropriate to obtain as much background information as possible. A starting point may be the acquisition of a business or the commencement of a new business venture. A review of the annual financial statements and associated working papers will disclose the company's yearly performance and any underlying business problems. Motive not apparent from an analysis of the company's financial transactions may become apparent from an investigation of the social relationships found within a business.

Any review of the status of a business must be objective. It should identify not only matters that are unfavorable to management and the owners of the company, but also matters that are favorable. The unfavorable matters may well be obvious, for example, a steady decline in sales, worsening creditor relations, or a significant withdrawal of funds immediately before the fire. On the other hand, an owner may have put a substantial amount of his or her own money into the business shortly before the fire.

Accounting evidence is likely to be extremely significant in establishing motive. The fire may have destroyed some or all of the accounting and financial records, as well as correspondence and file material that could have a bearing on the case. These records will have to be reconstructed to the extent possible; thus, third-party documentation will have to be obtained and interpreted.

Issues and Sources of Information. A review of several recent judgments shows that the main characteristics in an arson investigation to consider, investigate, and establish in evidence are as follows:

1. Ownership, including business structure, style, and relationships
2. Financial motive, that is the financial position of the owners and business, and existence of an insurance policy
3. Current events at or around the time of the fire, including the establishment of exclusive opportunity, and the origin of the fire as incendiary

Information will be sought from people directly and indirectly connected with the business, possibly including its bankers, lawyer, accountant, customers, suppliers, insurers, government agencies, and realtors.

The owner should always be given the opportunity to volunteer any personal or business records that he or she might have.

See below for a list of questions to consider and documents to examine.

Accounting Evidence. Forensic accountants can assist by investigating several issues, in particular those involving ownership and financial motive. They can analyze information from several sources and construct a chronology of the financial events leading up to the fire. They can analyze the financial records of the owner, the business, and third parties, and demonstrate the company's position at the time of the fire, comparing it with earlier periods.

The forensic accountant looks for significant detail when attempting to determine whether a financial motive exists. If little or nothing is available in the way of accounting books and records and supporting documentation, the forensic accountant will pursue other third party sources to secure information for the examination.

Obviously, any financial and accounting records of the business that are available will have to be examined and analyzed. As previously noted, it is important to provide the owner the opportunity to volunteer whatever personal or business records he or she has. Beyond this, the forensic accountant will seek information from others directly or indirectly connected with the business.

Key questions to consider include the following:

1. What financial condition was the business really in?
2. Who maintained the accounting records?
3. What accounting records would have been available?
4. What is the ownership structure?
5. Is the financial position of the owner solid?
6. What was the business's cash flow?

7. Does the business support the owner?
8. Does the owner support the business?
9. Have the essential matters been established?
10. Is the potential defendant cooperative?
11. What is the history and pattern of earnings?
12. Could ownership benefit from *selling out* to the insurance company?
13. What did the owner know about his financial state at the time of the fire?
14. Did any significant events occur at or around the time of the fire?
15. Who are the major suppliers and what were the business' relations with them?
16. Who are the major customers and what were the business' relations with them?
17. Who are the bankers and what were the business' relations with them?
18. Who is the external auditor?
19. Who is the outside legal counsel?
20. Is the business for sale and are negotiations currently being conducted?
21. Have there been any recent changes in insurance coverage?

Third-party documents to investigate include:

- Government (usually the Secretary of State of the state of incorporation or of a state in which the corporation is registered to do business) business registration records
- Recorded documents (for example, for land or other property)
- Work papers and files of accountants, auditors, or both
- Any secured transactions registered under the commercial code of the relevant state
- Tax returns
- Correspondence with customers and suppliers
- Bank credit files
- Credit files from other creditors
- Bank statements, canceled checks, deposit slips, credit memos, and debit memos (paper or microfiche records)
- Payroll information
- General ledger records
- Real estate listings

7.2.5 Procurement Fraud

All organizations including manufacturers, financial institutions, governments, and retailers, as well as private individuals are involved in the procurement process to acquire goods or services. For each and every kind of purchased item, ranging from commodities and equipment to a professional's time via a consulting services contract, there is a different kind of procurement fraud that can be perpetrated by the provider of the goods or services.

The risks and warning signs associated with each kind of procurement fraud vary depending on what is being purchased, and also by the kind and stage of the procurement process: Questions to ask when examining procurement fraud include:

- Is the purchase competitive or noncompetitive?
- What pricing method was used: fixed fee, cost per unit, cost-plus, or a combination thereof?
- Did the fraud occur at the requirements definition stage, the bidding and selection stage, or the contract performance and evaluation stage?

Some of the more common kinds of procurement fraud include:

- Bid rigging or price fixing
- False invoices
- Inflated costs
- Product substitution
- Secret commissions and kickbacks

Bid Rigging or Price Fixing

Bid rigging or price fixing, is the process of setting the price or terms of the contract between the various bidders without the knowledge or consent of the purchaser.

For example, bidders on a highway construction project may secretly meet before bids are submitted. During their meeting, they decide who will submit the low bid and what the bid should be. They may also decide who will bid on what jobs. This is known as bid rotation.

Bid rigging is usually characterized by the lack of *independent* competitive bids, or by prices that are close together. The entity seeking the bids is victimized by having to pay higher prices than the amount that would have been charged had there been no collusion.

False Invoices

Invoices submitted by a contractor for goods that have not been delivered, or for services that have not been performed are false.

Inflated Costs

Contractors often use a pricing method in which they invoice on a cost-plus basis. That is, the contractor receives payment for the actual cost of the job, plus a certain profit based on a percentage of the costs. Clearly, the successful bidder has a vested interest in keeping the costs high: the higher the cost, the higher the profit.

Typically, in order to obtain inflated profits, contractors falsify the cost of the product or service. This can be done through simple or complex means. Examples of the former include adding labor charges for nonexistent (*ghost*) employees or adding charges for materials not actually used. In the more sophisticated schemes, the costs are inflated through overhead allocations.

Product Substitution

Procurement contracts sometimes call for very exacting specifications on the materials used on the job. Contractors frequently believe the contract specifications are too rigid and, therefore, feel justified in substituting a less costly product or service, and keeping the difference.

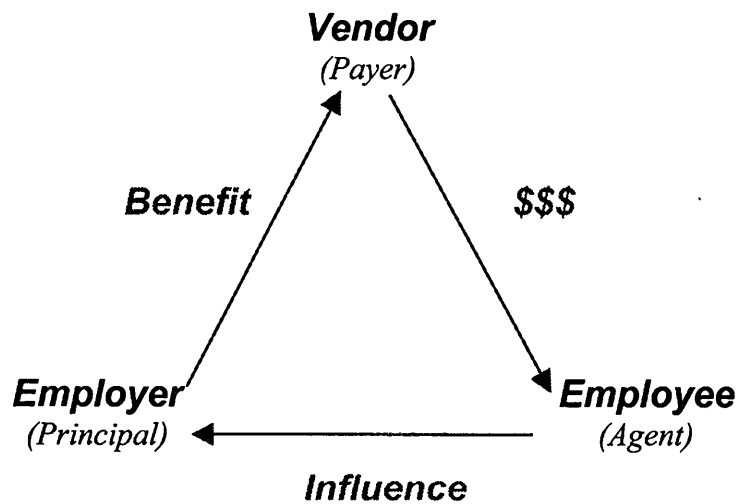
In one scheme, a contractor bid on a new runway for an airport authority and won the bid. The contract called for the depth of the concrete covering the runway to be a certain minimum. After hearing rumors from competitors that the contractor was pouring less concrete than the minimum, the authority's auditors checked the work orders and discovered that the paperwork reflected the concrete depth to hundredths of an inch. The auditor reasoned that concrete could not be poured so exactly, checked the actual work, and found the depth to be less than the contract specifications. The auditors concluded that the contractor was submitting false reports to the airport authority, and was reaping excess profit because it was supplying less material than that called for in the contract.

Secret Commissions and Kickbacks

Secret commissions and kickbacks are one of the most common forms of procurement fraud, and also one of the most difficult to detect. It involves the receipt of a secret payment, usually from one company (the vendor-payer) to a corporate executive (the agent) of another company (the procurer): the agent then exercises influence on the decision-making of his or her employer in a way that favors the vendor-payer. For example, a vendor submits false or inflated invoices for payment, which the procurer's corporate executive knowingly approves. This process is often described visually by the triangle of dishonesty shown in figure 7-1.

The key point to note is that secret commissions and kickbacks are a kind of fraud that generally accompanies other forms of procurement fraud (such as those described in this section).

Figure 7-1. Triangle of dishonesty



7.2.6 Organizational Bribe Giving

The two main kinds of bribes that benefit organizations are:

1. Bribing politicians and giving illegal campaign contributions.
2. Implementing commercial bribery as related to procurement fraud. Also included here are bribes for industrial espionage—that is, paying someone to reveal trade and other secrets about competitors.

Political Bribery

There are three generally recognized characteristics of political bribe giving:

1. Government benefits are often extremely valuable (or, for penalties and sanctions, very costly), but the demand for benefits can exceed the supply.
2. The government is the sole purveyor of the benefits and sanctions; you must do business with the government.
3. The bribe is an attempt to both bypass and guarantee the result of the normal processes, which are often lengthy, costly, and uncertain in result.

The most common form of political bribe giving is illegal campaign contributions, which have made headlines during the Clinton Administration.

Paying foreign politicians and governments was (and perhaps still is) common in order to conduct business in many countries. Since the mid-seventies, when the Foreign Corrupt Practices Act was enacted, paying bribes to foreign officials except in cases of national security has been unlawful.

Commercial Bribery

Commercial bribery involves making payments in exchange for the award of a contract, for industrial espionage, or for both.

In the triangle of dishonesty, a payment from a vendor to an employee would encourage the employee to influence the decision regarding the recipient of a lucrative contract.

Several federal and state laws address the practice of commercial bribery. Both the act of asking for or the making of a payment constitutes an offense. In some instances commercial bribery may also be a violation of the restraint-of-trade laws. For example, certain industries—notably the liquor industry—are specifically prohibited from paying for business. Over the years, many well-known, major businesses have been guilty of commercial bribery (a listing of names would not add learning other than the giants of industry are involved from-time-to-time in nefarious activities).

Industrial espionage can involve direct payments to third parties to secure valuable competitive information. It can also be accomplished indirectly, for example, through the hiring of a competitor's employees. In one case, several U.S. military procurement agents were charged with giving defense contractors information on more than \$500 million in Navy purchases that were going to be the subject of the competitive bidding process.

7.2.7 Industrial Espionage

Industrial espionage is a term that is broadly applied to activities whose main purpose is to obtain information or related assets from competitors or potential competitors. The classic forms of industrial espionage are trade-secret theft and copyright piracy.

Trade Secrets

There are three basic elements to a trade secret: novelty, value, and secrecy. Secrecy, concerns whether an organization handled its alleged *secret* in a protective manner. If a judge deems that an organization failed to protect a secret, that organization will not win judicial support if it charges an employee with theft of that secret.

Patent laws seek a compromise between capitalistic self-interest in a trade secret and social well-being by granting a seventeen-year monopoly to developers of innovative ideas. The U.S. Supreme Court, in its only ruling on trade secrets (*Kewanee Oil Co. v. Bicron Corp.*, 1974), declared the likelihood “remote indeed” that a company would not patent valuable information that it had developed. However, the Court overlooked the advantage, well-known to most companies, that trade secrets can be hoarded far beyond the seventeen-year patent limitation, a matter well documented by the success and secrecy of the formulas for Coca-Cola and Kentucky Fried Chicken, among others.

Leakage of trade secret information is said to be particularly likely from employees who go to work for competitors, careless secretaries, gregarious field sales personnel, and high-tech computer whizzes who often are more loyal to their equipment than to their fellow employees or employer. Temporary help is regarded as especially vulnerable: these employees do not have any company loyalty and can be planted for purposes of trade-secret theft. Sharing sensitive information among two or more individuals, neither of whom knows the full *secret*, is one way to reduce the possibility of compromising sensitive information. Another method can be used to protect mailing lists. By including at least one decoy address in a list, if the list is compromised, whoever uses it will be sending material to a fictional person at an address that actually is the list-owning company’s mail drop.

A review of court cases on trade-secret theft shows that defendants are typically smaller corporations that have hired scientists from larger organizations where they had previously worked for six to ten years. There also appears to be an unusual amount of trade-secret theft from family-owned businesses. The defendants in these cases claim that because they were outsiders, they believed their chances of advancement were hopeless, so they stole the proprietary information to benefit (ingratiate themselves with) their new employers.

Copyright Piracy

Copyright piracy is defined as the infringement of another’s copyright or other business rights. It is an activity usually undertaken by manufacturers, wholesalers or retailers that do not have any legal right to manufacture or copy the product, but who want to earn a quick profit (greed motive) or to ease a financial difficulty (need motive).

Bigtown Video Case Study

From August 1997 to May 1, 1998, John Smith was the owner, principal shareholder, director, president, and general manager of Bigtown Video Inc., a video store with three retail outlets. During this time Jack Brown was also a shareholder and secretary-treasurer of the company.

Bigtown Video's business included the sale and rental of prerecorded videocassettes as well as the sale of blank cassettes. The videotapes sold and rented by Bigtown Video fell into two categories: legitimate and "counterfeit." The legitimate tapes were obtained from sources authorized to manufacture and distribute the tapes in compliance with all copyright and distribution rights. They were packaged with stylized printed jackets showing the nature and content of the particular film. The counterfeit tapes had been duplicated from legitimate tapes, many of which had not yet been released to the public in videocassette form. The packaging of the counterfeit tapes was like that of a blank cassette package with the title of the film handwritten on the side panel. The legitimate tapes were displayed in the front of the stores. The counterfeit tapes were kept in the back rooms of the stores in a closet or in a drawer.

When cross-examined at trial, Mr. Brown testified that he and Mr. Smith had jointly decided to deal in counterfeit videocassettes in late 1997. The decision was made as a result of customer demands and financial difficulties. Mr. Brown would buy counterfeit cassettes from various sources and make duplicates of them. These actions were done with Mr. Smith's knowledge and consent. Mr. Smith rented the counterfeit videocassettes at rates of \$5 or more and sold them for prices ranging from \$60 to \$100 or more. From January 1998 until May 1998, the gross profit made by the company from each of the three stores was approximately \$1,500 per week, of which about 60 percent was attributed to the distribution of the counterfeit videotapes.

In Mr. Smith's cross-examination, he revealed that he was fully aware of the illegitimate origins of the counterfeit videocassettes supplied to him and that neither he, his suppliers, nor Bigtown Video had the right to distribute, rent or sell the cassettes. Mr. Smith knew that by dealing in these counterfeit tapes he was effectively depriving their owners of copyright and distribution revenues, which they would otherwise have been likely to earn but for the use of these illegitimate tapes: he was prejudicing the economic interests of the real owner. Mr. Smith made no attempt to contact the owners of the copyright or distribution rights in order to contribute revenues for his counterfeit use, to obtain these rights, and he had no intention of so doing.

Bob Green, a vice-president at Star-Studded Studios, testified about the effect of pirated videocassettes on the revenues of his company. He focused on four areas of impact and said:

1. That the inferior quality of pirated or counterfeit videocassettes tends to provide the viewer with a poor opinion of the film and the consequent negative publicity is harmful to the theatrical market.

2. That people who have seen a counterfeit videocassette are unlikely to buy the legitimate cassette upon its release.
 3. That for extremely high-grossing films, much of the profit arises out of repeated viewings of the film by the public. The effect of a counterfeit videocassette in such a situation is to diminish the theatrical value of the film by eliminating the possessor's desire to return to the theater.
 4. That with respect to distribution in other territories, the markets for legitimate cassettes have vanished due to the heavy influx of counterfeit videocassettes in those territories. In cross-examination Mr. Green admitted that he could not quantify the loss of profit by theatres from counterfeit videocassettes, nor could he reliably estimate the extent of loss for a given film or a given year.
-

7.2.8 Securities Fraud

There are four main kinds of securities fraud that fall within the category of commercial crime:

1. Knowingly providing misleading or false information in financial statements of a traded business enterprise. (See Chapter 10 for further information on financial statement fraud.)
2. *Churning*: An activity of brokers who buy and sell their clients' securities for the sole purpose of generating commissions.
3. Mixing (commingling) of funds.
4. Manipulating the market for a stock by altering the stock's price through influencing the factors that affect the market price or by controlling the pool of shares available for sale or purchase.

Misleading or False Financial Statements

In large companies, upper level management, whose intent is not necessarily to steal, often manipulates financial statement information. These managers wish to manipulate data to enhance profitability and thereby earn higher bonuses, or to impress the brass at headquarters, or to impress stockholders or lenders, or simply to comply with the goals imposed by senior management. In small companies, where false financial results can create a direct benefit for senior management, the intent of management is often sinister.

Intentionally falsifying financial statements can be accomplished by one of the following methods:

1. Misstatement of financial information by arbitrarily raising profits or lowering costs using techniques such as plugging sales or ending inventory, incorrectly capitalizing current expenses, deferring necessary repairs, falsifying sales invoices, and altering cost invoices.
2. Misrepresentation or omission of significant information.
3. Misapplication of accounting principles.

In the MiniScribe fraud, the company knowingly inflated inventories to deceive the auditors as to the value of assets on hand; the primary goal was to maintain and drive the share price of the company up in the public market.

In more recent instances, particularly in the high tech environment, *channel stuffing* (that is, just before year end, shipping inventory to distributors and dealers whether or not ordered, and booking the shipments as sales) was a popular method used to inflate sales to achieve projected and expected revenue goals. In many instances, product recorded as sold was returned shortly after year-end.

Heinz Catch-Up Case Study

Heinz has been a household name representing quality food products for more than one hundred years. The company had been well managed, profitable and socially responsible. But in the late 1970s, it received considerable unfavorable publicity for accounting irregularities. Some of its profit-center managers engaged in reducing its profits to create a cushion for the next year. The total amount of these pseudo-profit reductions was quite small (\$8.5 million) when compared to overall sales (\$2.4 billion). However, annual sales and profits were not what were reported to the IRS, the Securities and Exchange Commission (SEC), and company stockholders.

The disclosure of these irregularities occurred as a result of an antitrust suit brought by Heinz against Campbell Soup. In Campbell's discovery efforts, it snagged evidence that Heinz' advertising agency was billing for services that had not yet been rendered. When a Heinz executive was questioned about the matter, he pleaded the Fifth Amendment.

The antitrust suit was settled shortly afterwards, but the disclosure caused Heinz headquarters' personnel to launch an investigation into the accounting practices of several subsidiaries. Being highly decentralized, headquarters' personnel claimed they were unaware of the lower-level fudging. Headquarters monitored performance through budget forecasts of sales and expenses and an incentive compensation plan that paid off if high-end profit goals were met. Headquarters also monitored consistent growth in profits. Top management was committed to that overriding goal and, the company's earnings did rise consistently: for example, 1978 marked the fifteenth consecutive year of record profits.

Heinz had an explicit policy that prohibited its divisions from having any form of unrecorded assets or false entries in its books and records. And Heinz didn't measure short-term performance alone. The top nineteen executives, including division general managers, had long-term incentive plans in addition to the one-year plan.

What existed here initially were income transferals aided and abetted by vendors who supplied invoices one year for services that were not rendered until the next year. When that wasn't enough, false invoices were submitted one year and then reversed in the following year. But the amounts involved did not have a material effect on the company's reported profits.

Strangely, the problem at Heinz started in 1974 when it appeared that profits in the Heinz USA division would exceed those allowed by the wage and price controls in effect at the time. World headquarters sought a way to reduce the division's profit. Losses in commodity transactions did not reduce profits enough, so the division booked \$2 million in advertising services. Yet, instead of treating the expense as a prepaid item, the company charged the advertising expenses off immediately. Despite the lower profits of the division, world headquarters decided that the division had achieved its goal and paid the relevant bonuses.

By 1977, the following practices had evolved at the Heinz USA division:

1. Employees delayed year-end shipments until the beginning of the next year to ensure accurate invoicing dates.
2. Employees handled customer complaints about the delays by making the shipments, but misdating the shipping and invoice documents.
3. Employees did not record credits from vendors until the following year.
4. *Income management* became a way of life. One employee was given the task of maintaining private records to ensure the recovery of amounts paid to vendors on improper invoices.
5. The practice of delayed shipment and prepaid billing to assure that departmental budgeted amounts were met permeated the division down to the departmental level.
6. Ten separate vendors joined in supplying improper invoices.
7. Employees used other questionable tactics to manipulate income including inflated accruals, inventory adjustments, commodity transactions and customer rebates.

What can be learned from this case? First, exerting pressure for continuous growth in profits may foster improper accounting practices, particularly if coupled with an incentive compensation plan that rewards and reinforces continuous growth on the high side. Second, autonomous units with independent accounting capabilities might be tempted, under the above circumstances, to manipulate performance data.

Heinz isn't the only case in which autonomous accounting or pressure for performance led to manipulations of records. There were similar episodes in the 1980s at McCormick and Company, J. Walter Thompson, Datapoint Corporation, Saxon Industries, Ronson Corporation, Pepsico, AM International, U.S. Surgical, and Stauffer Chemical. More recently, companies like Sunbeam and Cendant have been in the news for the same kind of earnings manipulation.

Churning

Churning occurs when a broker buys and sells stock for a client to generate fees, rather than to protect the best interests of the client. Broker discretionary accounts are especially ripe for churning because they can be used to generate fees for both the brokerage firm and the broker, without much involvement or control by the actual investor.

In one case, two sisters gave brokers \$500,000 each to be held in discretionary brokerage accounts. The brokers executed more than 1,400 stock trades, allegedly earning themselves \$400,000 in commissions, while leaving the sisters with \$70,000.

Mixing of Funds

Another scheme involves mixing (commingling) client funds with the funds of the brokerage firm, or broker, or both. In these cases, brokers will use the client's stock as collateral for corporate or personal loans, and post the winning trades to themselves, while posting the losses to their clients. Some brokers also resort to out-and-out embezzlement of their client's money and stock.

Manipulating the Stock Market

Stock market manipulation is a crime perpetrated by a promoter who artificially influences the market price of shares in a company for self-benefit or for the benefit of his or her holding company at the expense of the investing public. In most cases, the promoter flogs his or her holdings to the public, the public pays an artificially high price for the stock, and the resulting increase in price lines the pockets of the promoter.

Promoters of the stock are usually self-styled financiers who start off owning the majority of the stock. Often other conspirators join the promoter, forming a control group consisting of financiers, warehousemen, or brokerage salespersons, some or all of whom might be acting under a corporate umbrella.

To increase the stock's price, the promoter subjects it to a multipronged attack. The promoter uses such weapons as influencing the demand for the stock and controlling the supply of the stock, warehousing the stock (parking), paying secret commissions, wash trading, and issuing fictitious press releases, all of which are intended to stimulate more trading than would otherwise occur.

The victim is the investing public. In many ways this particular fraud is similar to other investment scams that rely on telephone solicitations (boiler room operations) and high commission rates (which are often secret).

Reasons to Study This Kind of Crime. It has been argued that stock market manipulation is a very specialized kind of crime, restricted to the larger financial centers and, therefore, few CPAs are likely to come across them. Nevertheless, because of the great increase in stock market investments, residents anyplace in the country may become victims of stock market manipulation and may look to their CPA for advice. Further, an increasing number of CPAs are providing financial planning services, including investment advisory services, to their clients. These CPAs must be aware of stock manipulation schemes to protect both their clients and themselves.

In addition, stock market manipulation and the *modus operandi* may resemble other kinds of scams in which the price of an investment is influenced by the laws of supply and demand. Therefore, CPAs should be aware of this kind of crime. They could be called upon to speak to the public about prevention of white-collar crime in general or investment scams in particular. Also, they may become an investor in the stock market themselves.

Possible Red Flags. Red flags possibly signaling stock market manipulation, with the possible exception of churning and commingling of funds, are not as readily apparent as they are in some other kinds of economic crime. Most red flags seem to originate from an informant

close to or aware of the control group. In contrast, the regularly required reports investors receive should be reviewed on receipt to assure that there are not patent red flags, that is, there is no churning or commingling of funds. Of course, if the fraud involves falsifying these reports, discovery will probably be delayed until the fraudster is caught, by which time, the investor could well be wiped out.

The SEC and stock exchanges usually carry out investigations to detect this type of crime and the investigations are mainly analytical. Unusual price increases or large commissions earned by salespeople may be investigated, as may press releases or assets reported on financial statements.

Price as Determined by the Law of Supply and Demand. The law of supply and demand states, in essence, that the price of an item will rise when demand for the item exceeds the available supply of that item, and the price will fall when supply exceeds demand. Throughout a stock manipulation, the promoter attempts to control both the supply of, and the demand for, a stock in order to move the price higher. As supply is restricted, the price increases. As demand is stimulated, the price increases.

A stock market is a composite of the interests of many individuals and corporations offering to buy and sell shares. Individuals, however, are influenced not only by information (whether accurate or not), but also by motives such as greed or fear and by perceptions that may have little to do with facts or reason. Investors are capable of changing their investment decisions quickly, purchasing recklessly in a down cycle or staying out of the market entirely in anticipation of disappointing financial information. The common desire is to make profits and to prefer investments that are perceived as likely to produce profits, whether or not these perceptions are based in reality.

Thus, investors will often overreact in seeking to take advantage of price changes or in attempting to correct their errors. A single item of speculative news may dramatically change the number of people who are willing to purchase, hold or sell a particular investment, dramatically changing the demand for the shares. It is important to note that large volumes of shares are often exchanged. Accordingly, time is of the essence in keeping losses to a minimum and gaining the greatest possible profits. Precisely when a buy or sell transaction takes place can make a big difference in the value of the purchase or sale.

Market prices are generally influenced by the release of corporate information, such as news about profits, the announcement of a new product line, or the discovery of a new oil reserve, as well as by changes in government policy, forecasts, prospectuses, and in general, matters that occur in the ordinary daily conduct of a business.

In summary, the investing public, through the medium of publicly held stock, whether traded on an exchange, the NASDAQ or over the counter, is able to place a value on a share and to decide to buy or sell accordingly. As more people seek to buy shares, the price of a share will increase if the number of shares for sale on the market remains the same. Conversely, the price will fall if an excess supply of shares is available or if the public demand for the shares drops.

The Manipulation Process. Generally, a manipulation begins with the promoter falsely increasing demand and restricting or controlling the supply. The combined effect of this process is an increase in price. After a certain point, called the *blow off*, the promoter attempts to increase supply and dampen demand in order to reduce the price, allowing the

promoter to repurchase at a profit. Throughout, the promoter must act as a control valve in releasing the stock in order to control the market price, and hence the profits.

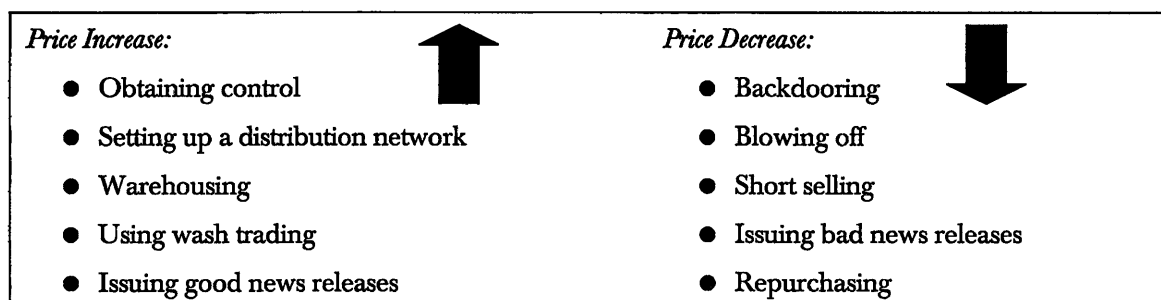
Manipulation may be motivated not only by a promoter wanting to make more money, but also by the desire to make the asset side of an investor's balance sheet look good or to improve the performance of an investment portfolio.

A promoter may use any combination of the following tactics to encourage the public to buy stock at higher and higher prices:

- Using buy or sell pressure by stock brokers who may be receiving secret commissions
- Distributing false press releases and rumors
- Releasing false ownership information
- Promoting fictitious or grossly exaggerated profits, assets or future prospects (or any combination thereof)
- Warehousing to help restrict the supply of shares
- Using wash trading (that is, trading that results in no change in beneficial ownership) to stimulate public interest due to high trading volumes
- Controlling the first or last trade of the day in order to set the highest possible price for the stock
- Dumping into foreign markets

Some or all of the activities generally used in the manipulation process are shown in figure 7-2.

Figure 7-2. Activities frequently used in the cycle of manipulating the stock market



A promoter who wanted to manipulate the price of a stock might use any combination of the activities listed below

1. **Obtaining Control:** The first step that a promoter usually takes is to gain control over an existing company's shares of stock to ensure that the public's selling off large quantities of the stock does not undermine his control over the supply of shares. Generally, 70-to-90 percent of the voting shares that are issued and outstanding must be acquired to exert effective control. The promoter can gain the necessary control by using one or a combination of the following:
 - Buying the shares of an inactive company that is already listed on an exchange (commonly known as *cleaning up the market*). The shares of the promoter's unlisted

company (which do not meet the requirements for listing on an exchange) can then become listed by merging the corporations and exchanging the unlisted shares for shares of the listed company.

- Buying a shell company that may have been inactive for a number of years.
- Underwriting an issue of new shares of a somewhat controlled company. This underwriting usually consists of a new issue of shares in an amount that far exceeds the original number of outstanding shares. To a promoter, this is the least desirable method, as it requires a prospectus, financial reporting, and an insider trading report. In addition, the promoter will have to arrange for his friends to purchase the new shares and hold them (park them) on his behalf an unequivocally fraudulent transaction.

2. *Setting up a Distribution Network:* A distribution network is set up with the promoter at its head. Immediately underneath the promoter are several distributors in cities that have stock traders or brokerages. Each of these distributors has access to a brokerage house's salespeople who then have access to the active traders. Via this network, the promoter now has control over what happens in the promoted stock's market. Secret commissions are sometimes paid to ensure that the network complies with the promoter's demands.

The traders let the salespeople know when trades are pending and keeps them informed as to the price movement of the promoted stock so that the promoter can take compensating action. The salesperson's job is to give the public a sales pitch as to why they should buy the stock and, once in, why they should stay in. In addition, the salesperson's activity will affect the daily trading volume. What members of the public do not know in this situation is that the shares they are purchasing are those of the promoters.

3. *Warehousing:* Warehousing places shares into the hands of people who are friendly to the promoter. This is essential in order to maintain control of the shares and continue to restrict and regulate the supply of shares available. This is often accomplished by having friends buy new offerings of the stock and continuing to hold these shares until the promoter instructs them to sell.
4. *Wash Trading:* To promote the public's interest and increase demand for the promoted stock, the promoter manipulates the volume of stock traded through wash-trading. Essentially, this procedure consists of a stock purchases and sales with no change in beneficial ownership. Wash trading can be accomplished through nominee accounts: accounts at banks or trust companies set up under the names of trustees, friends, aliases, or false company names. The promoter sells a block of shares and at the same time a nominee enters a buy order to match the sell transaction. While the stock is kept out of the public's hands, this active, ostensibly normal trading is reflected in the volume numbers the public sees. Hence, the market in the manipulated stock appears to be an active one in the public's eyes.
5. *Issuing Good News Releases:* One or more timely news releases may be issued to promote the stock, attracting further public interest. The news releases may include verifiable information but may also consist of unsubstantiated rumors, such as:
 - Anticipation of good results from drilling tests in resource-based companies

- Expectations for a likely acquisition of rights to explore property close to existing known resources
- Plans for diversification into a *glamour* industry

Generally the good news may be described as an intangible promise of future results. There is nothing of immediate value today. These good news releases are designed to stimulate the public interest and encourage them to buy shares, even at a high price.

6. **Backdooring:** *Backdooring* occurs when friends operating as a warehouse, which the promoter has previously set up, start selling their shares while the price is still increasing—contrary to their agreement with the promoter—before getting the word from the promoter to sell. The friends are backdooring the promoter, effectively double crossing the promoter. In order to sustain public demand, the promoter has to buy the backdoor shares at the market price if the existing public demand is not sufficient to support these sales.
7. **Blowing Off:** After the promoter has successfully stimulated demand, members of the public buy significant numbers of shares and then wait for the price to continue its anticipated rise. The promoter has already picked a tentative price at which he wants to dispose of his holdings. He starts selling his shares, as well as those of his nominees and friends. In these circumstances, the sale of unusually large amounts of stock is referred to as a *blow off*. The public, expecting a continued price rise, buy the promoter's shares over a relatively short period of time.

The price at which the promoter actually begins to blow off his holdings depends primarily on how much public demand the distribution network has created and how long the demand is sustained. By blowing off, the promoter has withdrawn all active support of the stock price. He ceases wash trading, the reported trading volume decreases, and the price begins to fall quickly as supply far exceeds demand.

8. **Short Selling:** Short selling is the act of selling stock that one does not yet own and is a legitimate market activity. The seller is gambling that the price will decrease and that he or she will be able to buy back the shares at a price lower than the current-selling price. In this situation, the promoter can safely sell short, because he or she knows that the price will go down. Thus, the promoter realizes a profit both as the price of the stock goes up and again as the price goes down.
9. **Issuing Bad News Releases:** At this point, the promoter often issues a news release about the company's misfortunes. The exact reverse of the good news release, the promoter intends the bad news release to drive down the price of the stock rapidly.
10. **Repurchasing:** The stock price has now reached rock bottom, and the public is willing to sell at any price. The promoter often buys back control of the company when the shares reach this low price and changes the name of the company in order to start the process again. The same company, under a new name, will go through the cycle again in a period of one to two years.

Secret Commissions. Secret commissions were previously mentioned in the distribution network discussion. Generally, secret commissions or bribes are given to people in the securities industry to induce them to push or promote the shares in the promoter's company and to advise the promoter of orders to purchase shares before the orders are entered. Secret commissions may also be paid to the wash traders in order to keep their support. Generally, secret commissions are paid in one or more of the following ways:

- By a check drawn on either a personal or a corporate bank account and payable to the recipient, to cash, or to a third party. If the check is paid to a third party, it will be endorsed by the named third party and cashed, with the cash being passed on to the true recipient of the secret commission.
- By a free delivery to the recipient of stock in signed-off or *street certificate* form, which can then be sold by the recipient on the market.
- By the issuance to the recipient of call options on the stock at a fixed price below the current market price.
- By selling a block of stock to a salesperson or another recipient at a fixed price and allowing that buyer to sell that block back at a higher price.

The Significance of Accounting Evidence. Accounting evidence is generally very significant in the prosecution of stock market manipulation cases because—

- The accountant can perform an analysis to determine whether change in beneficial ownership occurred (a wash trading analysis).
- Accounting evidence may be instrumental in identifying payments or receipts of secret commissions, if any.
- Accounting evidence can be used to establish the percentage of the public's participation in buying and selling shares when compared to the total transactions in the stock by the control group.
- Accounting evidence may assist in establishing that the perpetrators have benefited from the sale of the stock.

However, accounting evidence may not be as significant as *viva voce* evidence in initially identifying the control group, establishing the secret commission structure, and identifying who was paying and receiving these commissions.

Possible Preventive Measures. Perhaps the most significant stock manipulation preventive measure is to make the investing public aware that a salesperson's pitch will be persuasive, will play on the investor's greed, and will convey a sense of urgency. The following are questions that an investor should ask a salesperson to answer on the record concerning the specific representations being made about the investment. The answers given should help in identifying poor or fraudulent investments.

1. How risky is this stock?
2. What direct costs are paid out of the investors' funds, such as for commissions, or advertising, or both?
3. Can I get written documents (the prospectus at a minimum), and can you mail them to me?
4. What is the specific destination (that is, bank account, brokerage account) of my funds?
5. How can I sell the stock if I choose to do so, and how long will it take to dispose of the investment?
6. What are the names of the principal owners and officers of the salesperson's firm, and what are the names of the owners and officers of the company in which the investment is being made?

Gonna Put You in the Movies Corp. Case Study

In early 1998, Jack Smith started to promote a company called Acme Mines Co., a shell company listed on the Westville Stock Exchange. Smith had effective control of the outstanding shares. In order to promote public interest and buying, Smith made announcements—through investor bulletins and statutory statements to regulatory bodies—to the effect that Acme was about to diversify into the movie production business and other ventures. The announcement touted:

- An investment of \$175,000 in the production of a movie, which would return 25 percent of the profits to Acme
- A purchase yielding 58 percent control of a movie theater business called Everytown Theaters Ltd.
- An acquisition of distribution rights to *Krazy Kandy*, a confection that would be sold from automatic vending machines across the country

On February 4, 1998, Smith changed the name of the company from Acme Mines Co. to Gonna Put You in the Movies Corp. (GPY-Movies) to reflect its new objectives.

Smith's next step was to stimulate trading activity in GPY-Movies' stock on the Westville Stock Exchange. To accomplish this, offices were maintained in Bigtown and Westville and were operated by Mike Jones, a securities desk-trader, and the controller, Dave Brown. Their objectives appear to have been to maintain the market with effective control, match orders to create activity (wash trading), and systematically sell off the stock for profit.

Smith would tell Jones when to buy or sell. Jones would follow through via a series of controlled nominee accounts. Brown's job was to keep track of all the accounts, meet corporate requirements, and generally manage the money and the office in Bigtown. The nominee accounts were all in corporate names and could be traded by Mr. Smith, Mr. Jones or Mr. Brown.

The office in Bigtown was in the name of Anyco Investment Corp. The accounts at brokerage firms in both Westville and Bigtown were in the following names:

1. Metro Trading Associates.
2. Oakville Investments Co.
3. Pineville Trading Ltd.
4. Anyco Investment Corp.

At this time Smith was either an officer or director of each company and effectively controlled them. Stock positions in GPY-Movies were established through numerous Bigtown and Westville brokerage firms.

The eventual objective was to sell off or distribute the stock for a profit without causing an obvious decrease in the market price. To achieve this goal, Smith hired Robert Green who started to work out of the Bigtown Office around April 2, 1998. Smith instructed Green to sell stock through the accounts of Anyco and Metro

Trading and to limit the price to \$1.26 until an underwriting was effected, which was to occur on April 18, 1998.

Green's procedure was to prearrange all the buy orders so that they could be matched with any one of Smith's selling accounts. Whenever Green learned of a buy order, he would notify Jones of its size, price and the name of the brokerage firm. This meant that Green had to be in contact with sales reps or their distributors who would notify him of forthcoming buy orders. In order to secure their cooperation, Smith specifically authorized Green to pay sales reps a 15 percent commission over and above the amount sales reps would normally receive. In addition, Green, with the assistance of Smith and Brown, arranged for Wally Chang, a brokerage house manager, to use his sales force to distribute 300,000 shares of GPY-Movies throughout the United States for a 12½ percent commission.

On occasion, Smith arranged to provide cash to Green in order to make payments to sales reps. Brown made the checks payable to cash and drew them on one of the companies' accounts. Green made his own arrangements as to where and when to pay the sales reps.

Smith convinced two sales reps, Black and White, to set up an account in their firm. Whenever Black and White were able to persuade one of their clients to buy GPY-Movies shares, the offset would come out of Smith's account in the name of Metro Trading. In this way, Smith was able to sell off his position and pay Black and White with shares that they in turn sold through nominee accounts. Paul Wilson, an analyst, provided Smith with inside information on who was bidding or offering, as he was indebted to Smith for a substantial loan.

Thus, Smith and Jones, in an effort to generate personal gain, created a misleading appearance of active public trading in shares of GPY-Movies, both by wash trading and by the use of secret commissions. The result was a loss to the investing public.

7.2.9 Environmental Abuse

Generally there are two main kinds of environmental abuse that a company can commit:

1. Pollution
2. Misuse of natural resources

Pollution

While a certain level of pollution is tolerated by today's society, media attention has recently focused on companies that have gone too far. Society is, as a whole, becoming less tolerant of all forms of pollution, and this is reflected all the way down to the consumer—for instance, aerosol spray cans and cigarette smoking in restaurants are no longer tolerated in many jurisdictions. Laws have been passed to limit the levels of pollution, but not all companies comply with the laws, usually because of the added costs incurred.

Amount of Pollution. The amount of pollution and how it is determined depend on the nature and source of the pollution. For example, a perpetrator may have dumped garbage at an authorized site but in quantities greater than the dumping license permits. Or, a

perpetrator may have dumped garbage at an unauthorized site. Or, a perpetrator may have polluted the environment in some other way, for example, dumping toxic substances into a river, or exceeding the specified limits of emission of certain substances into the atmosphere.

Regardless of the nature and source of the pollution, the alleged offender's accounting and administrative records are likely to yield pertinent information about the physical quantities of substances that are themselves pollutants or that result in pollution. Financial records can also provide useful evidence as to the alleged offender's knowledge and intent. For example, an accounts receivable listing would reveal the names of the company's customers, but additional documents would be needed to assess the extent of the polluting activities. These documents might include invoices, bills of lading, weigh tickets, contracts, production reports, and so on.

Depending on the nature of the abuse, the financial records may help to put a dollar value on the cost of the damage done. For example, if you can establish that a company dumped in excess of the 5,000-ton-garbage limit permitted by its license, the courts can calculate the cost of the excess from the company's accounting records. This *cost* provides the judiciary with a yardstick against which to determine damages.

Dumping Unlimited Case Study

Dumping Unlimited was a carting company that had a license to dump waste material at a landfill site near Anytown. The company's license permitted dumping a maximum of 150 tons of material per day at the landfill.

Dumping Unlimited maintained a fleet of garbage trucks, which dumped the company's waste at the landfill site, and they also accepted waste material from other haulers on a daily basis.

Based on an analysis of weigh tickets, it was clear that the company was dumping quantities in excess of the permitted amount. To determine the value of these quantities, the excess tonnage was priced at the highest and the lowest price charged by the company, giving a range of values attributable to this offence.

Financial Capacity. Companies that are fined for noncompliance with antipollution laws often claim that they cannot afford either the costs of compliance at the time when the pollution was generated or the costs associated with cleaning up the after effects of the pollution.

Both of these issues are best examined by a CPA and involve examining financial statements and budgets.

There are relationships between various components in the financial statements, which help to identify historical issues relating to both profitability and viability. A review of the financial statements for a number of accounting periods will be helpful in determining

trends that would enable a CPA to compare the company's financial results with the costs required to comply with antipollution laws.

In order to assess whether a company can afford the costs of cleanup (particularly when that company claims it cannot), a CPA would need a crystal ball. In the absence of a crystal ball, the CPA should examine the company's budgets.

Management predicts the future by way of the budgeting process. Most enterprises that take the time to prepare budgets use them as tools for making financial and operating decisions. The range of budgets include operating budgets, capital budgets and cash flow budgets. A comprehensive operating and cash flow budget enables management to plan future operations and to decide how the company will pay for them. Access to past budgets, together with the corresponding historical results, allows the forensic accountant to interpret the proficiency of the company's budgeting process and to determine whether a company can or cannot afford the cleanup costs.

Mine Cleanup Case Study

In the 1990s the federal government filed suit against Mine Cleanup, a uranium mining company, for failure to clean up a former site. The mining company claimed it would be put out of business if it was required to pay the \$30 million required to clean up the site. Mine Cleanup management was attempting to set aside the clean-up order.

A thorough review of the company's financial statements, operating budgets, long term forecasts, and cash flow budgets revealed that the company was unable to pay the costs in the short term, but that it was possible for the company to comply with the cleanup order over an extended period. A negotiated agreement was reached between the federal government and the company wherein the government essentially provided the long-term financing for the cleanup so that the cleanup operations could commence immediately.

Natural Resource Abuse

Laws with respect to natural resource abuse (over-fishing, hunting, logging, mining, and so on, as well as neglecting the endangered-species legislation) vary from jurisdiction to jurisdiction and generally apply to both noncommercial and commercial harvesting of animals, marine life, and endangered species. Accounting evidence has little relevance to noncommercial activities; thus the focus in this section is primarily on commercial activities involving the following three areas:

1. Fur trapping and fur dealers
2. Commercial fishing
3. Endangered species

Note that companies that are involved in these commercial activities need to be aware that conservation officers appear to have a much broader right of access to business premises

than that available to law enforcement officers. Generally, the legislation allows the officers to search any aircraft, vehicle, vessel, camp, or office, without the requirement of a search warrant, if they believe that any fish or game has been killed or taken in contravention of the applicable state laws.

Fur Trapping and Fur Dealers. Fur trappers must be licensed to practice their trade in each state in which they operate. They are assigned maximum quotas for different kinds of wild life. They are generally required to have each pelt examined and registered, at which time a stamp is affixed to the inside of the pelt. The trapper is not required to submit written reports to the state; the next level in the distribution system does that.

The fur dealer obtains a license to purchase, receive, sell, or otherwise dispose of fur pelts. With a few limited exceptions (domestic animals, road kill, and so on) the fur dealer must ensure that the pelts being purchased have been examined and suitably stamped. Monthly reports are generally required from the fur dealer specifying:

1. The pelts purchased or received, including the name of the trapper or hunter from whom the fur dealer purchased or received the furs; the date on which such pelts were obtained; and the number and the kinds of animals, for example, beaver, mink, lynx, and otter.
2. The pelts sold or disposed of, including who the pelts were sold to by name, address, and license number; the date on which the pelts were sold, tanned or disposed of; and the number and kinds of animals.

The most common form of abuse is the handling of unauthorized pelts, which are purchased from a trapper or hunter, that are typically excluded from both of the monthly fur dealers' reports—that is, they are excluded from the report of pelts purchased, and from the report of pelts sold. These pelts typically bear no authorized stamp. The transactions often involve some financial consideration to the purchaser, for example, lower prices or secret commissions, which could be ascertained upon a review of the fur dealer's books and records. The unauthorized pelts are typically disposed of by being included in bundles of authorized fur pelts submitted to a fur auction outlet, or by being directly supplied to a tanning operation owned by the fur dealer.

Commercial Fishing. Commercial fishermen are generally licensed to work in designated regions within the United States and its waters, and are assigned maximum quotas by fish species and poundage. These fishermen are generally required to submit a monthly report that accumulates information on the port where the fish were landed, the weight of the catch by species, and the average price of fish sold.

Unlike the fur dealer, the commercial fisherman is not required to submit a report stating to whom the fish were sold.

The most common form of abuse involves the fisherman exceeding his quotas and failing to report the excesses in his monthly reporting. A review of the cash receipts, disbursements, and sales journals of the commercial fisherman should detect the abuse even though many purchases and sales are cash transactions that take place off the company's books. Because the reporting required is done by weight rather than by supplier or number of fish, it is necessary to reconcile the weight of fish caught to the weight of fish purchased by customers after allowing for wastage.

Endangered Species. In most jurisdictions, endangered species of fauna and flora are protected by laws that prohibit the killing, injuring, interfering with, taking, or attempting to do any of the above to any of the identified species of fauna or flora or their natural habitats.

Currently one of the major abuses is the exporting of certain endangered species of wild birds, particularly falcons, to other countries at an exorbitant profit to the perpetrators.

7.2.10 Economic Extortion

Economic extortion is a crime in which a financial benefit is sought or obtained through intimidation or persistent demands.

Some of the forms of crime described in this section of the Handbook could involve an element of economic extortion. For instance, bribes could be required in order to obtain a lucrative contract; an owner of a company could be squeezed out by one or more of its creditors for reasons other than insolvency; an employee could be forced to divulge an employer's trade secrets; or a company could be forced to pay a contractor to keep quiet about its environmental pollution problem. The common element in each of these situations is that the likely outcome of noncompliance with the extortionist's demands is perceived to be worse than the actual outcome of compliance.

Often, an extortionist's methods involve threats of physical violence, public disclosure of something that the victim would rather keep private, or financial ruin.

A Piece of the Action (Sport Megaplace) Case Study

In early 1994, Sport Megaplace was established as a state-approved organization to control the sale of lottery tickets in Megaplace and to apply the net proceeds from these sales to the development of amateur sports within Megaplace.

At that time the sale of lottery tickets included the sale of *Tinylotto* tickets, which was under the control of Mr. Johnson, and the sale of *Biglotto* tickets, which was under the control of Mr. Williams. These men were responsible for dividing Megaplace into wholesale distributorships so that both kinds of tickets could be sold regularly through wholesalers to retailers and then to the public.

However, Johnson and Williams only allowed others to obtain wholesale distributorships if they secretly agreed to pay 50 percent of the future profits to a holding company under the control of Johnson and Williams. The *silent-ownership* payments were structured as payments for management, consulting services and for office space.

The new distributors were led to believe that this arrangement was legitimate by the existence of a wholesale distributor agreement with Johnson and Williams' company, a reporting letter from a lawyer's office, a declaration of trust agreement, a power of attorney agreement, working papers from an accountant, banking resolutions and signature cards.

7.2.11 Customs Duty Fraud

Although customs laws vary from nation to nation, there are common threads and patterns of fraud that are inherent in transborder transactions. The following material describes typical customs fraud scenarios in Anyland.

The Customs Act applies to goods imported into Anyland. The Act categorizes imported goods by tariff schedules and prescribes rates of duty applicable to each item depending on its nature, the country of origin, and international treaty arrangements.

The duty payable to Anyland's Customs Service is a percentage (the duty rate) of the imported item's Value for Duty. Prior to January 1, 1998, the Customs Act based its determination of the Value for Duty amount on the fair market value of the goods at the time of export in the exporting country. In practice, this fair market value was usually the amount indicated on the commercial invoice. Customs officers did, however, have the option of disregarding the commercial invoice amount and determining a fair market value to be used for Value for Duty purposes using other information sources.

This fair market value determination for applying duty rates to imported goods did not comply with international trade agreements to which Anyland was a party. Thus, effective January 1, 1998, a revised procedure for determining the Value for Duty amount was introduced. The new basis, called the Transaction Value Method, specified the Value for Duty amount to be the price paid or payable to the exporter where the exporter and importer are dealing at arm's length. For imports between related parties, the onus is on the importer to prove that there was no influence on the commercial invoice price. In these situations, Value for Duty is determined on the following sequential bases:

1. Transaction value of identical goods
2. Transaction value of similar goods
3. Deductive value based on a gross profit reduction of the importer's selling price
4. Computed value

The abuse generally arises when the importer causes the Value for Duty of the imported product to be falsely understated, thereby reducing the amount of customs duty paid.

Importers abusing the customs regulations may vary in size of operation, ranging from small sole proprietors to large national distributors. The benefits from understating Value for Duty amounts can be enormous. In one case, the fine paid totaled \$25,000,000, arising from a conviction of evading customs duties over a fifteen-year period. There was also a civil court claim for \$105.2 million against the same company for unpaid duties on goods imported over a period of years. Even on a small scale, with duty rates ranging up to 30 percent or more, understating the Value for Duty amount may provide the importer with a 10-to-15 percent cost saving and a trade advantage over its competitors.

Because the Value for Duty amount generally is supported by both a commercial invoice and customs invoice prepared by the exporter, the duty and sales calculations rely on the integrity of the exporter's documentation. Many customs investigations have determined that the documents prepared by exporters understate the actual value at which the goods were sold.

Current customs practices continue to be conducive to fraud. Importers of legally importable goods are aware of the enormous volume of imports, the emphasis placed on illegal drug shipments, the shortage of customs officers, and the officers' inability to fully inspect all entries that provide a perceived window of opportunity to perpetrate fraud.

Investigation Issues

Red Flags. Customs investigations have uncovered various schemes to falsely reduce collectible duties. The presence of one or more of the following red flags may assist in identifying a customs under valuation.

1. *Apparent excess insurance:* Insurance coverage for the in-transit goods substantially exceeds the declared Value for Duty of the same goods.
2. *Competitor's complaints:* Competitor's complaints to customs or any other agency governing fair trade that it cannot match the importer's wholesale or retail prices.
3. *Poor quality documents:* The integrity of the exporter's documents may be suspect if any invoice is: printed on tissue paper, hand typed, not preprinted, or not prenumbered.
4. *Letters of credit or bank drafts:* Payments for the imported goods exceed the declared Value for Duty amount.
5. *Presence of blank invoices:* If Anyland customs invoices or export declarations, or the exporter's supplier invoices are known to exist at the importer's place of business and are found to be blank except for the exporter's authorization signature, the importer may be preparing such forms for presentation to Anyland's customs.
6. *Related exporter:* The importer and exporter are related parties and, therefore, do not deal at arm's length; there could be price collusion.
7. *A and B Commercial Invoices:* Total costs for the imported goods may be apportioned between two separate invoices (often having consecutive invoice numbers, or having the same invoice number with A and B suffixes), only one of which is submitted to customs for purpose of Value for Duty determination.
8. *Unreasonably high values allocated to nondutiable export costs:* The dutiable cost of product is artificially understated and the nondutiable cost of freight, for example, is overstated on the commercial and Anyland customs invoices.

Significance of the Accounting Evidence. After performing an overview, the forensic accountant can provide details for each entry and a summary schedule for all entries. This schedule quantifies the apparent Value for Duty shortage and calculates the apparent duty shortages, thereby determining the amount withheld.

In preparing this quantification, the forensic accountant assumes that documentation other than that used in the customs declaration in fact provides the *true* Value for Duty. The forensic accountant may need to obtain expert-witness evidence to substantiate this basis for valuation—perhaps a specialist from the Customs Service or from a lawyer.

In addition, in reviewing the importer's accounting books and records, the forensic accountant may be able to provide further support for the alleged undervaluation and may be helpful in refuting possible defense claims.

Testimony: Viva Voce Evidence. The forensic accountant may seek evidence from various other sources. Employees of the importer may be interviewed to provide evidence as to the

inner workings of the importer and to settle issues of ownership or control of the importing company. A customs' broker may provide testimony that, if presented with the documents on which the forensic accountant's calculations were based, a higher Value for Duty would have been declared.

7.2.12 Health Care Fraud

There are a wide variety of health care frauds that have recently been the subject of media attention. Many such cases are outside the scope of this section—that is, they relate to fraud committed by individuals rather than by corporations. Health care fraud committed by corporations typically involves one of the following:

1. Violations of occupational health and safety laws (OSHA).
2. Marketing of drugs that have not been adequately tested or for which the test results have been falsified.

7.2.13 Possession of Property Obtained by Crime

This offence refers to either the actual possession of property obtained by a crime, or to the possession of proceeds from the disposal of property obtained by a crime.

When a business is suspected to be in possession of stolen inventory, an examination of the financial records should be able to establish whether this inventory had been legitimately purchased.

A reconciliation of the inventory purchased and sold needs to be performed and compared to the inventory on hand at both the beginning and end of the period in question: the end date is usually set shortly after the date that the stolen inventory was allegedly obtained. The purchases and sales should be ascertained from the company's purchases and sales records, and also from updated accounts payable and accounts receivable listings. If there is a positive variance, it could result from an accounting discrepancy, which would need to be examined further, or it could result from the possession of property obtained by crime.

If the purchases, on the accounting records, appear to be legitimate, then the integrity of the supplier invoices must be assessed. Often, stolen inventory can be made to appear legitimate through overstatements on supplier invoices.

Don't Fence Me In Case Study

Acme Industries was acting as a fence for stolen car parts. These parts were stolen by third parties and were sold by Acme to authorized car dealerships at prices considerably lower than normal wholesale prices. When Acme's premises were searched on December 8, 1998, parts valued at approximately \$667,900 were seized.

Forensic accountants were retained to determine, by means of the available books of account and supporting documents, whether these parts were purchased legally or otherwise. Here are the steps followed to make the requested determination.

1. The accountant began by performing a period examination. The disbursement journal disclosed that a payment had been made to a firm of CPAs for services rendered to Acme. An interview with this firm revealed the existence of a draft set of financial statements for Acme, dated February 28, 1998. These financial statements, which were never issued in final form, disclosed inventory valued at \$16,500, with a note stating, "no physical inventory taken; inventory estimated for accounts." The draft financial statements established the opening date of the time period. The closing date was determined by the date of search and seizure, December 8, 1998. The period March 1, 1998, to December 8, 1998, was, therefore, the period examined.
2. The accountant then updated the financial records of Acme to the date of search and seizure. This step disclosed purchases from various suppliers totaling \$886,167. A similar updating of the sales of Acme resulted in a sales figure of \$1,007,815.
3. To calculate the book value of inventory, the accountant created a schedule, identified as *Apparent Inventory of Acme as of December 8, 1998*. It set out the total value of the goods available for sale of \$902,667 (opening inventory of \$16,500 plus the purchases made, during the period, of \$886,167).

The schedule set out the updated sales figure and a gross profit margin (sales minus cost of sales divided by sales) ranging from 10-to-30 percent. By deducting the gross profit margin, an apparent cost of goods sold was calculated, ranging from a high of \$907,000 at the 10 percent level to a low of \$705,470 at the 30 percent level. A comparison of the apparent cost of goods sold to the value of goods available for sale showed that there should have been no inventory as of December 8, 1998 at a 10 percent gross margin. At a 30 percent gross margin, the value of inventory at December 8 would have been \$197,197.

4. To perform a valuation of the parts seized, the accountant compared the goods seized to the inventory on hand calculated at the 10 percent gross margin level, indicating an excess quantity of physical parts on hand of approximately \$672,200. When a gross profit margin of 30 percent was applied, the excess on hand was approximately \$470,000. Based on the above procedures, Acme had in its possession an excess quantity of parts ranging in value from \$470,000 to \$672,200.

Interviews with three suppliers indicated that the invoices used in the calculation of purchases between March 1 and December 8, 1998 had been inflated or padded so that the invoiced value of goods purchased by Acme was greater than the actual value of the goods received. The padded portion of the payments Acme made to its suppliers were paid to the wife of Acme's owner in cash.

Padding the supplier's invoices made the stolen goods on hand harder to detect or easier to explain away, or both. The inflated purchase prices also allowed cash to be removed from Acme, tax free, under the guise of an expense. The payments to suppliers were converted into cash with the excess (padded) portion of the invoiced price being returned to the owner's wife as cash.

This disclosure made it necessary to revise the calculated value of inventory as of December 8, 1998, to reflect the alleged nonpurchases in Acme's dealings with the

three suppliers who were padding their invoices. These alleged nonpurchases totaled some \$263,000, thereby increasing the value of the excess quantity of parts in the possession of Acme to a figure between \$735,000 and \$935,000. These findings not only placed the onus on the owner of Acme to explain the source of the excess quantity of parts seized but also disclosed the existence of a fraudulent scheme involving the three suppliers.

7.2.14 Coupon Redemption Fraud

Coupon redemption fraud involves the fraudulent collection and conversion of coupons designed to promote various kinds of merchandise. For example, a newspaper coupon for a box of cereal may require the purchaser to present it at a supermarket to receive twenty-five cents off the purchase price of the cereal. Normally, the manufacturer reimburses the supermarket for the discount it paid plus a token fee, perhaps several cents, to cover the cost of processing the coupon and returning it to the manufacturer.

Unscrupulous grocery and supermarket owners will collect coupons, in some cases from an intermediary, and redeem them as though merchandise has been purchased from them, when in fact, it has not been. Although the individual amounts can be small, the volume in most consumables can make it profitable for stores to engage in these schemes.

7.3 PREVENTION OF COMMERCIAL CRIME

Four forces can operate to reduce commercial crime:

1. Increased awareness—that is, decreasing the likelihood that a victim will be “taken.”
2. Formal deterrence—that is, the fear of formal, officially imposed sanctions (conviction and punishment by the government).
3. Informal deterrence—that is, the fear of informally imposed sanctions, such as the loss of respectability or a career.
4. Ethics—that is, the internalization of values that discourage violations of legal codes.

7.3.1 Increased Awareness

Increased awareness is achieved through education and by experience. However, experience can be a costly way to increase awareness. With increased awareness, the investor, customer, competitor, and general public are more likely to closely scrutinize a situation and ask questions that would raise alarm bells and prevent them from suffering a loss. For instance:

- Investors should be wary of schemes pitching high rates of return in a short time.
- Investors also should be wary of schemes with foreign intrigue.
- Investors should thoroughly examine franchise opportunities before any funds are invested. Brochures and marketing pitches should be viewed with skepticism, particularly in the case of new or unconventional franchisers. Detailed financial information, including costs and profit margins of the franchiser for any goods and

services they are contracting to provide, should be reviewed to determine the motives of the franchiser.

- Investors should ask stock promoters a series of questions about the stock the promoter is pushing to determine the extent to which that promoter is tied to the stock.

7.3.2 Formal Deterrence

A crime control strategy has little chance of success unless offenders are punished. However, formal levels of current enforcement are, by all measures, extremely low. One novel approach is enforced self-regulation. Under this idea, the government would compel each company to write unique rules for itself or its employees. A governmental agency would monitor compliance. Two examples of successes in the noncriminal area are the Federal Aviation Administration, which monitors self-regulation for the U.S. airline industry, and the Federal Trade Commission, which monitors rules that the U.S. advertising industry has largely set for itself.

However, there are problems with self-regulation, and the industries that attempt to regulate themselves have spotty records at best. In one study of the 320,000 physicians in the United States, an average of only seventy-two medical licenses per year were revoked.

It may be that increased enforcement can only come at the expense of a complete and total revision of the criminal justice system. Many commercial criminals have little fear of detection because of the constant barrage of information that demonstrates the police and courts simply cannot keep up with the pace of criminal offenses. Until potential offenders have the perception that they will be caught and punished, we should not expect a reversal of this crime trend.

However, many researchers believe there are better deterrents to commercial crime than incarceration of the individuals who are directly involved. They argue that the most effective deterrents are:

- Monetary penalties
- Adverse publicity

The following remedial steps could be adopted to deal with commercial crime:

1. Strengthen consent agreements and decrees (under which companies do not admit that what they were doing was wrong, but agree to stop doing it) to provide substantial remedies for violations of the agreement and to include systematic follow-ups.
2. Increase fine ceilings, assessing fines according to the nature of the violation and in proportion to the company's annual sales.
3. Enact stiff criminal penalties for violations of health and safety or environmental regulations that recklessly endanger the public or employees.
4. Introduce stronger statutes to prohibit companies that previously had violated federal laws from receiving federal contracts.
5. Promote mandatory publicity for corporate civil and criminal violations.
6. Increase more extensive use of imprisonment with longer sentences. Replace community service with incarceration, except for unusual circumstances.
7. Prevent convicted corporate offenders from being indemnified by their companies.

8. Prohibit for three years management officials convicted of criminally violating corporate responsibilities from assuming similar management positions in their company or others.
9. Make directors liable, but not criminally, for being derelict in their duty to prevent illegal corporate actions.
10. Enact a new commercial bribery statute to help prosecute corporate executives who receive kickbacks from their customers or suppliers.

7.3.3 Informal Deterrence

Most commercial criminals, compared to more traditional offenders, perceive the informal sanctions of the loss of career and prestige to be a greater deterrent. They are, therefore, theoretically more deterred from misbehaving by those consequences than by incarceration.

For example, a bank president, who was told he was about to be indicted, spent most of his time asking whether the charges were going to be made public. When told that indeed the charges would be public, the banker, promptly committed suicide.

Informal sanctions often exist without formal sanctions. The imposition of formal sanctions, however, will usually lead to additional informal sanctions.

7.3.4 Ethics

Behaviorists generally conclude that one of the single most important factors influencing group behavior is the attitude of management, who—in many reported instances—have been claimed by employees to have exerted pressure on them to engage in unethical behavior.

One prime example is the famous Equity Funding Case, which occurred in the early 1970s. It was uncovered when a disgruntled former employee went to the authorities. For nearly ten years, the Equity Funding Corporation falsified more than 56,000 life insurance policies and overstated their assets by \$120 million. It was estimated that fifty to 75 employees, who managed to keep the scheme a secret for several years, were involved. The trustee appointed to sort out the massive fraud, Robert Loeffler, said, “Of almost equal importance was the surprising ability of the originators of the fraud to recruit new participants over the years.”

Teaching people that certain behaviors are illegal and therefore inappropriate is uncomplicated and extremely effective in reducing crime. Moral education that discourages illegal behavior, from the top to the bottom of an organization, must be continuous. Simply put, people must be informed as to what behavior is acceptable and what is not so that they can alter their actions appropriately.

CHAPTER 8:

Computer Crime, Computer Criminals, and Computer Evidence

| | | |
|-------|---|----|
| 8.1 | Overview | 3 |
| 8.1.1 | Security | 4 |
| 8.1.2 | Evolution of Computer Crime | 5 |
| 8.2 | Computer-Related Crimes..... | 5 |
| 8.2.1 | Intellectual Property | 6 |
| 8.2.2 | Computer Hardware | 6 |
| 8.2.3 | Computer Crimes and the Law..... | 6 |
| 8.3 | A Brief History of Computer Crime | 7 |
| 8.4 | Computer Crime Today | 8 |
| 8.4.1 | Classification of Computer Fraud | 10 |
| 8.4.2 | The Most Common Computer Crimes | 11 |
| 8.5 | Fraud and the Internet | 12 |
| 8.5.1 | Fraud-Friendly Internet Characteristics..... | 13 |
| 8.5.2 | Computer Crime Laws..... | 15 |
| 8.5.3 | The Tools of Fraud on the Internet | 16 |
| 8.5.4 | Internet Frauds: The Top 10 and Beyond..... | 17 |
| 8.6 | Computer Criminal Profiles | 20 |
| 8.6.1 | Predictions | 20 |
| 8.6.2 | Reasons for Committing Computer Crimes | 22 |
| 8.7 | Controls for Preventing and Detecting Computer Crime | 23 |
| 8.7.1 | Internal Control and Security Systems | 24 |
| 8.7.2 | Factors That Encourage Computer Crime..... | 25 |
| 8.7.3 | Factors That Discourage Computer Crime..... | 26 |
| 8.7.4 | Information Technology Controls for Compliance with Sarbanes-Oxley..... | 27 |
| 8.7.5 | Security Countermeasures to Computer Crime | 32 |
| 8.7.6 | Solutions | 33 |

| | | |
|-------|--|----|
| 8.8 | Computer Fraud, Computer Evidence, and the Science of Computer Forensics..... | 34 |
| 8.8.1 | Why Computer Evidence Has Become a Vital Consideration in Fraud Investigations | 34 |
| 8.8.2 | The Complexities of Data Storage: Looking Under the Hood | 34 |
| 8.8.3 | Computer Forensics Versus Data Recovery | 40 |
| 8.8.4 | What Is Computer Forensics? | 40 |
| 8.8.5 | Making the Best Use of Computer Forensics in Fraud Investigations | 43 |
| 8.9 | Selected Computer Crimes..... | 45 |
| 8.9.1 | Brief Case Synopses..... | 45 |
| 8.9.2 | Case Study: A Closer Look | 48 |
| 8.10 | Conclusion | 50 |
| 8.11 | Computer Crime Checklists..... | 51 |

CHAPTER 8:

Computer Crime, Computer Criminals, and Computer Evidence

8.1 OVERVIEW

The growing use and increasing complexity of the computer have made certain kinds of crimes easier to commit, harder to detect, and often very difficult to prosecute. The commission of computer crimes has also been facilitated by the spread of the Internet and the creation of global intranets in transnational corporations that permit access to computers anywhere in the world from points anywhere in the world.

A computer-related crime is simply one in which a computer is used either to commit or assist with the commission of a crime, or is itself the target of a crime. Traditional crimes committed *using* computers may include embezzlement, larceny (theft of property and proprietary information), fraud, extortion (blackmail), forgery, and counterfeiting. Traditional crimes committed *targeting* computers may include sabotage, vandalism, electronic burglary, wiretapping, and the gaining of illegal access either by impersonating an authorized user or by exceeding one's authority. In addition, the U.S. federal and state governments as well as the governments of many countries around the world have defined a completely separate class of criminal offenses—computer crimes—that specifically criminalize a growing variety of behaviors ranging from deliberate distribution of viruses to theft or destruction of information from corporate or government computers. Other laws, such as the Economic Espionage Act and the USA Patriot Act, have also provided additional grounds for prosecuting computer-related crimes. Prison sentences for conviction on a charge of computer crime are now given frequently and can be substantial. In the United States, under current guidance from the attorney general, federal prosecutors are directed to seek maximum sentences for offenders, including computer criminals. Since parole has been ended in the federal prison system, it is fair to conclude that those convicted of federal computer offenses should be prepared to serve a substantial sentence in a federal correctional facility.

In fact, the white-collar crime with by far the fastest growth rate in the United States is identity theft. Because computers storing hundreds of thousands of personal records including names, Social Security numbers, birth dates, and other key identifiers are often insufficiently protected, they are a target of identity thieves. This information is either used by the thieves themselves to impersonate the victims or sold to others operating scams of various kinds.

Until recently, a person committing a computer crime was assumed to be a hacker who was some sort of warped computer geek, information technology specialist, or programming genius. Today, nothing could be further from the truth. In fact, anyone with access to a computer managing assets or confidential information is in a position to commit a com-

puter crime. The proliferation of computers and their ready accessibility have made them a target of opportunity for professional and amateur thieves alike. The result has been billions of dollars in losses from computer crimes, according to surveys by the Federal Bureau of Investigation and other bodies. In addition, a counterculture movement of computer misusers has published detailed instructions on how to compromise various kinds of computers and distributed the software with which to do it. No longer does the hacker have to be a computer genius; now all he or she needs to know is how to download and execute software and to follow instructions.

The high valuation the investment community places on companies providing computer security solutions is testimony to the significance of computer security to the modern organization. In light of the threat of cyber-attacks by terrorists or others that has been recognized since the attacks on the World Trade Center and Pentagon on September 11, 2001, there is an increasing awareness of the importance that must be given to computer and information security.

8.1.1 Security

Assuring security for a computer system is no different from having appropriate protection for manual accounting files or of any other recordkeeping system. Because of the disparity in technologies, each system requires its own particular security tools and methods. The objective, however, is the same: to achieve reasonable and cost-effective controls by which an unauthorized act is likely to be prevented or, if not prevented, at least detected. While each organization must ultimately decide for itself how much security is enough to meet its particular needs, standards, such as ISO 17799 (July, 2005)¹, are emerging that can serve as baselines against which to measure the state of information security in any given organization.

Of course, technology has changed radically over the last decade as companies have moved from large central systems (mainframes) to interconnected local and wide area networks (LANs and WANs). Many companies are looking into alternate technologies, such as grid networks, wireless networks, and biometric authentication. Of course, each of these technologies brings new security concerns. The Internet, for example, has made global e-mail a part of almost everyone's daily life. But the power of e-mail also makes companies concerned that it may be used to send out confidential information. In addition, the adoption period for other new technologies such as Instant Messaging (IM) is even shorter than it was for e-mail. The software for managing IM is less available whereas e-mail has a mature set of utilities to manage and even record messages.

There was a time when *security* meant locking the door to the room housing the mainframe. That is not enough any more. One central machine has been replaced by hundreds or even thousands of PCs (each probably exceeding the power of that old mainframe in many ways) connected into internal networks and most likely connected to the outside world as well through both private and corporate networks plus the global Internet.

Terms such as *firewalls* (programs and devices designed to prevent invasion of a system by an outsider) and *intrusion detection systems* (software and hardware designed to detect

¹ See <http://www.computersecurity.com/index.htm>

unauthorized activity within a network) had no real applicability to the world of computers as recently as 10 years ago but are now essential requirements for any reasonably managed corporate or government computer operation.

8.1.2 Evolution of Computer Crime

In looking at computer crime, it is important to remember that computers are just machines that carry out programmed instructions. When a crime involves a computer, the computer is not the criminal; the person manipulating the program or using the computer to perpetrate an illegal act is the criminal. Computers are an *instrument of crime* in the same sense that a phone or fax machine can facilitate the commission of an insider trading offense. While certain kinds of crime, such as planting a computer virus, would not be possible without a computer, others are simply new versions of old crimes that are now facilitated by modern computer technology. As that technology advances, criminal minds will inevitably continue to look for new ways to exploit the computer. Remember that some of our finer prisons teach computer skills to inmates as part of their education and rehabilitation programs!

For example, consider the theft of a new computer chip design. Printed out, the details of the design might require a dozen thick notebooks and a large roll of detailed circuit diagrams. That same information in computer form would easily fit on a tape cassette smaller than the common audiocassettes used for music, or on a “thumb drive” or hard drive with a diameter of one inch. The information could also be transmitted in minutes via the Internet as a file attached to one or more e-mail messages or even hidden within a photograph.

Most experts agree that computer crime is a growing problem and that the tools to prevent it are evolving, but so are new ways of committing those crimes. Feeling confident that your systems are 100 percent secure is *never* a good idea. Given the speed of evolution of both computers and the methods for committing computer crime, such complacency has become downright dangerous!

This chapter should provide you with a basic understanding of computer crime, how it has evolved, and the ways that computer criminals are likely to attack organizations such as yours.

8.2 COMPUTER-RELATED CRIMES

In today’s organizations, virtually every asset from money to proprietary and confidential information is likely to be recorded on some computer’s hard drive, and perhaps on a backup computer tape or disk. Every day trillions of dollars are transferred between bank accounts relying on computerized records and computerized data communications. Millions of individuals rarely see the inside of a bank. Their pay is deposited directly into their accounts and when they need cash they head for the nearest automated teller machine (ATM). Even many bills can be paid by direct transfers of money from their accounts to those of their creditors. Many other transactions that have traditionally required a visit to a bank branch can also be accomplished online via the Internet. Yet money may not be the most valuable commodity on the computer.

8.2.1 Intellectual Property

Intellectual property such as business plans and trade secrets can have immense value. There are unique differences between stealing information and stealing almost anything else. If \$100 is stolen from you, the thief has deprived you of your money. Similarly, if your car is stolen, the thief has it and you do not. A thief can steal information, particularly that stored on a computer, and you can still have it. If the thief is really skilled, your information can be stolen without you ever knowing an incident has taken place. Computers can thus be used to facilitate the theft of money by manipulating banking or accounting records, and goods by manipulating inventory, shipping records, or receivables records. Information is usually stolen by copying. Intellectual property theft is usually a combination of computer-assisted traditional crimes such as simple theft, insider trading, and so on, and of newly defined crimes such as economic espionage (theft of company secrets for the benefit of another organization) or computer intrusion (criminalization of unauthorized access into another organization's computers). Computer crime laws exist at both the federal and state levels in the United States and have counterparts in dozens of other countries. Some countries have very fine infrastructures for the investigation and prosecution of computer crimes. Others may have laws in place but lack the infrastructure to pursue prosecutions unless the victim provides the expertise to gather and analyze the evidence. Multinational organizations should bear this in mind in assessing risk.

8.2.2 Computer Hardware

Another class of computer crime attempts to target computers themselves. The intentional infection of your computer by a virus can cause a huge disruption of your business when it is triggered to destroy data, particularly if that data has not been backed up. In some cases, criminals may take more direct action to damage your computer. These attack profiles are sometimes referred to as *denial of service* attacks, because they are designed to deprive the rightful users of access to their systems. Other attacks may be designed to cause communication problems; for example, one disgruntled technician decided to bring down the communication links between the company's computers, in effect temporarily destroying the network.

8.2.3 Computer Crimes and the Law

Whether a target is the computer itself or the information residing in the computer, the attempted attack may well be a crime. For any act to be criminal, however, there has to be a law that declares that particular course of action to be criminal. Until the passage of specific computer crime laws during the past 25 years, prosecutors had had to find ways to apply traditional laws, such as those governing wire or mail fraud, to high-tech crimes. It is also important to remember that laws generally apply only within the state or country in which they are promulgated. Because the Internet can be accessed from anywhere in the world, perpetrators can carry out crimes from anywhere, especially from countries that have weak computer crime laws or from which extradition is unlikely. Some laws specifically require the victims to show that they had adequately safeguarded the information that was stolen or that they provided specific notification to the perpetrator that the information was not in the public domain.

Unfortunately, in our society, there are far too few law enforcement and prosecution personnel who are specialists in computer crime investigation. There are very specific procedures known as *computer forensics* that must be followed in handling and analyzing computer files and equipment if the evidence of the offense is to be admissible in a civil or criminal court. Carelessness in following these procedures may cause a prosecution to fail or a lawsuit to be dismissed. Corporations should be aware that even the most well-intentioned attempts of their in-house technical or investigative personnel to examine computers involved in an offense, unless conducted to very exacting forensic standards of data collection, storage and analysis, might result in evidence being rendered permanently inadmissible. Once a crime occurs, or a civil lawsuit is filed, a court is going to apply the appropriate rules of evidence to determine whether any of the actions taken in collecting, storing, or processing the data could have modified the evidence or otherwise damaged its integrity.

8.3 A BRIEF HISTORY OF COMPUTER CRIME

No one knows who the first computer criminal was. Undoubtedly, as soon as punch-card equipment came into use in the 1950s, someone figured out how to falsify records and make an illicit dollar. However, computer-related crimes have certainly been around since the early 1970s. Throughout the rest of that decade, computer crimes tended to focus on the manipulation of computer records to obtain money. In the 1980s, we began to see cases in which the target of the crime was the information on the computer. Insider trading was facilitated by the relative anonymity with which information could be accessed in many systems as well as the casual way that security was handled by many firms.

In one of the largest early cases, an insurance company took advantage of its accounting firm's computer *naiveté* to perpetrate a huge fraud. The insurer created thousands of bogus policies, identifiable through special policy numbers. When the auditors, as part of random checks, wanted to see some of these nonexistent policies, they were told the policies could be pulled from their warehouse and would be available the next day. The auditors never insisted on accompanying the client to the warehouse, but merely accepted that they could have the documents in the morning. That evening, the perpetrators busily created the appropriate documentation to prove the validity of the policies. Millions of dollars were funneled out of the company through this scheme. This case marked the period when auditors learned that it was vital to include computer systems in their audit plans.

In another noteworthy case, the chief teller of a bank located in Brooklyn, New York, devised a plan to manipulate dormant accounts using the bank's new computer system. He discovered that he could move money in and out of those inactive accounts simply by using his supervisor's key. Because he was highly trusted, his supervisor would give him the key whenever he asked for it without determining why he needed it. This control of the inactive accounts through the supervisor's key assumed the supervisor knew and approved every transaction involving these accounts. The careless surrender of the key to the chief teller nullified the whole security system and allowed him to withdraw several hundred thousand dollars. Even though the manipulations all showed up on the daily accounting reports, there were so many thousands of irregularities as a result of the changeover to the complex new computer system that the internal auditors were not able to keep up with the volume and ignored what they considered low-priority items, such as the dormant account transactions.

Unfortunately for the perpetrator, while he was a gifted fraudster, he was also a dedicated but spectacularly unsuccessful horseplayer. When the attorney general of New York State conducted a raid on his bookmaker, the volume of his gambling (generally around \$10,000 to \$12,000 per day) was discovered and the source of his funds uncovered. He was convicted of theft and imprisoned.

In another case, a young man in California discovered that the phone company had installed a system that permitted its employees to order equipment to be delivered to job sites using a push-button phone. He obtained the requisite code numbers from manuals recovered from the phone company's trash bins. Using the codes, he ordered the computer to arrange the delivery of equipment to downtown manholes. He then collected the valuable equipment with his own truck (bought at auction from the phone company and repainted in phone company colors), and eventually sold it to foreign phone companies. His scheme was discovered when he refused to give his truck driver a raise and the driver turned him in. It was shown that he had stolen about \$1.1 million in equipment. He was tried, convicted, and after a 90-day stay in jail, promptly established a business as a consultant to attorneys who defended computer criminals. His ads proudly proclaimed that he had "actual courtroom experience."

Today, computer crime has progressed from crimes committed by individuals against individuals and companies to a topic of great concern to governments: *Information warfare* has emerged as a real threat to national infrastructures. Indeed, the use of the Internet as a facilitator of communications by terrorists and as an instrument for the potential targeting of the information processing infrastructure is a matter of great concern to government and corporate security professionals alike.

8.4 COMPUTER CRIME TODAY

Computer crime is in the news. Whether it is the arrest of the creator of a damaging computer virus or a person using computers to sell child pornography, the media have realized that our society has become worried about technology failures. This media attention has had an unintended effect that can be a problem.

If you were to believe the media, hackers are the number one cause of computer crime problems. In fact, however, the major problem is computer-facilitated crime committed by employees and others who have been granted access to a system. Because the public perception of threats is often a key factor in deciding how to spend security dollars, what is actually a *misperception* may lead to an inappropriate allocation of resources with the result that the expensive new security measures do not address the real risk. Today, many companies are realizing that this misallocation may well be the case.

The problem of preventing computer crime is no different from that of preventing any other crime against a business. Accountants used to work to discourage crime by requiring separation of duties between people handling cash or other assets and those making the entries in the books of the company concerning the assets. By separating access to assets from access to the records of those assets, the theory was that two or more people would have to conspire to carry out a fraud and thus increase the likelihood of detection.

Along with separation of duties, accountants have traditionally depended on the paper trail of records that document transactions. This paper trail required that all transactions be

entered into journals that would be backed up by source documents such as invoices, purchase orders, receiving reports, canceled checks, sales receipts, and vendor invoices.

Of course, in spite of the best efforts of the accountants, fraud did, does, and will continue to occur. Accounting systems are neither foolproof nor fraud proof. Determined criminals can still find ways to circumvent or override controls.

Computers haven't really changed anything. A crook is still a crook. Fraud, theft, and embezzlement are still possible in the age of computers. Indeed, some argue that crime has become more likely as paper trails are replaced by electronic trails, which are not as easily verified by traditional methods. The speed of processing has taken precedence over maintenance of effective controls, according to some writers. CPAs should determine how to validate the information stored in computer systems. That has become more difficult as computer architectures have evolved from central mainframe computers to networks of hundreds or even thousands of PCs and file servers distributed throughout the company, and sometimes even throughout the world.

As stated earlier, surveys, including those conducted by the Federal Bureau of Investigation, the Computer Security Institute, and the American Society for Industrial Security, show that computer crime is responsible for billions of dollars of loss each year. Many of these surveys indicate that the average loss in a computer crime is higher than in other crimes. It is often more difficult to prosecute a computer crime than a traditional crime. Evidence taken from a computer is very difficult to connect to an individual because computer data can be manipulated. Therefore, providing proof not only that the crime occurred but also how it occurred and who committed it can be a complex process. Part of the problem, as noted earlier, is that there are a limited number of police and prosecutors who are trained in the investigation and prosecution of computer crime. However, forensic audit specialists that specialize in investigative computer techniques have access to an array of analysis programs that can be used to reconstruct data on hard drives and recover data and uncover what others think may be hidden. Even data that has been overwritten several times can sometimes be recovered, but such tools are not widely available and require skill and experience and patience to use. The curse of computer based fraud is that computers can be used to try to cover up the trail at the surface level, but the blessing is that some data just never seems to go away, having been stored in multiple places and accessible by the highly trained fraud professional.

In fact, new opportunities for theft, fraud, and embezzlement have been created by computer technology. Accounting records once kept under lock and key in the accounting department are now stored on computers that can be accessed remotely. The systems are available not only to authorized users (employees who have a job-related requirement to access and use the accounting system) but also to data entry clerks, computer operators, systems analysts, and programmers. If the computer's access control security system is not set correctly, unauthorized employees or even outsiders can gain access to the system. With the proper skills and a criminal inclination, individuals can manipulate systems and change programs not only to commit fraud but also to make it difficult to find evidence that the fraud has even been committed.

8.4.1 Classification of Computer Fraud

Generally, there is no accepted *chart-of-accounts* for computer fraud. If there were, it would constantly be changing. But certain computer-fraud activities that could affect a business's chart-of-accounts should be recognized: manipulating computer inputs, manipulating programs, and tampering with outputs.

Manipulating Computer Inputs

One of the most frequent bases of computer crime involves the falsification of computer inputs. Those inputs may involve putting false transactions into the system, modifying actual transactions or, in some schemes, not putting information into the system.

From an accounting standpoint, the main reasons for manipulating inputs are to overstate or understate revenues, assets, expenses, and liabilities. The objective of the perpetrator determines the manipulation necessary. Sometimes the objective is to provide false data to managers, stockholders, analysts, reporters, creditors, or government agencies. Sometimes the manipulation is part of an embezzlement scheme, such as entering false invoices into an accounts payable system. There can be little question that the manipulation of data is among the most common forms of computer-related fraud.

Input fraud should be among the easiest to detect and prevent with effective supervision and controls. These include:

- Separation of duties
- Audit trails
- Control totals and access controls (both those that limit access to data entry screens and those that place limits on values that can be entered)
- Appropriate testing of sample transactions

However, simple tests of accounting records and documents may not always reveal complex frauds. One computer-aided fraud that resulted in an SEC Enforcement and Administrative action was the case of Livent. The computer became an integral part of the fraud scheme. Lack of proper internal control and security and access controls, as well as knowledge of the audit approach by the controller, the former audit engagement partner aided a multifaced fraud. The SEC wrote:

Because of the sheer magnitude and dollar amount of the manipulations, it became necessary for senior management to be able to track both the real and the phony numbers . . . enlist the assistance of the manager of Livent's information services department to write a program that would enable the accounting staff to override the accounting system without a paper or transaction trail.²

More discussion of the Livent case is provided in the case summary at the end of this chapter.

Manipulating Programs

Another major class of computer crime involves altering the instructions computers use to manipulate input files and databases. These can range from schemes in which programs are

² United States of America before the Securities and Exchange Commission. Litigation Release 1095, Administrative Proceeding File No. 3-9806. See <http://www.sec.gov/litigation/admin/34-40937.htm>

designed to process fraudulent entries without making audit trail entries, to those featuring deliberate miscalculations to shortchange bank depositors of fractions of a cent of interest, which can then be accumulated and stolen. Programs may be designed with fraudulent intent from the outset or may be modified at some point to add the fraudulent activities. For example, fraudsters at a rental car company modified a computer program to add one gallon to the *capacity* of the fuel tank of cars returned with less than a full tank of gas. Each car was charged for being refilled plus an extra US\$3 for the phantom gallon. Multiplied by thousands of rental transactions per week, the amount of money collected was substantial. In another case, a program developed to calculate mortgage overpayments was adjusted by fraudsters to shave one day off of the overpayment period, thus reducing the amount to be refunded to the client but leaving one day's worth of the overpayment to be taken by the fraudsters. Again, while the effect on an individual account was small, the overall total across all accounts was massive.

Outsourcing program development to either domestic or international programming shops creates the risk that an unauthorized code might be introduced that would permit program manipulation at some future date. Obviously, any outsourcing plan should call for careful and thorough testing of the new code before assuming that it is completely accurate.

The elements of IT general controls practice that mitigates this risk are called program development and program change controls. Only authorized and properly documented changes to functioning code should be permitted. Access to programs and code should be restricted to those individuals whose programming or program implementation duties do not set up segregation of duties conflicts by their having access to accounting functions.

Tampering With Outputs

Yet another category of computer fraud involves tampering with the results of computer activity: reports and files. This category includes theft of confidential or proprietary information such as customer lists, research and development results, company business plans, employee information, secret formulas, and so on. According to the previously mentioned surveys, these intellectual property thefts are apparently escalating as global competition increases. Computers have undoubtedly facilitated the thefts because they have provided the capability for fast copying of huge databases and at the same time provided the capability for moving the copied data around the globe at tremendous speeds through data communications networks. Intellectual property theft by computer is a unique crime since nothing is physically removed and there may be no record that the crime even took place.

8.4.2 The Most Common Computer Crimes

Regardless of the evolution of computer technology, the manipulation of inputs and outputs is still the most common form of computer crime. (For a detailed discussion of financial statement fraud, please refer to Chapter 10, "Reducing the Risk of Financial Statement Fraud".)

Computers are frequently manipulated to get to assets, the most popular being cash, information that can be converted to cash, or both. To steal cash, input is frequently manipulated through submission of falsified documents such as invoices from vendors, suppliers or contractors; claims for government benefits; refund or credit claims; payroll, or

expense accounts. The phony claims can involve anyone from clerks to senior executives, although employees in either the claims approval or accounting functions are most often involved. From an accounting viewpoint, the false claim is a fake debit to an expense so a corresponding credit can be posted to the cash account to cover the issuance of a check or funds transfer.

Executive Computer Crimes

In the higher levels of an organization, the nature of fraud changes. Rather than simply grabbing cash, fraudsters may design account manipulation to exaggerate profits by overstating sales or booking them before the transaction is completed. A similar effect on profits can be created by understating expenses either through simple reduction of the numbers or improper deferral to a later accounting period. The playing of the nearly infinite range of variations on these themes depends only on the ingenuity of the perpetrators. For example, profits may be overstated by increasing ending inventory of manufactured goods or merchandise held for sale. These adjustments result in the understatement of the cost of goods sold and raise net profits.

Manipulation of operating results is probably more highly motivated today than ever before. With increasing stock market volatility as well as an insistence on continuous growth and on beating analysts' expectations every quarter, managers may turn to manipulation to borrow time in order to turn around what they believe to be temporary problems. With so much of their personal wealth tied up in company stock, managers have a tremendous motivation to keep the numbers where the market perceives they should be. Or manipulation may be done to make the company a more attractive merger or acquisition target on the assumption that in the course of the merger the falsification will be overlooked or attributed to some undefined error. Or manipulation may be done for personal greed; in many companies, the executive compensation plan is directly tied to reported results.

Executives often have the ability to direct that employees circumvent or "override the controls" to achieve management objectives, sometimes with fraudulent intent³. Executives at PharMor in the early 1990s, a large chain of pharmacies, directed the misstatement of computerized inventory amounts over several periods in order to enhance financial results. Despite the fact that its auditors, Coopers & Lybrand, found the fraud, creditors and suppliers of PharMor played havoc with the auditors in the courts and in settlements for not finding the fraud earlier.

As described later, executives of Livent directed the writing of a computer program to keep track of the elements of a multifaceted, complex fraud and to hide the fraud from the auditors.

8.5 FRAUD AND THE INTERNET

Some have called the Internet the best thing ever to happen to technologically minded fraudsters. The global Internet was, of course, never consciously designed to serve illicit purposes, but substantial evidence shows it has turned out to be a facilitator of fraud. This

³ An excellent reference is the AICPA's *Management Override Of Internal Controls: The Achilles' Heel of Fraud Prevention*. AICPA, 2005.

section looks at the characteristics of the Internet that make it “fraud-friendly,” the kinds of frauds occurring on a global basis, and some of the steps you can take to avoid becoming the next victim of an Internet fraud.

8.5.1 Fraud-Friendly Internet Characteristics

How Secure Is the Internet?

The Internet was never designed to be a vehicle for secure communication. Because the Internet evolved in a somewhat haphazard way and because no one really “owns” it, there is no central “systems administrator” to ensure that the Internet is a secure means of communications or to even guarantee its reliability. The Internet is run, to the extent that such a huge system can be said to be “run,” by a volunteer group called The Internet Society. The standards that let systems all over the world communicate through the Web, e-mail, instant messaging (IM), and so on, are orchestrated by another volunteer group called the Internet Engineering Task Force (IETF).

The IETF operates through a system known as Request for Comment (RFC). Proposals are written in documents called RFCs, and anyone is welcome to comment on them. Once the comment period has expired, the IETF looks at the comments and may decide to modify the RFCs or to issue them. The collection of all RFCs constitutes the operating rules of the global Internet. Nowhere will you find a guarantee that the Internet is secure, that communications cannot or will not be intercepted, that any message or data sent via the Internet will arrive on a timely basis or, in fact, that it will arrive at all. There is nothing in the RFCs that provides for positive authentication. As long as the Internet is provided with an Internet Protocol (IP) address that it can process, the messages go there.

So the would-be Internet fraudster starts out with the advantage that there is nothing in the underlying infrastructure that would stand in the way of carrying out almost any scheme that can be imagined. Added to this inherent openness is the weakness of procedures that have in the past characterized some of the companies that sell and register Web addresses. Consider all this, and you can begin to understand how fraudsters have been able to hijack Web sites and transfer message traffic intended for elsewhere to servers under their control. The bottom line is this: The basic structure of the Internet does not require any particular security. That being the case, only someone who is very *naive* would believe that the Internet is a secure vehicle where content should automatically be regarded as credible.

How Truthful Is the Internet?

Truth on the Internet is optional. You can say anything you want on the Internet, true or false, reasonable or unreasonable, for any purpose or for no purpose at all. There is a famous cartoon of a dog sitting in front of a computer typing away on the keyboard. The caption is “On the Internet, no one knows you’re a dog.” The ability to tell lies combined with the gullibility of a portion of the population has made some fraudsters very rich very quickly. You can create a Web site at no cost at any of a number of services in various countries and you can make the Web site look like anything you want.

A few years ago, a high-profile fraud was perpetrated in just that way. A posting on a financial bulletin board indicated that a company was about to be purchased by a foreign corporation. As evidence of the accuracy of this posting, the person provided a link to what appeared to be a page of the Bloomberg news service running a story on the takeover. The

price of the stock jumped almost instantly. The only problem was that there was no Bloomberg story. The takeover was made up and the Bloomberg page was a forgery. The perpetrator of this fraud was caught and prosecuted. There have been a lot of cases like this. False stories posted on message boards are legendary. During the Internet "bubble" of the late 1990s, even vague rumors could trigger massive buying or selling sprees in technology stocks and a number of people decided that this was a good way to get rich quick. Some were caught, others were not.

One other aspect of lies on the Internet involves the use of false identities. If you want to make a posting seem real, you can have 40 or 50 different "people" posting supportive information. Of course, all of them can easily be the same actual person using 40 or 50 e-mail addresses set up on various (usually free) services. The identities may be of real people whose names have been "borrowed" (without their knowledge or consent, of course) or just made up.

Anonymity on the Internet

Anyone can use any of the readily available tools to hide their identity and location on the Internet. The Federal Bureau of Investigation recently released a warning that people were receiving e-mails purportedly from the FBI asking for personal information. It is very simple to change the return address that appears on an e-mail. Anyone who knows where his or her e-mail system or browser stores his or her name and return address can change them. Further, there are services such as Anonymizer that will send your e-mails through a series of servers that will cause your location to be untraceable.

Tools can also provide you with the ability to browse the World Wide Web without having your actual location traceable. On a simple level, anyone can go to an e-mail service such as Hotmail or Yahoo and have a working e-mail account within five minutes in any name; there is no verification process to determine whether any information provided by the account holder is accurate. Similarly, free services such as NetZero or Juno will provide an e-mail address and very inexpensive Internet access. Sometimes, specials such as those sometimes used by AOL can provide free Internet time as an inducement to use the service. And terminals connected to the Internet are available at little or no cost at public libraries, Internet cafés, shopping malls, and in some airport concourses.

Physical Jurisdiction of the Internet

The Internet is global. It exists in cyberspace, which is unbounded. Just because a message seems to come from a given location is no proof that it is actually from there. In one recent case, a Web address indicated that the server was in Venezuela; however, it was determined that the server was actually in northern New Jersey. How was this done? Remember that every URL—for example, www.aicpa.org—must be translated to what is called an Internet protocol (IP) address.

An IP address consists of four numbers from 0 to 255, separated by dots, for example, 123.67.209.41. The Internet uses the IP address to route your message to its destination. The translation between the name you type and the IP address is handled by the Domain Naming System (DNS). When you register a URL, you have to provide the IP address of the DNS that will know the IP address to which traffic bound for that URL should be sent. It can be changed at any time.

Nothing in the technical underpinnings of the Internet prevents you from having a URL indicating that you are in Uruguay (for example, www.xyz.uy, where *uy* is the code for Uruguay) associated with an IP address of a server in a completely different part of the world. This is something often seen in the *.com* domain. People and businesses all over the world have Internet domain names that end in *.com*, but both they and their servers can be located anywhere.

For the fraudster, it becomes a relatively easy matter to have servers located in some jurisdiction that has weak computer crime laws even though the servers will appear to the Internet visitor to be local. Internet service providers (ISPs) are the businesses that provide the connection between you or your company and the Internet. As with any other industry, they vary greatly in size, experience, and security. In the majority of cases, you can establish an account on an ISP quickly and easily without ever physically showing up at the ISP's premises. It is all done through the Internet. So, a fraudster could easily set up a server through an ISP in a country with weak computer crime laws or in a country unlikely to cooperate with countries likely to be on his or her trail.

8.5.2 Computer Crime Laws

The Limitations of Computer Crime Laws

Computer crime laws are not universal. Many countries either have not promulgated strong computer crime laws or need to update them. Others have laws on the books, but no trained law enforcement or prosecutorial resources to enforce them.

Other countries have no laws whatsoever concerning computer crime. In addition, artificially created jurisdictions are on the rise. For example, the "Principality of Sealand" exists on a former World War II anti-aircraft artillery platform off the coast of England. An entrepreneur has declared it to be sovereign territory, appointed himself prince (and his wife princess), and his son (who is the current prince) is converting the platform into a computer-server farm where people can install servers that exist outside any normal jurisdiction. The prince has said that your data may "reside" on his territory as long as you do not break his laws: He does not favor child pornography, large volumes of junk e-mails or, according to a recent press release, terrorism. He will not recognize any other jurisdiction as having power over Sealand. No subpoenas or court orders from other nations will be accepted.

Even if computer crime laws have been enacted and cover a given jurisdiction, they may not be strong enough or current enough to be effective. There is a saying that computer technology advances at the speed of light, but computer crime laws advance at the speed of government. An example of a law that needed updating can be found in the case of the person identified as the creator of the "I Love You" computer virus. As the result of an international investigation by government computer-crime investigators from around the world working together in a model of cooperation, a suspect was arrested in the Philippines. The raid on his residence and his arrest were televised and the tape played around the world. However, he was almost immediately released after it was determined that the deliberate transmission of a worm or virus program was not a specific violation of then-enforceable Philippine law. (As you might have guessed, his release was not covered by the TV reporters. The statutes of the Philippines have since been revised.)

There is another problem in bringing identified computer criminals to justice. If a victim country wishes to extradite a suspect for trial, several hurdles have to be overcome. First, both countries involved, that is, the country of residence of the crime victim and the one where the alleged perpetrator is arrested, must be signatories to an extradition treaty that covers the offense. Second, the national government of the victim has to want the suspect badly enough to go through the considerable paperwork and costs associated with an extradition proceeding. At the same time, the country holding the suspect has to have an interest in extraditing him or her; there are all sorts of political reasons why that might not be the case. And finally, treaties typically have provisions stating that extradition can occur only if the alleged offense is, in fact, a crime in both countries. As a result, if the act is not a crime where the suspect is being held, extradition may not even be a possibility.

8.5.3 The Tools of Fraud on the Internet

Availability of Internet Tools of Fraud

The tools of fraud are easily available on the Internet. If you want to set up a Web site that appears to be that of an investment news service, nothing could be simpler. Just use utility programs to copy the page of the legitimate business, apply the right tools, and you can build pages that can convincingly spoof almost any other site. Need a logo? Unless a site has taken the right precautions, stealing a perfect digital copy of a logo or photo requires only a couple of mouse clicks.

Fraud-Friendly Tools

The tools to hide what you are doing are easily available. Programs like PGP (Pretty Good Privacy),⁴ can provide the encryption of messages or documents that are so strong that most governments around the world cannot break them. Worse, perhaps, are tools that involve what is called *steganography*. This permits a large document to be hidden within a picture without making perceptible changes in the image. To further assist the potential computer fraudster, many "underground" sites contain links to tutorials that teach newcomers how to exploit these capabilities.

Recordkeeping Limitations

Internet sites keep limited records. People who run Internet sites are not required by law or regulation (with very few exceptions) to maintain logs of access. Even where logs are maintained, the volumes of information involved become so large that the logs are not maintained for long. The result is that where a computer fraud occurs, there may be little evidence for investigators to follow to prove a case. This limitation is often not realized by companies until an incident occurs. With planning, it is often possible to structure a hierarchy of records where the most critical access records are maintained for a longer time than, say, routine access to records.

Policing the Internet

There are not enough qualified investigators to cover Internet fraud cases. The reality is that qualified computer crime investigators can make substantially higher salaries in the private sector than they can in government. Given the increased importance placed on security by corporations following the attacks on the World Trade Center and Pentagon on

⁴ <http://www.pgp.com/>

September 11, 2001, however, the demand for those skills is rising. As a result, it is anticipated that government law enforcement bodies will find it harder to retain top cybercops, in the face of the substantially higher pay scales in the private sector. Governments will not, therefore, be able to investigate all cases. That will be good news for the fraudsters. However, it must be said that the government's overworked computer investigative resources do a great job and, when combined with private-sector corporate resources, the picture for the fraudster is not as rosy as it otherwise might be. Add to this the policy determination by the U.S. Justice Department to seek harsher sentences for criminals, including computer criminals, and the risks for the potential fraudster are considerable.

8.5.4 Internet Frauds: The Top 10 and Beyond

Many characteristics of the Internet make it a more fraud-friendly environment than we might wish. After all, the impersonality of computer interface makes it easier for fraudsters to take advantage of their victims without having to face them; on the contrary, they may silently mock their victims for their greed and naiveté. Given these characteristics, what types of frauds can we see? Fortunately, the National Consumers League, in cooperation with the National Association of Attorneys General, the Federal Trade Commission, and Project Phonebusters in Canada, operates the Internet Fraud Watch, and keeps statistics on frauds. While there is no question that they do not receive reports of all frauds and their focus is consumer frauds, they are a good place to start. Following are important frauds that are not on their Top 10 list. The percentages noted are from the 2005 January to December survey.

The Internet Fraud Watch Top 10

1. *Online auctions (42 percent of complaints)*. These include receipt of counterfeit or shoddy products, payments sent without delivery of any products, and abuse of credit cards used for purchase payments. With the tremendous popularity of sites such as E-bay (which tries hard to control the fraud problem), fraudsters have found this to be a very effective way to get people to part with their money.
2. *General merchandise sales (30 percent)*. People who have been scammed on direct sales are amazed to find that the diamond-encrusted Rolex watch they purchased for \$99 from some Web site is not completely genuine. In one instance, the victim of a phony watch scheme was told that the "bargain" was only possible because it was part of a batch of watches on which the watch manufacturer Movado had somehow misspelled their own name. This category of fraud also includes all other merchandise complaints.
3. *Nigerian money offers (8 percent)*. This has quickly replaced the mailed letter as the preferred way of advertising for new victims in this classic fraud. This involves sending out an e-mail informing you that the sender is the widow of the late dictator of the country and that he socked away some number like \$80 million for a rainy day. Or, that the author is an executive of the Nigerian National Oil Company and that he and his associates have been receiving kickbacks of 1 percent, 2 percent, or 3 percent of oil revenues. In all cases, they have chosen you to assist them in laundering their dirty money. In return for supplying your bank account information, letterhead, and so on, you will be in for 20 percent or 33 percent or 40 percent or 50 percent of all those millions. Sometimes you have to kick in a couple of thousand dollars to show that you are committed to the scheme. If you fall for this one you should be committed. Not only have people lost many thousands of dollars, some have actually been murdered

when they journeyed to Africa to meet their “partners” in the scheme. The average loss is reported to be nearly \$7,000. What is more surprising is the advancement of this scheme in the ratings to number 3 over a few years.

4. *Fake checks (6 percent)*. These complaints are the result of bogus payment checks for goods or services.
5. *Lotteries or lottery clubs (4 percent)*. Fraudsters successfully extract from the victim a fee, but never deliver the promised winnings, many times referencing foreign lotteries. Fraudulent clubs to “pool” contributions and share winnings also ensnare the naïve.
6. *Phishing (2 percent)*. This scheme has come to be known by hackers as “phishing” (pronounced “fishing”). A well-known example was a message sent by hackers to millions of people telling them that unless they updated their “security information” they would no longer be able to be users of the E-bay service. Some of these “fish” bit and filled out detailed questionnaires with such information as Social Security numbers, checking account information, mother’s maiden name, and much else. Only after they discovered that they were identity theft victims did they realize what had happened. In other cases, phony emails from seemingly legitimate companies, complete with company logos and other identifying information representing themselves as ISPs, banks and major utilities have been successful in getting the unwary to cough up personal information. Why get dirty diving in a dumpster for personal information when you can extract that information in comfort? Legitimate businesses do not ask for this information via email.
7. *Advance fee loans (1 percent)*. This is another familiar fraud taken into cyberspace. The availability of “marketing” CDs containing millions of e-mail addresses combined with the essentially zero-cost of sending out large volumes of e-mail messages allow these schemes to be profitable even when a very low percentage of people fall for the scheme such as paying an up-front fee for a loan.
8. *Information/Adult services (1 percent)*. Pornography is one of the few consistent moneymakers on the Internet. Therefore, it is easy to see why entrepreneurial fraudsters have jumped on the bandwagon. The schemes range from the simple failure to deliver the smut promised and paid for to outright threats of cyber-blackmail, sometimes involving planting pornographic images of children on a victim’s computers. For consumers still using dial-up services, fraudsters can without your permission “connect” you to a remote site (e.g., where a phone number can be used to bill charges) and start to run up a charge for “services” which will be presented to you with your next phone bill, courtesy of your legitimate phone company. Always check your phone bill, and shame on the phone companies for doing business with “fronts” for scammers.
9. *Work at home (1 percent)*. This scam is as old as time; it boils down to taking the same old scheme and putting it on the Internet.
10. *Internet access services (1 percent)*. These complaints involve ISPs who fail to deliver. Often billing themselves as bargain basement ISPs, they cannot survive by providing unlimited access for only \$2.95 per month.

Beyond the Top 10

Internet Fraud Watch also lists some additional popular frauds against consumers, which include the following:

- Franchise opportunities
- Buyers clubs
- Credit card protection plans
- Credit repair services
- Magazine solicitations
- Pyramid schemes and illegitimate multilevel marketing
- Scholarship scams
- Sweepstakes and prize offers

In the area of frauds against businesses, the Internet has also proved to be a great facilitator. The schemes are as broad as the mind can imagine. Here are a few examples:

- Sending out fake electronic invoices for goods or services never provided.
- Selling stolen or false intellectual property. For example, “Hello. You don’t know me but I am a research scientist with XYZ Pharmaceuticals. I have the formula for our new Ultracillin drug and feel that the company has treated me badly, so I want to sell the formula to you. . . .”
- Involving a company in money laundering. Money launderers need legitimate companies with whom they can engage in falsified buy and sell transactions to carry out their illicit purposes. Sometimes the companies know that they are becoming involved in illegal dealings but don’t care. Other times, they claim that they never suspected that the duffle bags of cash came from inappropriate sources.

Avoiding Victimization

What can you do to avoid becoming the next victim of an Internet-facilitated fraud? Here are some tips.

- *Offers that are too good to be true are too good to be true.* Unless there is a rational explanation, people are not looking to give away products and services at a loss. This is not to say that there are not real bargains to be had. Quite the contrary, there are real deals out there, but you have to be wary. In one recent case, a computer peripheral was offered at a substantial discount (\$17.99 for a \$99.99 item). Investigation showed that the vendor had decided to rename the product and was dumping inventory with the discontinued logo. Another case (brand-new and reduced from \$100 to \$7) involved a device made by a manufacturer who had gone out of business. The liquidator was glad to get anything for the products. And a cellular phone that sells for \$400 without a service subscription may really be “free after rebates” if you sign up for service. But for the most part, impossible deals are impossible. Why, do you think, did the widow of that Nigerian dictator happen to select you from all the other people in the world to offer you \$17 million for your minimal involvement in helping her to get her late husband’s ill-gotten gains out of the country?
- Most reputable manufacturing and sales organizations do not use free e-mail services such as Yahoo or Hotmail as their primary cyber-communications vehicle. If the return e-mail address is at one of these free services, consider yourself warned!
- Giving your credit card information in an e-mail is essentially always a bad idea.

- Similarly, sending confidential personal information such as credit card application data in e-mail is a bad idea.
- Read the URL. If you are looking at a site that purports to be operated by a major corporation, it should be located at that company's Web site. It should not be at a source of free or very low cost Web site hosting such as Tripod, Geocities or Homestead. Be careful of Web site redirection in which, through the use of frame technology, actual Web addresses are hidden. Also remember that it is easy to set up a Web site that contains some unsuspecting company's name. An offer that has you respond to a Web site at <http://www.microsoft.joeshouseoffraud.com> is not the same as one that sends you to <http://www.microsoft.com>. There are also ways to disguise a URL in the form of a numeric address.
- Check out vendors before sending them a check. Due diligence operates in the cyber-world just as it does elsewhere. Check out those you plan to do business with. If they do not want to provide the information you need to do this, think twice about doing the deal.
- If you are the victim of a fraud, report it. Fraudsters depend on their victims not reporting their crimes. Even if it is impossible to prosecute them for what they did to you, your report may fit into a pattern that can lead to prosecution, to their being denied service by their ISP, to filtering by ISPs, or to other outcomes.

8.6 COMPUTER CRIMINAL PROFILES

Who commits computer crime? It would be useful to have a profile of the offender to use in perhaps predicting who might commit the crimes.

8.6.1 Predictions

In the 1980s, criminologists who focused their attention on white-collar crime argued that the perpetrators tended to be trusted employees with unresolvable personal problems, usually financial in nature. These included indebtedness as a result of illness in the family; problems with alcohol, narcotics, or gambling; expensive tastes; or sexual pursuits.

At about the same time, various studies provided a profile of the computer criminal. In this profile the culprit:

1. Is male, white, and between 19 and 30 years of age.
2. Has no prior criminal record.
3. Identifies with technology more than with the employer's business.
4. Is bright, creative, energetic, willing to accept challenges, and highly motivated.
5. Is employed in the field of either information processing or accounting.
6. Feels a desperate need for money because of personal problems.
7. Feels exploited by his or her employer and wants to get even. The culprit feels that promotions, salary increases, bonuses, stock options, and so on, are not fairly distributed. Others have gotten more than they deserve through various forms of favoritism.

8. Does not intend to hurt people, just the employer, who is perceived as cold, indifferent, uncaring, and exploitive.
9. Does not have a self-image as a criminal.
10. Believes that actions against *the establishment* are justified for political or social reasons.
11. Perceives beating the system as a challenge worthy of his or her efforts.

In addition, four frequently cited characteristics are symptoms of trouble:

1. *High living*. Not too long ago, eyebrows were raised at the programmer who showed up in the company parking lot in a new Mercedes convertible. However, in the turn-of-the-century marketplace, programmers who had been through one or two initial public offerings (IPOs) could easily afford any car they want. Nonetheless, a discrepancy between lifestyle and income must be regarded as suspicious.
2. *Ultra dedication to the job*. The bookkeeper or computer programmer who never takes a vacation is either very dedicated (increasingly less likely in today's business environment) or afraid that some scheme would come to light if he or she were not around to control things. In many states, banking laws, for example, require that bank officers take at least one two-week period of vacation and prohibit the officers from even visiting their office or accessing it remotely during that period. The theory, of course, is that many schemes will fall apart over a period of two weeks if left alone.
3. *Aging*. As some people age, they grow increasingly resentful of perceived wrongs; for example, the awarding of increased salaries and stock to younger employees. Therefore, they may feel justified in stealing if they think they can get away with it. For example, a period of continued layoffs may seem to the employee like the perfect time to get a final bonus by stealing some intellectual property or otherwise causing problems.
4. *Chronic lateness*. The common wisdom held that people who were constantly late with their work were late because they were trying to fabricate or cover up something they were doing.

In today's environment, how valid are these assumptions? Most perpetrators who are caught committing computer crimes are male, but a growing number of women are making their marks in fraud. Perpetrators also tend to be young. In spite of the previous lists, few indicators, however, actually have any kind of predictive power. Does this mean that the perpetration of computer manipulations is unpredictable?

Certainly, no simple test will detect whether a person who has never committed a crime in the past will or will not commit one in the future given the proper circumstances and motivations. However, a review of cases over the past few years reveals one interesting phenomenon: *Those who committed these offenses often had problems with former employers who were glad to be rid of them.* Companies that do not perform background checks that include contacting former employers and checking for falsification on employment applications are the fraudster's friend. The perpetrators can ignore their pasts and start anew at a company that appears to have weak security. Certainly, former employers can lie about an employee or refuse to give any reference beyond confirmation of employment. A thorough background check should pick up at least some potential problem employees. In one recent case, a company hired a woman and decided to save the cost of a background investigation because she was coming to work for them directly from another company known to conduct thorough investigations. After she sabotaged company systems, it was determined

that she had never worked for that other company and that the university that purportedly awarded her BA and MBA degrees had never heard of her. That initial lie of past employment was accepted and, as a result, her true background was never discovered.

Three other things about perpetrators are important. First, an offender does not have to be a computer genius to pull off a major fraud. People who can gain access to a system, either because they are authorized to use it or because the security controls are weak, can potentially manipulate that system for personal advantage even if they cannot directly access the computer. If they can fake the data by filling out a form, they can manipulate it.

Second, it is easy—but dangerous—to limit consideration of risk to employees. Many companies today, particularly in high-tech industries, make considerable use of temporary employees and independent contractors. All too often, because they are not carried on the books as employees, they are not subject to the same background checks and security measures. It should be clear that computers do not care whether they are manipulated by employees or independent contractors. Anyone who has access should be subject to the same controls as regular employees.

Third, there are offenders you will never meet, who will never meet you, but who may cause you great difficulties. These are the virus writers and virus distributors who develop and spread their plagues simply because they can.

8.6.2 Reasons for Committing Computer Crimes

Criminologists investigating why crimes are committed often use a four-element model, sometimes called MOMM: Motivation, Opportunity, Means, and Methods.

Motivation represents the reason one is willing to commit a crime. Motivation can be related to both personal or internal conditions and external conditions. Personal motivators include the following:

- *Economic.* Economically motivated perpetrators act to fulfill the need or desire for financial gain, money, or other assets or information that can be turned into money.
- *Egocentric.* Egocentric perpetrators have a need to show off their talents in committing what may be perceived by others as a complex crime. Money or other assets are sometimes part of the crime, but frequently they are not the underlying motivation. Certainly, assets symbolize a measure of the success of the venture and demonstrate the prowess and ingenuity of the criminal. Many hackers fall into this category. But for many others, their downfall is the need to brag about their exploits and thus gain favor in the eyes of their peer group.
- *Ideological.* Ideologically motivated perpetrators feel compelled to seek revenge against someone or something they perceive as oppressing or exploiting, either them personally, or even other individuals unknown to them. Terrorist bombings of computer centers are an extreme example of this kind of action. The sabotage of systems by disgruntled employees or ex-employees is frequently observed. Experts in terrorism have expressed significant concern that in a highly technological society, attacks targeting computer systems are likely. For example, an attack that disables ATMs in a region will cause disruption because banks have sharply reduced the number of tellers available for transactions. The lines in front of that limited number of tellers during the hours that banks are open would cause disruptions as banks try to figure out how to handle the

crowds. If the computerized traffic lights used in some cities were to be attacked, massive traffic jams could occur.

- **Psychotic.** Psychotic perpetrators are people suffering from delusional types of mental disease that distort reality by validating feelings of grandeur or persecution, or exaggerate hatred or fear of the organization or of particular people in the organization (often direct superiors). These feelings can be so strong that they may take extreme actions against their perceived enemies to relieve their anxieties. One way of acting out these feelings is exemplified by the person who shows up at the office with a gun and kills those he or she believes are “out to get them.” Another way this kind of troubled individual may lash out at these imaginary adversaries is to attack the computer systems that may be perceived as facilitating the work of supposed enemies. The subject of workplace violence is an important one, but is outside the scope of this *Handbook*.

Environmental Motivators

Environmental motivators are those conditions in the corporate culture or even in society in general that are claimed as motivators. But no external motivator can force anyone to commit a crime. It would be accurate to say, instead, that environmental motivators may aggravate personal motives. These include the work environment, reward systems, levels of interpersonal trust, corporate ethics, and stress and weaknesses in internal controls or security systems that may lead people to believe that they can get away with a crime.

It was indicated earlier that there are no guaranteed ways of spotting a computer criminal any more than any other kind of criminal and that people commit offenses for many different reasons. Does this mean there is nothing that can prevent computer crime? Nothing could be further from the truth. It may not be possible to know specifically who will commit a crime, but given the right circumstances someone is likely to try. The next section looks at the things a business can do to reduce the chance that it will be victimized by a computer criminal.

8.7 CONTROLS FOR PREVENTING AND DETECTING COMPUTER CRIME

It would be nice to assume that everyone associated with a business is honest. A totally honest workforce would certainly eliminate the need for controls to prevent crime. Of course, that assumption is not viable. People will commit crimes for many reasons, some of which are rational, others of which may make no sense to the observer. The larger the organization, the more likely it is that someone is out to commit a crime. Managers who subscribe to this belief are not necessarily paranoid. In fact, most managers can name their disgruntled employees.

There are those who will steal under the best of employment circumstances. Scott Charney, founding director of the Justice Department’s computer crime section and now head of security at Microsoft Corporation, observed that “at any given moment, there is a percentage of the population that is up to no good.”

Others would not steal even if they were the worst treated employees of Ebenezer Scrooge in *A Christmas Carol* (the pre-ghostly-visits Scrooge, of course).

8.7.1 Internal Control and Security Systems

Internal controls and security systems are designed on the basis of past experience, both in the company in which they are installed and in other companies. The challenge here is to build in enough controls to discourage and discover criminal behavior without breaking the bank in costs or going overboard on security. Companies that have been victimized often react by increasing controls to the point at which the controls can become oppressive and actually interfere with company operations. Although rational companies set up rules to define acceptable and unacceptable behavior, too many constraints make people feel oppressed, distrusted, and under constant surveillance. If the employees perceive what they consider to be excessive controls that make it difficult or impossible to carry out their jobs, they will put infinite energy into finding "work-arounds" that let them get their work done, even if these subterfuges violate the controls.

Since its very founding, our society has been based on freedoms and rights. Citizens highly value our freedoms of speech, religion, and assembly but these freedoms are not absolute. Citizens can speak their minds but cannot freely slander or libel another individual. Citizens cannot, as one famous jurist put it, feel free to yell "FIRE" in a crowded theatre. Citizens cannot trade on inside information or release secret company information without expecting to suffer legal consequences.

Well-designed controls should provide similar checks and balances. The risks, threats, and other vulnerabilities in today's marketplace and technological environment need to be considered, while responsibilities to employees, the value of their contributions, and their need for satisfaction in the workplace need to be taken into account. This consideration includes the provision of a work environment that encourages outstanding performance, profitability and efficiency.

A competent systems analyst or information security specialist can design layer upon layer of controls. Those in excess of what is required by the nature of the risks are not cost-effective. They can place undue burdens both on those who must work under them and those who must monitor and control them. A company's requirement for effective internal controls does not represent a justification for a siege mentality or the construction of an impregnable fortress. Done effectively, the development of internal controls is a matter of proper balance and equilibrium and should not create paranoia.

Looking at the potential for theft and fraud and the actions available to prevent crime brings forth several conclusions:

- Most prevention efforts focus on building more accounting, access, or physical security controls.
- It is vital to recognize that there are limits to technological and procedural controls. Given the speed with which computer and data communications technology evolves and the complexity of modern systems, it is difficult for improvements in protection and detection mechanisms to keep pace.
- It is also important for companies to recognize that improvements in the working environment, including a positive ethical climate and strong interpersonal trust, help discourage criminal thinking and behavior and, as a result, are a part of the control environment. Some factors in the business environment are likely to encourage

computer crime and others discourage it. Clearly, the need is to minimize the criminal behavioral motivators and maximize the non-criminal motivators.

8.7.2 Factors That Encourage Computer Crime

The factors that enhance the probability that a company will be the target of theft, fraud, embezzlement, and corruption, including computer crime, can be either motivational (related to the corporate reward system and company policies) or personal (related to the character of a particular perpetrator).

The following are motivational factors that encourage computer crime:

- Inadequate rewards, including pay, fringe benefits, stock and stock options, bonuses, incentives, perquisites, job security, meaningful work, and promotional opportunities.
- Inadequate management controls, including failure to communicate expected standards of job performance or job-related behavior, ambiguity in work roles, relationships, responsibilities, and areas of accountability.
- Inadequate reinforcement and performance feedback mechanisms, including lack of recognition for good work, loyalty, longevity and effort; lack of meaningful recognition for outstanding performance; delayed or nonexistent feedback on performance inadequacies or unacceptable on-the-job behavior.
- Failure to offer counseling when performance or behavior falls below acceptable levels.
- Acceptance of mediocre performance as the standard.
- Inadequate support and lack of resources to meet standards by, for example, not providing authority to hire sufficient personnel to meet requirements for quality, quantity, and timeliness of work produced.
- Inadequate operational reviews, audits, inspections, and follow-throughs to ensure compliance with company policies, priorities, procedures, and government regulations.
- Condoning inappropriate ethical norms or inappropriate behavior. If potential perpetrators believe that the company will not report their activities to the police, but would rather handle the incident through a quiet resignation, the deterrent effect of a potentially long prison sentence disappears.
- Failure to control hostility generated by promotion or destructive competitiveness among departments, offices, or personnel.
- Failure to control bias or unfairness in selection, promotion, compensation, and appraisal.
- An uncertain future where a company faces merger, acquisition, or failure.

The following are common problems that can become personal motivations for computer crime:

- Inadequate standards of recruitment and selection
- Inadequate orientation and training on security matters and on sanctions for violating security rules
- Unresolved personal financial problems
- Unresolved problems relating to personal status

- Failure to verify prior employment history, educational qualifications, financial stability, and character before appointments to sensitive positions
- Inadequate control of the level of job-related stress and anxiety
- Inadequate employee communication programs to monitor and help relieve uncertainty and anxiety among employees

8.7.3 Factors That Discourage Computer Crime

Computer crime can be discouraged through measures designed not only to prevent crime but also to detect attempts to engage in computer crimes. The recommended prevention measures are the following:

1. *Internal accounting controls.* These traditional measures to discourage crime are as important in an automated environment as in a manual-processing environment. They include the following:
 - Separation and rotation of duties. As personnel change jobs, so must their access codes be changed to match their current job requirements.
 - Periodic internal audits by trained, competent personnel, surprise inspections, and computer security reviews.
 - Absolute insistence that control policies and procedures be documented in writing.
 - Dual signature authorities, dollar authorization limits, expiration dates for signature authorizations, and check amount limits. These should be established and audited both routinely and by surprise.
 - Offline controls and limits, including batch controls and hash totals.
 - Feedback mechanisms to permit employees to report problems in security or control without fear of retribution.
2. *Computer access controls.* These controls may include the following:
 - Authentication and identification controls, including keys or smartcards, passwords, biometrics, callback systems, one-time passwords, time- and day-constrained access, and periodic code and password changes.
 - Compartmentalization, also known as need to know.
 - Use of encryption to protect data while stored or in transit.
3. *Firewalls.* The use of firewalls and similar safeguards prevents unauthorized access through the Internet. Firewalls, however, are only effective when they are properly sited within the company network and when they are properly configured. A very small error in entering a firewall configuration file may result in the firewall not providing the security that users and management expect.

The measures to detect attempts to commit computer crime include the following:

1. A system of logging and follow-up of exceptions should be designed and implemented to log unusual activities; procedures should be in place to follow up on reported exceptions, such as the following:
 - Transactions that are out of sequence, out of priority, or otherwise out-of-standard
 - Aborted runs and entries, including repeated unsuccessful attempts to enter the system
 - Attempts to access applications or functions beyond a person's authorization

2. Logging and following up on variances should be able to indicate a problem may have occurred or is occurring.
3. General logging should be in place because, when problems are uncovered, logs of access, Web activity, and other actions, may be vital evidence in tracking down the person involved. Logs should be maintained for at least a few months before being erased. Large log files can be filtered so high-risk transactions can be registered at a lower volume, thus permitting longer storage of the log.
4. Awareness of employee attitudes and satisfaction levels should be developed and maintained.
5. Sensitivity should be developed and maintained to reports that particular individuals are having problems, living beyond their means, or talking about “getting even” for perceived slights.
6. Newly developed *intrusion detection systems* should be used that have artificial intelligence capabilities to detect unusual transactions flowing through a system. These are evolving and have the prospect of being an order-of-magnitude improvement in crime detection technology. Several specialized companies can now help manage such systems and provide remote monitoring and response assistance 24/7. For many organizations, these third-party monitoring services can be a very cost-effective way of maintaining a constant watch on their systems.

8.7.4 Information Technology Controls for Compliance with Sarbanes-Oxley

Information technology is a complex and important part of any internal control system since it records transactions, transfers information, constructs databases, provides e-mail systems and gives access to the Internet. It is also open to tampering through unauthorized use for the purpose of manipulating data.

To be compliant with the requirements of Sarbanes-Oxley, reference must be made to the COSO framework for the implementation of a system of control that will meet the standards acceptable under the SEC final rules. The COSO framework divides IT controls into two types:

- General controls
- Application controls

General controls include:

- Data center operations
- Systems software controls
- Access security
- Application system development and maintenance

Application controls manage data processing to ensure completeness and accuracy of transaction processing as well as a proper interface between applications.

Within the COSO framework, guidance will be needed for the information technology that manages financial information, and disclosure controls and procedures. The 1992 COSO *Internal Control—Integrated Framework* document lightly touched on Information Technology

controls within the Framework. However, the 2006 release of the COSO's *Internal Control over Financial Reporting—Guidance for Smaller Public Companies* provides much more discussion of the role of IT controls in meeting organizational control objectives. Although not officially linked to COSO or to the Sarbanes-Oxley requirements, the COBIT (Control Objectives for Information and related Technology) framework of the Information Systems Audit and Control Association (ISACA) is a respected framework for an analysis of IT controls effectiveness, but is very detailed. Many IT professionals, however, believe the COBIT framework is an acceptable tool in meeting SEC and PCAOB requirements. In a recent guidance document entitled "IT Control Objectives for Sarbanes-Oxley," the IT Governance Institute (ITGI) has taken COBIT and linked it to the COSO framework on the implementation side and to the PCAOB standards, especially AS2, on the audit side, and has simplified and reduced the number of control objectives that are illustrated in COBIT.⁵

Beyond the public company environment, the same IT framework applies to all entities. COBIT and the ITGI publication can be valuable to an entity in understanding the elements of IT controls and in self-assessment and upgrading controls. Auditing standards for non-public entities also emphasize the role and importance of IT controls, and beginning in 2007, the auditor's explicitly required understanding of risks, will include internal controls, which in turn includes significant, relevant IT controls.⁶ Significant deficiencies and material weaknesses identified by the auditor will be annually communicated in writing to "those charged with governance" in private companies (this Standard is actually effective for most private company audits in 2006⁷).

COBIT takes off from the premise that the job of an IT system is to "[e]nsure the delivery of *information* to the business that addresses the required information criteria." This result is achieved by "[c]reating and maintaining a system of process and control excellence that considers all IT resources."

IT controls must be maintained to avoid the creation of what the PCAOB calls a "material weakness" which would result in an adverse report on the effectiveness of internal controls for those companies reporting under Section 404 of the Sarbanes-Oxley Act. Information from the early implementers of Section 404 indicates that IT general controls, especially access and security controls, were often remediated during the assessment process, even in the largest "well controlled" companies.

The criteria of an effective IT system are:

- **Integrity:** accurate and complete information created through valid and authorized transactions
- **Availability:** information available when needed; software and hardware available because safeguarded
- **Compliance:** meeting the standards of information required for management to comply with SEC, Internal Revenue and other laws and regulations

⁵ For further information, see the ISACA Web site at www.isaca.org or the ITGI Web site at www.itgi.org.

⁶ SAS No. 109 *Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement*. AICPA, 2006

⁷ SAS No. 112 *Communicating Internal Control Related Matters Identified in an Audit*. AICPA, 2006.

Secondary qualities applying to all information are:

- *Effectiveness*: relevance, timeliness, correctness, consistency and utility
- *Efficiency*: optimum and maximum use of resources
- *Confidentiality*: protection from unauthorized disclosure

IT system controls need to be treated separately because of the key role they play in information assembly and processing and, therefore, the risk their abuse presents to the internal control over financial reporting. Massive amounts of sensitive financial data are carried in vulnerable databases. Once access is gained, even authorized access by a person with criminal intent, data can be manipulated for fraudulent purposes and the reliability of the reporting process compromised. According to the IT Governance Institute, the basic body of general IT controls is a set of controls over:

- The IT environment
- Computer operations
- Access to programs and data
- Program development and changes

The IT Governance Institute lays out what it calls the “compliance roadmap,” which is a series of nine steps to bring a company’s IT system into compliance with Sarbanes-Oxley. Key among these are:

- Plan and scope
- Perform risk assessment
- Identify significant accounts/controls
- Document control design
- Evaluate control design
- Evaluate operational effectiveness
- Identify and remediate deficiencies

Plan and Scope

Given the fact that the SEC final rules limit control compliance to internal control over financial reporting and those system components that do or can influence financial reporting, not all IT processes of a given company will need to be reviewed. All applications, systems and their physical locations, functions, and uses should be ascertained, however, before beginning any review. A careful review of such an inventory may reveal that certain production statistics are used to monitor financial information results, or that the maintenance of certain regulatory reports might be critical to some elements of a disclosure. Thus, there may not be a simple “bright line” that easily classifies the systems and their relation to financial reporting.

The financial reporting process and its supporting IT systems and subsystems must first of all be distinguished from all the other IT systems. The most important systems affecting financial reporting will be those controlling:

- The initiation, recording, processing and reporting of financial information
- The selection and application of GAAP-compliant accounting policies

- Antifraud programs
- Accounts involving judgments and estimates
- The period-end financial reporting process including journal, general ledger entries as well as adjustments to the financial statements

Perform Risk Assessment

Once the components affecting the internal control of financial reporting have been identified, the risk assessment can begin. Determination of the risk level will simultaneously reveal the documentation and testing required to measure the effectiveness of the controls: the greater the risk, the greater the need for testing and documentation. The relative risks of centralizing processing here or outsourcing overseas must also be evaluated. If most processing is outsourced overseas, the risks at each location must be assessed.

Failures that would have direct and immediate consequences are:

- Security breaches
- Implementation of an unapproved change
- Unavailability of the system/application
- Failure to maintain the system/application
- Calculation, completeness and other integrity failures

Identify Significant Account/Controls

As noted above, the two broad categories of IT controls identified by the COSO framework are general controls and application controls. General controls are those that support the continuous working of all information systems. These include data center operations, acquisition and implementation of operating systems, access security and application system development. Application controls govern information processing and are designed to ensure completeness, accuracy, authorization and validity.

Document Control Design

This may be the most difficult part of demonstrating effective IT controls for many companies. For example, the PCAOB requires that documentation of controls when an audit of internal controls is required must be sufficient for the auditor to be able to evaluate the effectiveness of the control. This means that management itself needs to have sufficient documentation to be able to attest to the effectiveness of the internal control over financial reporting. Documentation will be needed to describe the control design and effectiveness in providing accurate financial reports, preventing and detecting fraud, safeguarding assets and the results of management tests of the system. This documentation can take many electronic and paper forms, including manuals, process models, flowcharts, job descriptions, etc. Inadequate documentation is considered by the PCAOB to be a deficiency in the control over financial reporting. The aforementioned COBIT and ITGI guidance documents identify control objectives that are useful in assessing the completeness and effectiveness of the design of control procedures.

Evaluate Control Design

The evaluation of control design must review any of the four key types of controls that are integral to meeting the control objectives for any of the five components of internal control:

1. Preventive
2. Detective
3. Automated
4. Manual

This review will evaluate their effectiveness in controlling risk by audit assertion. What might have been an adequate design to meet a tolerable business risk due to the cost-benefit of implementing a better control may now be inadequate to meet the standards of effective implementation when independent attestation of controls effectiveness is required by the external auditor.

Evaluate Operational Effectiveness

Evaluating operational effectiveness means regular system testing. The general controls that govern all systems including those controlling financial reporting should be tested frequently since a breakdown at this level will have far-reaching consequences. Effective IT general controls can be used to limit the testing in any automated controls operating under the general controls. Otherwise, the underlying application controls need to be tested often to ascertain continued effectiveness.

Of special concern here is the quality of testing done at any external service organization performing outsourced services. For example, payroll is often prepared by a service organization, rather than performing this task internally. The risk is that IT controls at a service company in, say, India might be adequate to meet company reporting standards but may not be sufficiently evidenced to meet US auditing standards. In this case, the company is forced to rely on the service organization's auditor. In the United States, a "SAS 70" service auditor's report is an auditor-to-auditor communication that can be useful to management and the auditor in ascertaining that the design (Type 1 report) and effectiveness (Type 2 report) of the service organizations controls are worthy of reliance. In an audit of internal controls, or where an auditor wishes to place high reliance on the service organization's controls, a Type 2 report, relatively timely with respect to the "as of" reporting date by the company, should be obtained. If such a report is not available, the controls of the service organization should be examined directly or the inputs and outputs to the service organization should be controlled and tested.

Even more troublesome can be entire functions like IT management or the entire accounting system that becomes outsourced as an efficiency measure. Although such arrangements can be beneficial, management remains responsible for the function and its effective operation from the perspective of maintaining effective control. The more distant the service organization is from the other parts of the business, and the less controlled the business environment is in which the service organization is located, the higher the risk that information or assets will be vulnerable to misappropriation.

Identify and Remediate Deficiencies

The criterion by which an internal control is judged to have a significant deficiency or a material weakness is the effect it will have on the ability of the system to produce reliable financial statements. Although IT general controls over application controls are important, they do not "per se" cause misstatements, but permit them to occur in the underlying application controls. The application controls governing financial reporting are the "source"

of problems and should be the most thoroughly tested and tested near the reporting date. All remediation must have taken place in time for management to meet the "as of" date that will appear in the annual report and 10-K.

8.7.5 Security Countermeasures to Computer Crime

The focus of Chapter 4 of this *Handbook* is computer security in general. General reference works go into much more detail concerning computer practice and computer security than can be provided here.⁸ The focus of this section is the specific measures that are often used to prevent computer crimes by those either inside or outside an organization. While some measures are applicable to almost all situations, it is vital that each organization considers those controls that are appropriate to its particular circumstances.

Security Holes

One of the unpleasant realities of today's systems environment is that the systems used, including operating systems, firewalls, and security packages, as well as application systems, are not perfect when they are released by the manufacturers to their customers. Security problems are discovered regularly. Information about ways to exploit security holes is quickly reported worldwide by independent bulletin board systems, government-funded sites such as the U.S. Computer Emergency Response Team at Carnegie-Mellon University, private sector monitoring sites such as that of Internet Security Systems (ISS), and the software manufacturers themselves. Sometimes the problem and the ways to exploit it are reported before a repair patch can be developed. It has become absolutely vital, therefore, that every organization monitor these information sources to be certain that all relevant holes in security are understood and closed as soon as possible.

If the hole is not closed, and experience indicates that this is often the case, a company can continue to operate with known holes in its security. It is also vital that the internal auditors understand the importance of monitoring and closing software holes and that this is included in the review plan.

Not all updates recommended by vendors are critical security issues. Some are for efficiency, some are to provide new features, some correct functionality problems. Each company must evaluate which updates are critical. A substantial cost is involved in constantly updating systems, and each update could introduce new problems.

It should also be noted that in addition to patches, there is a second, closely related issue called configuration. Unless the right selections are made in setting up software for use, security may be at a lower level than it ought to be. Improper configuration may result in security features being turned off or security warnings being ignored.

Computer Access Control

Controls that allow only authorized people access to sensitive systems include the following:

- *Passwords.* Use passwords that are long enough to be difficult to guess. Passwords should not be composed of simple words, names of relatives, and so on, and should be changed

⁸ For example, *Information Technology Audits* by Xenia Parker. CCH. 2006.

regularly. Some organizations have had good results by requiring every password to combine upper and lower case letters, numbers, and special characters.

- *Compartmentalization.* Restrict users to the specific files and programs they have a job-related need to access. This requires updates as necessary to conform access to needs of people moving from assignment to assignment within the organization.
- *Use of biometrics.* Use fingerprints, iris recognition, hand geometry, and other new technologies for added measures of control.
- *Use of one-time passwords.* Use hardware or software that generates a new password for each access. This may be generated through the passage of time or using a calculator-like device to enter a randomly generated “challenge” number and get a response number that is then entered into the computer to validate identity.
- *Automatic log off.* Use this measure to prevent unauthorized access to the system when authorized users fail to log off.
- *Time-day controls.* Restrict personnel access to those times when they are supposed to be on duty. An extension of this concept for companies using automated time clock systems is to deny access and report a violation if access is attempted when an employee is not shown in the time clock system as being present.
- *Dial-back systems.* Use these systems when access is through a dial-up system. On accepting a user ID and password, the system hangs up and dials an established number at which the approved user is standing by. This is very helpful when a person works at a predictable location, for example, the home office of a telecommuting employee.
- *MAC address controls.* Where an employee is located at the end of a broadband connection, it may be possible to limit connectivity to your system only to those physical devices you have authorized. Every Ethernet adapter, for example, has what is called a Machine Address Control (or MAC) address unique to that adapter.
- *Random personal information checks.* Implement this means of identifying unauthorized log-in attempts. The system randomly transmits a question that only the authorized individual could answer and denies access unless the right answer is received. If several personal questions are on file, this technique can be very effective.
- *Internet authentication.* Use this control for telecommuting employees. With telecommuting on the rise, many companies are taking advantage of low-cost, high-bandwidth Internet connections such as asymmetric digital subscriber lines (DSL) and cable TV modems, which offer download speeds of up to 1.5MB per second and uploads of 400KB per second for nominal monthly charges, and include continuous access, twenty-four hours a day, seven days a week. The connection between a user’s computer and a company server can be encrypted with simple tools like SSL (Secure Sockets Layer).

8.7.6 Solutions

When investigating computer crimes, investigators and forensic accountants often discover what could have been done to prevent the crimes. The following are some of the most frequently found items. The organizations failed to:

- Have written policies and security rules for the use of computers and systems.

- Have temporary employees and independent contractors follow the same security rules as regular employees.
- Adjust access as people changed responsibilities internally.
- Keep up with and close security holes in applications, firewalls, and operating systems.
- Maintain virus protection on a fully updated basis.

Some of the suggestions to improve computer security include implementing the following:

- More effective policies for security over proprietary information
- Better interaction between the human resources department, the systems department, and corporate security functions
- Better internal accounting controls
- Better supervision of those with sensitive access to systems
- Better employee instruction in security issues
- Better computer audit software
- Better software security
- Better physical security in the workplace

8.8 COMPUTER FRAUD, COMPUTER EVIDENCE, AND THE SCIENCE OF COMPUTER FORENSICS

8.8.1 Why Computer Evidence Has Become a Vital Consideration in Fraud Investigations

With virtually every document in today's organizations prepared on some kind of computer, the odds are that evidence of fraud will be found on the spinning surface of a hard drive, or stored on a backup tape or optical platter (CD/DVD). Some of the data needed by the fraud investigator or forensic accountant will be easily retrievable. But there are many instances in which data that would prove vital to an investigation is not available to the average user. *That does not mean that the data are not there; it simply means that tools and technologies that would not be used in everyday computer usage must be brought to bear.* And because of the sensitivity of the data and the possibility that any data brought to light may represent potential evidence that might be important in a civil or criminal proceeding, it is vital that it be handled in a way consistent with good evidence-preservation procedures.

To explain computer evidence, and how it can be retrieved and authenticated for use in a fraud investigation, this section begins with a brief consideration of why data can exist in ways that are outside of a user's control.

8.8.2 The Complexities of Data Storage: Looking Under the Hood

You don't have to know how an internal combustion engine works to drive your car or know how a TV works to watch your favorite shows. Similarly, you don't have to know how a computer works to use it, but when it comes to computer evidence issues in fraud investigations, it pays to have some level of knowledge.

The first thing to remember is that you tell the computer what you want to do (by clicking icons or entering data or text on the keyboard). In a very real sense, however, the computer is actually being run by the operating system (for example, Windows, Mac OS, Linux, or Unix) and the application program that is used to perform the functions you want to perform (for example, Word or WordPerfect for word processing, and Outlook or Lotus Notes for e-mail). In fact, the operating system mediates almost everything, passing your inputs to the applications and the outputs of the applications to the screen, storage drives, printers, or data communications lines. The operating system also can provide for connections between applications. For example, if you have written a document and want to save it as an Adobe Portable Document Format (PDF) file, the operating system can transfer your document from your word processor to the Adobe Acrobat software, and then store the resulting PDF file on the hard drive.

Application programs also generate evidence that is often overlooked. For example, word processing programs generate automatic backup copies of files during editing. When you choose to print a document, the application creates a temporary file with the current document in it so you can continue the editing process while you wait.

A brief look “under the hood” shows how much computer-based evidence is potentially available, provided you know how to obtain it, analyze it, and use it most effectively to support investigations. There are cases, however, in which the examination of files may result in a breach of privacy or even constitute a crime under relevant laws, such as the Electronic Communication Privacy Act. Investigators who wish to access computer files should consult with a qualified lawyer to make sure that they will not get themselves or their investigation into trouble. There are many places on a typical PC where potential evidence relevant to a fraud investigation could be stored.

Standard Files

Data on a PC can simply be in a regular file easily accessed or copied with the normal operating system tools. Looking at the file without taking the proper forensic precautions can cause changes in the internal structure of the file that could create severe problems in later forensic analysis or in getting data admitted as evidence. For that reason, viewing standard files without the right tools and techniques may result in the file being changed and may render the information inadmissible.

When a file is “erased,” the first letter of the file name is changed to a special character; the actual data that makes up the file are not deleted or overwritten. This special character tells the operating system to act as if the file is not there and indicates that the areas on the hard drive where the data are stored are available for reuse. The data are still there; however, the operating system is just treating it as invisible. Until the data are actually written over, however, forensic specialists can see the contents; in effect they have the ability to “un-erase” the file.

A higher level of erasure, called “formatting” (using the Format C: command in DOS), is commonly believed to destroy all data on a hard disk completely. This is not always true. Formatting is often done in what is called a high-level format, which resets the index of files on the hard drive but does not erase the actual data. The right tools often make it possible to recover either entire files or portions of files. Sophisticated programs are used by governments and by forensic auditors that can read information that has been written over, even many times. Other software that attempts to completely clean the information from

the computer needs to be used when a full erasure is desired, but even the commercial versions of those programs can be interrogated and some data recovered.

E-mail Files

E-mail has become ubiquitous. Billions of messages are carried across the global Internet or moved within corporate mail servers every day. People use e-mail so routinely they may use it to transmit information that should not be sent in this way. It is often vital to be able to search and review e-mail message traffic to identify potentially useful evidence.

Different e-mail systems operate in different ways. Some use network-based disks as their primary message storage, while others download all of the messages to the end user's PC and delete them from the server. Microsoft's Outlook, for example, works by storing messages on the network mail server and transmitting the data to the PC as needed. Recovering e-mail files can be complex.

Unless you have specialized recovery tools, even the straightforward process of getting e-mail messages off a backup tape can be a big job, requiring you to rebuild the mail server completely. With the right tools, it is possible to search and extract data from e-mail backup files efficiently.

Instant Messaging

Instant messaging (IM) has become a very popular means of communication between people who are online simultaneously. Although IM traffic is not always recoverable, it is sometimes possible to recover some portion of the records to see who was communicating with whom, when, and what they were saying. In some industries, such as the investment business, where orders are accepted through IM or e-mail links, regulation may require an organization to maintain copies of IM traffic (and e-mail, voicemail, and phone call recordings) for a specified period.

Temporary or Transitory Files

Application programs such as word processing or spreadsheet programs often create temporary files to be used while the program is running but are often erased before the run ends. The key to harvesting application programs for electronic evidence is the user does not control these files and usually does not know that these files have even been created and erased. One example of this is a print buffer file, a file created by a word processor to transmit data to the printer and erased as soon as the document is printed. When these files are recoverable, it is possible to see what the user printed but never intended to store. In one case, such evidence helped identify an employee in a securities trading room who was writing threatening messages to a coworker. The perpetrator entered the data on her word processor without saving it, hit the print icon, and then shut down the program, believing the message had not been saved. When the files were recovered, it was possible to determine the exact time they were printed and then to use a security camera video to see who was sitting at that machine at that time.

Swap Files (Cache Files)

The operating system maintains a number of files for managing storage, temporarily storing memory data on the hard drive, and other purposes. One of the key files of this type is called a swap file, which the operating system uses to store megabytes of data and all of the decisions about what is stored and when it is stored. The typical user is unaware of the

existence of this hidden file, which can contain a wide variety of information whether the user ever intended it to be stored or not. The swap file can be searched and analyzed in the course of a computer forensic examination.

Audit Trails, Usage and Firewall Logs, and Systems

The various components of modern systems applications, firewalls, and proxy servers often keep logs of their activities. Because these log files sometimes are available only for a short time, it is important to act quickly to capture them to maximize the amount of information that will be available to assist the investigations team. Most users are unaware of the existence of these files, although in sophisticated cases of hacking or systems intrusion, perpetrators often try to disable or destroy the log files that record their misdeeds. For this reason, it is obviously vital that systems managers take steps to severely limit who can gain access to the log files, turn log recording on and off, and erase them.

Compressed Files

Despite existing hard drive storage space, the advent of inexpensive CD-ROMs capable of holding 700MB of data, DVD-ROMs that can carry almost 5GB of data, and the promise of even larger storage media, it is still common to find files stored in various compressed forms to save space. Compression permits more data to be transmitted in less time. File compression is particularly popular for files intended to be transmitted across the Internet where some parts of the transmission line may operate only at dial-up speeds. The most popular format is the zip format. While these files are compressed, in general they can be treated like any other file. Some software that creates and processes zip files can also password protect them. The password is subject to reverse engineering and generally can be recovered with the right software and hardware tools.

Encrypted Files

Encryption subjects an original file (plain text version) to various substitutions and mathematical operations to generate a file (encrypted version) that cannot be read by unauthorized people. The rules by which plain text files are converted into encrypted files and vice versa are called encryption algorithms. To use cryptographic algorithms, both the sender and receiver have to have a value known as a key. If a file is encrypted using the rule that each letter will be replaced by the letter that follows it in the alphabet, with “z” being replaced with “a”, that system provides for a certain level of security, but it can be easily broken. This algorithm is called single substitution (in which each letter is always substituted for another letter) and the key is to use the following letter in the alphabet.

Until the 1970s, cryptographic algorithms existed in hundreds of variations, but all shared one characteristic: The key used to encrypt a file had to be used to decrypt it. This is called symmetric key cryptography. In the 1970s, two groups of mathematicians devised a completely new form of cryptography called asymmetric key cryptography, or public key cryptography. These systems are based on generating keys as pairs of numbers (each of which can be hundreds or thousands of characters in length) with a unique relationship. The paired keys are called the public key and the secret key. If a message is encrypted using the public key, it can only be decrypted by the secret key; if the message is encrypted with the secret key, only the public key can decrypt it. The public key can be freely distributed and can even be put into a directory accessible to the world. If User A wants to send User B a message, User A encrypts it using User B’s public key. User A knows that

only User B can read it because that requires the secret key, which only User B has. Of course, User B has no assurance that the message actually came from User A, but if User A were to encrypt the message twice, once with User B's public key and once with User A's secret key, the situation would change. Because User B needs to use his secret key, he knows the message was destined for him. Because User B also needs to use User A's public key to decrypt it, he has assurance that it came from User A.

In forensics, investigators encounter encrypted files. Some encryption systems can be defeated either through reverse engineering of the password by using commercially available software or through brute-force methods such as trying every combination until you hit the right one. For shorter keys, brute-force methods can be very effective, given the speed of modern computers. For long keys, the decryption process can be effectively impossible. Although there are sometimes ways to get the password, the general rule is that not all encrypted files can be read. Sometimes a plain text file can be recovered even after encryption because the cryptographic system did not do a thorough job of deleting it.

Browser History and Cache Files

A page viewed on the Internet using a browser program such as Internet Explorer, Netscape, or Opera is the result of processing information sent across the Internet. Generally, pages are defined using languages such as HTML (HyperText Markup Language) or XML (Extensible Markup Language). They can be made up of dozens of independent elements. Every picture, graphic line and other element is actually a separate file that could have been gathered from servers around the world through a process invisible to the user. Two areas on a hard drive store information about the identity and content of Web pages visited by the user. The history file contains a list of Web sites visited over weeks of browsing, but it can be erased or overwritten. The cache file stores the various files downloaded to create the pages seen in the browser. By storing (or caching) them on the local drive, it becomes possible to review pages and recreate them quickly. These files are very important in forensic investigations involving Internet browsing habits and can provide very useful information about what was accessed and when.

Cookie Files

No discussion of Internet browsers is complete without considering the potential value of the cookie file. In Internet terminology, a cookie is a small file that is written to the hard drive by the Web sites you visit. Cookies can be read by the Web site that issues them. For example, registered users of Amazon.com may have wondered how Amazon recognizes them when they return to the site. The answer is that when registered users go to Amazon's Web site, Amazon's site reads the cookie and uses the data stored in it to establish the computer's identity. Some cookies are issued by companies that provide tracking services across many Web sites. For example, companies offering pornography on the Web can subscribe to cookie services such as Sexhound or Sextracker to discover which of their other serviced Web sites have been visited by the user. Cookies can have great forensic value in determining those sites visited by a user. Cookie files are generally invisible to the user but, through the menus of the browser, cookie files can be erased.

Embedded Information (Metadata)

Information stored by a program can contain more data than meets the eye. Consider, for example, a typical word processing system like Microsoft Word. Obviously, Word stores

the text of your file, but it also stores far more. Basic information is stored in the “Properties” fields, which contain such potentially useful data as:

- The date and time the file was created, last updated, last accessed, and last printed
- Who was logged into the computer when the document was last saved
- How many times the document has been edited, and the total time it has been open for editing
- Who was logged in when the document was created

Clearly, this information can be of great value to the fraud investigator. If a person said that he or she wrote the document but never changed it, or claimed that it was printed long after the actual print date, such testimony can be impeached by metadata (data about data). Many application programs save metadata. It is vital that the fraud investigator understand this to avoid overlooking potentially valuable information.

Application Data Not Visible to the User

Aside from the metadata, the file can also contain changes made to the document using the “Track Changes” in the “Tools” menu. Word can also store multiple versions of a document within one file, with only the latest visible to the casual user. Knowing that this data may be present is again important to the fraud investigator, as it can have a significant impact on a case.

Slack Space

Storage space on a computer hard drive is divided into allocation units, usually called clusters. The cluster is the smallest amount of data that can be associated with a file. If a file needs more data than can be stored in a cluster, the operating system assigns it more space in one-cluster units, which are not necessarily contiguous. Thus, the operating system associates every file with one or more clusters, but never fractions of clusters. Files are of different lengths and are not necessarily the size of a cluster or an exact multiple. If a file takes up more than one cluster, every cluster but the last one will be filled (if the last cluster were filled, the computer would have to assign another one). The last cluster of the file stores whatever amount is needed to finish the job. At that point, a special character (end of file character, or EOF) is written. Anything that exists between the EOF character and the end of the cluster is called slack space.

Slack space can be very important in a forensic examination. Assume File XYZ—an important file in your case—was erased, leaving the clusters assigned to the file available for reuse. One of the clusters was reused, but only the first 10 percent of the cluster was overwritten with new data, which was followed by an EOF character. Whatever was there before the overwrite (in this case a part of the XYZ file) is still there, invisible to the operating system because the operating system is programmed to stop reading a cluster when it hits an EOF character. The system assumes that the file is complete, and ignores the rest of the cluster. With forensic tools, the slack space can be searched and read, and that can provide access to what might otherwise be unavailable data.

Hidden Files

Every file on a system has characteristics. One of these is called hidden. Hidden files are actually there and are no different from any other file except they do not appear on

directory listings. Forensic specialists can find these files. Sometimes, when they have been deliberately hidden, they can contain information of great value to the investigator.

Taking a broader view, data does not necessarily have to be physically stored on a PC. Here are some options to consider:

- File server disk drives
- Removable storage devices
- Disks that are part of network attached storage (NAS) systems or storage area networks (SANs)
- Backup data storage, including tapes and optical disks
- Onsite storage away from the computers
- Offsite storage, formal or informal
- Vendors

8.8.3 Computer Forensics Versus Data Recovery

The science of extracting information from computers in connection with various forms of investigation is called computer forensics (CF) and has become an important tool for investigators working in both the public and private sectors. This section looks at how CF works and provides some guidelines for fraud investigators to enable them to make the most efficient and effective use of CF in their work.

CF must be performed in a lawful way. Various jurisdictions have laws covering ownership of computers and computer data and the circumstances under which they may be examined. Fraud examiners should review such matters with counsel. For the purposes of this section, it is assumed that the examiner has determined that there is no legal impediment to a CF examination.

It is important at the outset to differentiate between CF and a technology previously discussed, data recovery. Data recovery is used where there is hardware or software damage to a storage device. The objective of data recovery is simply to recover the data; it is not necessarily associated with a CF investigation. Of course, since any CF investigation must begin with a fully operational disk or tape, data recovery techniques are an important tool and must be used if the device is damaged.

8.8.4 What Is Computer Forensics?

CF is the science of analyzing digital systems and data for information relevant to an investigation that may end up in the civil or criminal courts. Like all other forms of forensics, it has both capabilities and limitations. It is not infallible. It cannot guarantee that information being sought will be found. CF professionals must carry out their examinations objectively and report them accurately, whether or not their findings support their clients' position. The value of forensic science itself depends on this level of independence and intellectual honesty.

CF can be divided into four areas for discussion:

- Data acquisition
- Data analysis

- Reporting of results
- Qualification of CF experts

Data Acquisition

Before any analysis can occur, the CF engineer or analyst must have files or drives to analyze and an indication of what is to be examined.

Acquisition of material on files or drives must be carried out with methodologies that meet a recognized standard of completeness and accuracy. For example, any methodology must be able to capture not only the visible files but also the various forms of data not normally available to the user. For this reason, CF engineers use only a limited number of techniques for capturing data from computers. The objective of their data capture methodologies is to ensure that nothing was added or subtracted during the data capture process. The investigator can use software packages specifically designed for computer forensics that are known through careful testing and court experience to be forensically accurate. In addition, the investigator can use hardware that can be connected directly to either a computer or a hard drive to make a perfect copy of every byte of data on the drive, including those that do not have any informational content. For example, if a 120 gigabyte hard drive contains only 2 gigabytes of user data, a forensic copy would still be 120 gigabytes long. Backup tapes and files can also be used for forensic examination, but they carry only visible records. Also remember that the image file may prove useful to the forensic accountant as a source of files for examination.

All data, once retrieved, must be safeguarded. Where appropriate, standard chain-of-custody documentation and materials (for example, seals and bags) should be used so the investigator can show that no modification of the retrieved data could have occurred. Where it is unclear whether chain-of-custody control is needed, fraud examiners should err on the side of caution. Until the results of the CF examination are complete, it is impossible to say with certainty what is going to be found or its importance to the case, so it is better to institute chain-of-custody procedures on a routine basis and discontinue them only when a decision has been made not to use the data as evidence in the case. Even if chain-of-custody turns out not to be needed for the CF examination, it may be important to show the authenticity and reliability of the files used for forensic accounting processes.

The other form of data required before an examination can begin is that needed to guide the examiner in conducting the work. For example, there may be a relevant period of time to be reviewed, or a list of names, companies, accounts, or other ways to differentiate relevant from irrelevant material. Experienced CF examiners will work closely with their clients to help them create the most useful key word lists and other catalogues of relevant material.

Acquisition of data may seem impossible, for example, when a machine has an inoperative hard drive. Drives may be physically damaged or the software impaired either accidentally or deliberately to prevent analysis. Data recovery, as discussed earlier, can restore data from damaged hardware or software into a form useful to CF analysis.

Data Analysis

Forensic analysis uses a variety of specialized software packages to examine the collected data. Some of these tools are designed to extract information from backup tapes. For

example, techniques exist to extract e-mail accurately from e-mail server backup files without having to completely rebuild the server. As discussed in Section 8.8.2, "The Complexities of Data Storage: Looking Under the Hood," forensic tools are used to search a number of areas not generally visible to users, including:

- *Erased files.* CF tools can recognize the entries for erased files in file allocation tables and determine whether the space has been reused. In many cases, it is possible to restore either an entire file or at least parts of the file.
- *Slack space.* Files that have been erased and have had their storage clusters assigned to another file may still be retrievable in part by an examination of slack space. Specialized CF tools can read beyond the first EOF mark in a cluster and can search slack space very efficiently.
- *Swap/page files.* While parts of the swap file will undoubtedly be machine-language computer programs, there are also likely to be fragments of text, spreadsheets, and databases that may prove useful in a CF examination. This area may also include data from e-mail messages or instant messaging sessions.
- *Temporary files.* Like any other erased program, temporary files are capable of being accessed by CF tools until they are overwritten.
- *Print buffer files.* CF professionals can often find these files and examine their contents.
- *Compressed files.* The CF organization should either have one of the software programs available to search these files in their compressed form or be able to decompress them.
- *Password protected files.* Systems users have various techniques to protect their files from casual observers. Programs such as Microsoft Word, WordPerfect, Excel, and others provide the capability to encrypt a document and password protect it. Such capabilities are also now being built into some e-mail and instant messaging programs. Other programs are available that perform this encryption as their basic function. A well-known and popular program of this kind is PGP (Pretty Good Privacy.) The reality is that software exists that can crack the encryption on many common packages, but it may require anything from minutes to days of work on a complex of decryption machines. For others, the encryption is so strong (cryptographers use the term *cryptographic robustness*) that without access to the password or pass phrase used, decryption may be impossible in any practical sense.
- *Browser history and cache files.* These files can be examined during a CF analysis to determine browsing activity. Although these files can be erased, as with any other file, the data that is not overwritten is still subject to search and may be retrievable.
- *Cookie files.* Normally, cookies are invisible to the user (although it is not hard for a browser user to find the files) and for this reason are often forgotten. Cookies can be of great interest in a CF investigation to enable the investigator to see where the browser was pointed, and when various cookies were written to the hard drive.
- *Metadata.* Metadata is really data about how the user has manipulated the operating system and application programs. E-mail files also typically contain significant fields of metadata. CF analysis of metadata can be of great importance in a case.

Some organizations performing CF analysis may use commercial CF tools exclusively. Other organizations may have internal research and development groups that provide them with proprietary capabilities that may exceed those of standard commercial products.

However, in this case, the fraud examiner should inquire into the forensic adequacy of such tools.

Reporting of Results

Fraud examiners should carefully and critically review every CF report provided to them. Information in a CF report must be defensible and forensically accurate. Here are some points to question:

- “We conducted an examination of Jane Roberts’s computer.” The examiner should be precise about what was examined, and should be careful to not draw conclusions. It is probably more accurate to say, “We conducted an examination of a Dell Model XXXX computer, Serial Number XXXXXXX, bearing a Doe and Company Property Tag numbered XXXXX. We were informed by Joe Smith, General Counsel of Doe and Company, that this computer was routinely used by Jane Roberts. When imaging the computer, we noted that the room in which it was located (7-234) had Jane Roberts’s name on the door, and that there were several diplomas and awards on the walls, all of which had Ms. Roberts’s name on them.”
- “This file was entered into the machine by Jane Roberts.” What evidence can the CF examiners show to prove who was sitting at the keyboard at the time the file was entered? They may be able to show that her account was logged in or produce other evidence, such as a phone log record stating her office phone was in use at the time the file was entered. But without such direct or corroborative evidence, it is better to simply stick to what was found on the machine without drawing conclusions that may not be objectively supportable.

Of course, this is no different from the test to which any expert’s report would be subjected. All CF reports must be reviewed to be sure that no conclusions are reached without a documented basis. Even though a CF examination may seem and even be highly technical, the conclusions must still be supportable and completely understood by the fraud examiner.

Qualifications of CF Experts

Like any other experts, CF witnesses must qualify to be accepted by the courts. You need to be confident both that their training, experience, education, and reputation will make them acceptable and that they have the ability to carry out the kinds of examination that you will require. You must also feel confident that, if they appear in court, they will be able to withstand a sharp cross-examination.

Sometimes a brilliant technician is a terrible witness.

8.8.5 Making the Best Use of Computer Forensics in Fraud Investigations

CF can be complex, time-consuming, and expensive. There are ways to balance costs and expected outcomes, although, as in any other forensic science, there can be no guarantee of success.

- Time may be your enemy. Consider separating the process of data capture from data analysis in your planning. Computer data can be easily lost, either when the storage media is destroyed or the data is removed by software so thoroughly as to eliminate any

chance of recovery. For this reason, any information possibly necessary for an investigation could be made available by having it copied in a forensically sound manner. Once the copy is made and sealed under chain-of-custody control, it should be safe and available for analysis when and if needed. If the data is not captured quickly, it may be subject to deliberate or inadvertent alteration or destruction.

- There may be processes in place that will automatically destroy data on a regular basis. E-mail systems, for example, may be programmed to retain data only for a limited period. Once erased, this data may be difficult to reconstruct. Archival tapes may be recycled and reused at fixed intervals, and their content may be overwritten. At the very least, consider having counsel issue a document preservation letter or obtain a court order to stop data destruction. This letter or order should specifically address automated time-based destruction processes. While the content of the letter or order must be customized by counsel to the particular situation, the following example may be of interest:

Please be advised that [*Plaintiffs/Defendants/Third Party*] believe electronically stored information to be an important and irreplaceable source of discovery and/or evidence in the above referenced matter.

The discovery requests served in this matter seek information from [*Plaintiff's/Defendant's*] computer systems, removable electronic media and other locations. This includes, but is not limited to, e-mail and other electronic communications, word processing documents, spreadsheets, databases, calendars, telephone logs, contact manager information, Internet usage files, and network access information.

The laws and rules prohibiting destruction of evidence apply to electronically stored information in the same manner that they apply to other evidence. Due to its format, electronic information is easily deleted, modified, or corrupted. Accordingly, [*Plaintiffs/Defendants/Third Party*] must take every reasonable step to preserve this information until the final resolution of this matter. This includes, but is not limited to, an obligation to discontinue all data destruction and backup tape recycling policies.

If this correspondence is in any respect unclear, please do not hesitate to call me.

Obviously, in drafting this letter, the more intelligence you have about the party on whom it is being served, the better. This is an area in which your CF resources may be of assistance to counsel in customizing the details to provide the best coverage.

- Plan the examination carefully. You should, in discussions with your CF provider, agree on what kinds of tests and reviews are to be conducted, on which machines or archives the tests will be run, the search terms to be used for each part of the project, and the time and resources that will be involved. Also determine how you will receive your results (for example, printed form, CDs, or DVDs). Determine whether you will need specialized software to review material provided to you in machine-readable form, particularly if you do not have the specific software that was used to create the files. There are commercial packages that can provide you with the ability to access such files without having the original software. Some CF providers supply proprietary software

with their reports to assist you in both being able to read their results and conducting additional searches for new key words or other terms on your own.

8.9 SELECTED COMPUTER CRIMES

8.9.1 Brief Case Synopses

It is useful to look at actual cases of computer crime to see the challenges businesses face if targeted by an offender. In each of these brief case studies, consider how your organization's existing security system would have fared, how your own organization would have reacted, and how likely it is that your current system of internal controls would have identified the problem and traced it back to the guilty parties.

ER Fraud Case Study

A computer operator at a hospital was charged with embezzling \$40,000 by submitting false invoices that were processed through the hospital's computer system. At the same time, the hospital's assistant data processing manager accepted a \$41,000 bribe from a consultant who stole an additional \$150,000 by submitting false invoices for computer services. Both the operator and the assistant manager had prior convictions for computer-related crimes. Because computer personnel were not directly involved in patient care, hospital policy did not require a background check. An inexpensive reference check with previous employers could have possibly prevented the crime because the offenders would probably not have been hired when it was revealed that they had falsified their employment applications.

Even Experts Have Bad Days Case Study

A partner at a major international consulting firm received an anonymous call suggesting that one of the firm's senior information systems managers was defrauding the firm through a scheme involving false invoicing for supplies such as laser toner cartridges and backup tape cartridges. A confidential internal investigation was carried out and no problems were revealed. Every invoice could be shown to tie directly to the actual material that had been delivered. The report seemed to be false but a member of the firm's management committee decided that someone independent of the company should take a second look. Investigators were hired and they discovered that the material had been delivered, but they could find no record of the firm that supplied the materials. A simple background check on the vendor showed that it was just a shell formed by the senior information systems manager. He had developed a scheme in which he would place orders with the shell company (actually, with himself) and then order the same material from a reputable supplier who sent it to his home overnight. He would open the boxes, remove the original vendor's invoices, insert his own invoices (which were exactly

15 percent higher than what he had paid) and then reship them. This simple scam resulted in a loss to the company of more than \$300,000.

As shown in this case, vendor fraud can occur even in situations where all the materials are actually received. No employees had questioned why so many orders were being placed with a company no one had ever heard of when major vendors could provide the same material in less time and at a lower cost.

The Invoice Looked Good Case Study

The scam was brilliant. The accounting manager had found a way to get his employing company to pay for his gambling losses in Las Vegas. Every time he needed to send a payment, he simply created an invoice for services at some distant office. The invoices were always from different companies but on all of them he put a stamp on which he wrote their vendor number in the company's system. Of course, the vendor number was one the accounting manager had assigned to the holding company that owned the casino. Of course, the casino was always glad to see him on his quarterly visits: It didn't care whether the check was made out to it or to its parent company. Because the computer system would not reject the invoice as long as the vendor number was valid, the computer generated the check in the weekly check run; it was signed by another machine and mailed out with thousands of other checks.

The scheme worked for years, until the outside auditors decided to conduct an internal control review. They discovered there was no match between vendor names on invoices and vendor numbers. In checking a vendor list, one of the auditors recognized the name of the casino's parent company and wondered why this unlikely organization would be a vendor. The manager told the auditor that the company held meetings at the casinos owned by the company. Unfortunately for the manager, the auditors checked his story, and the scheme was revealed.

Breaking the Bank Case Study

A European bank sustained losses estimated at \$65 million over a two-year period when the head of the foreign currency transfer department and her assistant, who had broken the bank's computer transfer codes, were able to move money into outside accounts. The fraud was discovered through an audit and the two perpetrators were arrested. Afterwards, everyone asked how it was possible for such a large amount of money to be stolen with no one noticing and raising the alarm. Further investigation showed that the bank was involved in complex money laundering and tax evasion activities. Apparently, the two managers believed that with all the manipulation going on no one would notice their independent scheme. They were almost right.

A New Form of Fraud Case Study

An employee of an insurance company in Florida had the dubious honor of being one of the first people convicted under that state's computer crime law. The employee was a benefits clerk with the company and used her expertise in the company's systems and procedures to steal more than \$200,000 in two years. She filled in the forms that benefits examiners used to approve claims and entered them into her computer terminal. She used a variety of names and policy numbers—all real—and created the paperwork to back up the claims. Her mistake was always using only three mailing addresses for the checks: her own, her father's, or her boyfriend's. The security department of the company discovered the fraud by looking for unusual patterns of payment addresses.

Welfare? Yes, We're Faring Very Well, Thank You! Case Study

It may be impossible to discover exactly how much they stole but a state Department of Social Services learned that one of its supervisors worked in collusion with a clerk to steal \$300,000. This was a simple matter of input falsification. The clerk and supervisor submitted dozens of false claims for benefits and collected the payments. The fraud was discovered when a data input clerk noticed that the authorization data on one of the forms she was entering was incomplete. She called the eligibility worker whose signature had been forged by the supervisor to check on the incomplete form. When that person denied authorizing the claim or signing the form, an investigation was performed and the fraud was discovered.

When Time Stood Still Case Study

Wouldn't it be great to get the results of horse races before they ran? Imagine always betting on long shots when you know the winner. Just a dream? Not for the computer operator at a government-run betting agency in Australia. He figured a way to reverse time. Just before certain races, he reset the system clock to read three minutes earlier than it actually was. As soon as the race was run, he called his girlfriend, who was an off-track telephone-betting clerk. She immediately entered bets on the winner. Because the computer believed that the race had not yet started, the bets were accepted. Then, the operator would reset the clock. Unfortunately, we cannot report that the scheme was uncovered by brilliant work by internal auditors, external auditors, corporate security personnel or even outstanding police work. The operator's girlfriend turned him in when she discovered he was seeing another woman.

Livent: Computer Programs Written to Conceal Management Fraud

Livent was a Canadian based producer of live theatre. They also were listed on NASDAQ. Between 1990 and 1998 senior management engaged in numerous frauds to misappropriate funds and report inflated earnings. The chief financial officer was the recent former audit partner in charge of the engagement, and participated in the fraud. Kickbacks were directed to senior management who authorized excessive charges for and manipulated descriptions of services. Those costs were improperly carried to long-term fixed assets. In addition, excess costs on losing shows were improperly charged or transferred to shows that were still in development or had a longer period for amortizing costs, hiding the overall losses. Each quarter the company removed expenses and liabilities from the books, only to reinstate them after the quarter. The execution of the changes on a batch basis via a specially written computer program was designed to hide the nature of the activity from auditor scrutiny by making the adjustments look like original transactions. The SEC Administrative Proceeding states:

“Because of the sheer magnitude and dollar amount of the manipulations, it became necessary for senior management to be able to track both the real and the phony numbers. At Eckstein’s direction, Malcolm maintained computer files of the manipulations that tracked the details of expense capitalizations, expense rolls and show-to-show cost transfers from 1995 through the first quarter of 1998.”⁹

8.9.2 Case Study: A Closer Look

There are thousands of cases of serious computer crimes on the books. Some were presented in the previous section. To provide a closer look at the way these cases are investigated, one full-length case study is included. This case involves deliberate actions by an insider who disrupted the e-mail capabilities of an organization.

The Case of the Suicidal Computers Case Study

It happened, as do so many unpleasant things, in the dark of night. A dozen computers—each dedicated as an e-mail router for a major financial services firm—apparently made a mutual decision, precisely at 5:00 A.M. one morning, to commit suicide. At that time, each of the computers, suddenly and without warning, proceeded to completely reformat each of their hard disk drives. From that moment on, e-mail within the huge global organization stopped. Any message that was sent outside of the local office was not going to be delivered.

⁹ United States before the SEC, previously cited.

Within an hour, the problem was noticed. Within two, it was apparent that the problem was not small and was not going to be easy to fix. Because many of the important daily operating communications of the company went through e-mail, it was clear that a back-up plan would be needed to replace the damaged communications links. While one group of managers developed a plan to keep the organization functioning, the chief information officer passed the word to the company's communications manager to fix the problem. The data communications manager immediately contacted the manufacturer. Because the organization was a large and valued customer, the manufacturer put two systems engineers on the next available flight.

At the same time, the director of corporate security recognized that, while it was possibly an accident—perhaps a programming bug—that caused this crisis, it was probably a deliberate act of sabotage. If it were, he knew he would need proof to determine who had caused it. The director of corporate security also understood that proof requires evidence that could be admitted in a court of law. Fortunately, the director had previous experience in computer fraud cases in which evidence that might have existed was destroyed in the attempt to fix software problems. Therefore, two calls were made: The first was to the chief executive officer of the company, who gave him authority to investigate the incident and, if it were shown to be deliberate, to identify and punish the perpetrator. The second call was to a private investigations firm that specialized in high-technology incidents.

The investigators understood that they could not interfere with the repair efforts; nevertheless, they immediately went to the data center. They briefed the repair team, and made a simple request: Please, do not destroy or change anything that might be the cause of the incident without checking with us first; and keep detailed notes of your findings.

Over the two days it took to identify the problem and complete repairs, the investigators collected evidence, both in the form of software and in written statements from the software engineers.

During the investigation, it was discovered that one e-mail server had not reformatted itself. Because of a hardware problem, it had been shut down when the incident occurred. When the engineers discovered this, they examined the unit. One of the company's technicians noticed that the program that controls the processing of daily backups indicated it had been modified a few weeks earlier.

The technician who was responsible for backup knew that she had not changed the program in months. Nevertheless, the program had been changed. It still performed its normal backup but there was a new routine that checked the date every time the program ran. On a specific date, the program had just two lines of code to be executed and those two lines instructed the computer to reformat its hard drives immediately without warning and without any report being generated. The investigators took possession of the server since it was now apparent that the act was deliberate.

Over a 48-hour period, the problem was solved and all systems were checked for the existence of the deadly software. Before the engineers from the computer manufacturer left, the investigators assigned them one additional task. Using the

notes they made during the previous 48 hours, each of the engineers wrote a memo documenting his or her findings in the context of what was now a potential criminal investigation. These statements were quickly reviewed and then signed and sworn to before a notary. This action converted a memo into a sworn affidavit, which could have great value in any future court action.

With the e-mail system back in operation, the data center management worked with the investigative team to determine who could have inserted the killer code into the dozen servers. Because of security measures built into the system, very few people had the authority to make those changes. In fact, the investigators were told, only four employees had that authority and all were exemplary employees, so far beyond suspicion that no one could conceive of any of them having done this. Yet it had to be one of them. Who else could it be?

That was the question put to the head of the e-mail management group, where the four suspects worked. She was convinced that none of the four employees was responsible; however, she had another candidate under consideration. He had resigned some weeks earlier, but, as a member of the group, he would have had the authority. Why had he left? Because he felt that he was misunderstood and insufficiently appreciated. He believed he knew far more than the others in the group, including the group head, about e-mail technology. He had publicly gone to senior data center management to request a promotion to group head. When his managers decided that they would keep the present manager, this disgruntled employee had given notice and told others that the company did not deserve him.

An examination of the former employee's computer revealed evidence of the destructive code that had caused the shutdown. Several versions of the code were found, including the key line that delayed the destruction until several weeks after he left the company. On the evidence presented by the investigators, the case was referred to law enforcement. The police accepted the case and reviewed the evidence. The case was brought to the county prosecutor, who determined the actions to modify the computer's program were a violation of the state's computer crime laws and that he would prosecute.

8.10 CONCLUSION

One of the peculiar things about the field of computer crime is that one can say almost anything and go unchallenged. The only thing people seem to agree on is that most computer crime is probably never reported either because it is never discovered or because the company is embarrassed and chooses to handle it administratively. Often the company will forego prosecution if the offender resigns and agrees never to discuss the incident. This is why people who commit computer crimes can, in effect, get away with it and go on to another company with their reputations apparently intact.

This chapter has tried to show that it's a myth that only those with tremendous computer skills can commit a computer crime. Any employee, temporary worker, or independent contractor with authorized access, as well as anyone with unauthorized access can do it. Since most computer crimes involve input or output manipulations, the individuals most

able to commit these crimes are not developers but employees in departments that use the systems. This is not to say that systems people do not commit computer crimes; they do, but they are not typically likely to do so.

Further, the commonly held belief that most computer crime is committed by outside hackers who gain access to systems through almost mystical abilities is also a myth. Most of the incidents involve actions by insiders. Again, enough occurrences do involve those outside the organization to make defensive systems such as firewalls absolutely necessary.

A third myth is that computer-related thefts including fraud and embezzlement are not detected by audit but by accident. If that were true, and it is not, it would imply that the criminals are somehow more intelligent or more skillful or perhaps more cunning than the noncriminals. This is also not the case. Sound internal security, accounting, and audit systems are very effective and do catch the bad guys. It is when these controls are not in place or when they are implemented with insufficient resources that the criminals get the upper hand.

As computer security becomes an increasingly important aspect of technology, it is likely that better mechanisms to prevent and detect computer crimes will evolve. But to gain the needed protection, it will be necessary for companies to adopt the technology and to implement it properly. Again, those who fail to assign sufficient resources to prevent problems are doomed to have such troubles.

Finally, once a security weakness is identified in a system, whether by hackers or security experts, and the knowledge of the hole becomes public, it is important that it be closed quickly. There is nothing more discouraging than having to tell a victim company that it was hit by a perpetrator who used a well-known hole to enter its system and that all along there had been an easy-to-install, free patch out there but that it was never installed.

8.11 COMPUTER CRIME CHECKLISTS

Internal and external auditors and IT department management can use the following checklists “Evaluating a Company’s Electronic Data Management Policies,” “Evaluating the Corporate Environment for Computer-Crime-Friendly Characteristics,” and “The State of Authentication,” to help them understand and recognize the red flags that may indicate the presence of fraud in their organizations and those of their clients. Generally, all *No* answers require investigation and follow-up to determine whether remedial action is needed. The results should be documented. Use the “Ref” column to cross-reference the checklist to any additional working papers.

These checklists are intended for general guidance and information only. Use of these checklists does not guarantee the prevention or detection of fraud and it is not intended as a substitute for audits or similar procedures. If computer crime is suspected, seek the advice of a knowledgeable computer-forensics professional.

TABLE 8.1 EVALUATING A COMPANY'S ELECTRONIC DATA MANAGEMENT POLICIES

| Evaluating a Company's Electronic Data Management Policies Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| <p>Note: This table is adapted from the publication "Top Ten Tips for Effective Electronic Data Management," previously provided on the Kroll Ontrack website as part of the Legal Tools section of the site. (www.krollontrack.com)</p> | | | | |
| <p>1. Has the company put in place the policies and procedures needed to actively manage electronic data storage systems?</p> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <p>2. Does the company maintain current records of the types of hardware and software in use, and the onsite and offsite locations of all electronic documents?</p> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <p>3. Does the company have a written records management policy for both paper and electronic documents that schedules on and offsite retention periods as well as destruction?</p> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <p>4. Does the company train everyone to carry out their responsibilities under the data retention and destruction policies?</p> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <p>5. Does the company have a written policy covering:</p> <p>a. Employee use of hardware and software?</p> <p>b. Employee use of unauthorized software?</p> <p>c. Responsibility for data security?</p> <p>d. Company rights of surveillance?</p> <p>e. The change of passwords at specific time intervals?</p> <p>f. The de-activation of passwords when an employee is transferred or terminated?</p> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <p>f. The de-activation of passwords when an employee is transferred or terminated?</p> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <p>6. Are there adequate security measures covering the transmission of data into and out of the company? Has any data of high sensitivity been designed to be encrypted in transmission?</p> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <p>7. Is there a litigation response team in place that can respond to data preservation requests and discovery orders to ensure compliance? The team should be comprised of outside and in-house legal counsel, representatives from human resources, business-line management, and IT.</p> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| <p>8. Does the technology used to destroy electronic documents produce a record certifying complete destruction? Have "standards" for data writing over files been referenced and adhered to in the data erasure process?</p> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

TABLE 8.1 (continued)

| Evaluating a Company's Electronic Data Management Policies Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| 9. Do policies enumerate the data retention requirement of regulatory agencies (e.g., SEC) or jurisdictions (e.g., States) or laws (Sarbanes-Oxley Act of 2002) to ensure that electronic documents are retained in accordance with requirements? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 10. Does the company have a procedure to halt automatic destruction of e-mails and other data that might be required to be retained? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

TABLE 8.2 EVALUATING THE CORPORATE ENVIRONMENT FOR COMPUTER-CRIME-FRIENDLY CHARACTERISTICS

| Evaluating the Corporate Environment for Computer-Crime-Friendly Characteristics | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| 1. Do pay rates and employee benefit programs compare favorably with the industry and area where the company is located? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 2. Are there grounds for actual or possible employee discontent? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 3. Does management define and communicate clearly to employees the expected standards of work performance and on-the-job behavior? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 4. Does the company have effective and consistent programs in place to recognize and reward good work and to provide feedback for inadequate or unacceptable performance or workplace behavior? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 5. Does the company provide counseling when work or behavior is substandard? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 6. Are the performance and behavioral standards reasonable and achievable? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 7. Does the company provide the resources and support necessary to meet or exceed standards? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 8. Are there reasonable and adequate internal controls, reviews, audits, inspections and reporting mechanisms to assure that company policies, procedures and rules are being followed? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 9. Does the company demonstrate through policy and practice that it will not condone violation of ethical norms or inappropriate behavior? Does the top management demonstrate the proper "tone at the top" in its practices and actions? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 10. Does the company recognize destructive competitiveness between employees and managers and intervene to stop it? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 11. Does the company have objective standards that avoid bias or material unfairness in hiring, promotion, pay, appraisals, assignments, overtime, etc., and does it have a mechanism in place to appropriately investigate and handle complaints in these areas? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 12. Is the company facing a merger, acquisition or business failure that may give employees an increased desire to "watch out for themselves"? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

TABLE 8.2 (continued)

| Evaluating the Corporate Environment for Computer-Crime-Friendly Characteristics | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| 13. Does the company have an anti-fraud program with an anonymous tip fraud “hot-line” number that is known to employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 14. Does the company communicate the protections afforded by Whistleblower and other laws and regulations to its employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

TABLE 8.3 THE STATE OF AUTHENTICATION

| The State of Authentication Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| 1. Are all system users required to log on using a User ID and a password? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 2. Are there written and enforced policies requiring users to safeguard their password and not to share it with others? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 3. Does more than one person use the same user account? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 4. Are there written and enforced policies for password construction? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 5. Are there written and enforced policies requiring regular password changes and prohibiting re-use of old passwords? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 6. Is there a mechanism by which an employee can report the possible compromise of a password and change it? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 7. Is there a mechanism to recover lost passwords that prevents anyone other than the responsible employee from re-using it to access an account? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 8. Is there a policy regarding termination of system access when an employee leaves the company? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 9. Are non-employees such as consultants and temps required to sign a confidentiality and computer-use agreement before being assigned a password? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 10. Do passwords limit employee access to authorized applications only? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 11. Do supervisors or "super users" have access to the system only through personally identifiable accounts? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 12. Are accounts reviewed regularly to assure that each represents an actual employee or authorized non-employee, and that there are no accounts unaccounted for? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

TABLE 8.4 SARBANES-OXLEY AND INTERNAL CONTROL OVER IT

| Internal Control Over IT Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| 1. Has management received and read <i>COBIT from ISACA or the IT Control Objectives for Sarbanes-Oxley</i> from the IT Governance Institute? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 2. Are the CEO, CFO and CIO familiar with the COSO and COBIT frameworks? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 3. Have the IT systems and subsystems controlling financial reporting been identified? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 4. Is the IT system designed to prevent the creation of deficiencies, significant deficiencies or material weaknesses through the application software? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 5. Can the IT system provide the integrity of information, availability and compliance required by the SEC final rules? Note: This consideration is linked to the information and communication component in COSO. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 6. Can the IT system provide the security from unauthorized access or disclosure required to ensure the integrity of the financial reporting process? Unauthorized access can be prevented at the application software level or at the network level, depending on the security software design employed. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 7. Is the process of program development secure against tampering? Are programs tested against the specifications and user needs before they are brought on-line? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 8. Is there a strategic plan for the IT system? Are upgrade assessments scheduled to ensure that systems are “current” but not disrupted by minor changes and unimportant updates? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 9. Is someone responsible for the management of third-party services? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 10. Are all overseas service providers monitored closely for their effect on the financial reporting process and compliance with Sarbanes-Oxley? Are direct tests or a Type 2 “SAS 70” report available on outsourced processes? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 11. Is a quality assurance methodology in place for the introduction of new applications? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 12. Are all aspects of the IT system well documented? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 13. Is the system tested regularly and all deficiencies and changes documented? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

(continued)

TABLE 8.4 (continued)

| Internal Control Over IT Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| 14. Is there a well-documented approval process in place for all changes to hardware or software? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 15. Are the effects of all changes on other parts of the system investigated and well documented? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 16. Has a risk assessment determined the likelihood and consequences of a failure anywhere in the system? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 17. Is there a monitoring process in place covering all relevant IT general controls components—access and security, new program development, program changes and operations? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 18. Is the “tone at the top” of the IT function assessed and evidenced? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 19. Is there a mechanism or process for determining when and who to call when specialists and consultants are needed for various IT related special tasks? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 20. Are test results for the IT controls over the financial reporting process compiled in a report for review by management? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

CHAPTER 9:

Dealing With a Known or Suspected Fraud

| | | |
|-------|--|----|
| 9.1 | Overview..... | 3 |
| 9.1.1 | Purpose and Scope..... | 3 |
| 9.1.2 | Forensics and Forensic Accounting..... | 4 |
| 9.2 | The Five-Step Investigative Approach..... | 4 |
| 9.2.1 | Planning | 5 |
| 9.2.2 | Evidence Gathering | 7 |
| 9.2.3 | Analyzing and Testing..... | 11 |
| 9.2.4 | Reporting and Testifying..... | 11 |
| 9.2.5 | Case Resolution..... | 16 |
| 9.3 | Forensic Accountants..... | 16 |
| 9.3.1 | Professional Skills and Attributes | 17 |
| 9.3.2 | Ethics | 20 |
| 9.3.3 | Kinds of Services Offered..... | 21 |
| 9.4 | Dealing With a Known or Suspected Fraud Checklist..... | 22 |

CHAPTER 9:

Dealing With a Known or Suspected Fraud

9.1 OVERVIEW

9.1.1 Purpose and Scope

The primary focus of this Handbook is fraud prevention, not fraud investigation. Likewise, this Handbook is intended primarily for the CPA, whether in public practice or in industry, who is responsible for fraud prevention, rather than the full-time fraud investigator. However, professional fraud investigators will also find this Handbook useful in many ways, and occasionally there may be some crossover between the two functions; nevertheless, the distinction between the two is an important one. Prevention cannot come without an understanding of how fraud is perpetrated and the means by which it is concealed. To reach this understanding, it is necessary to have a firm foundation in fraud investigation techniques.

The experienced fraud investigators achieve their status through professional training and, most important, extensive experience in the investigation of fraud. It is well beyond the scope of this Handbook—indeed, it would be a virtually unachievable goal for any text—to synthesize the knowledge and expertise gained by an experienced forensic and investigative CPA over many years. There is simply no substitute for experience.

Nevertheless, virtually all CPAs should be concerned with fraud prevention, investigation and reporting, whether internally to an employing company, to a client, or to a court. Occasionally and despite the best fraud prevention efforts, a known or suspected fraud situation may surface. It is important in such circumstances that the CPA—

1. Be capable of acting competently: that is, perform the acts that should be performed and avoid or not perform those acts that should not be performed.
2. Understand the role of the forensic accountant and others who may be called in as part of the fraud investigation.

This chapter should serve to introduce the CPA to fraud investigation and reporting. It is not intended as a substitute for professional expertise in fraud investigation. Until the requisite experience is gained, in all cases involving fraud or suspected fraud, the inexperienced CPA should seek the assistance of a lawyer knowledgeable about fraud and a CPA experienced in forensic accounting.

9.1.2 Forensics and Forensic Accounting

The term *forensic* can be defined as, “belonging to, used in, or suitable to courts of law.” This term describes the standards that are applicable to the discipline in question—that is, a forensic medical examiner would conduct autopsies to a standard required for court purposes, and a forensic accountant would conduct financial analyses to a standard required for court purposes. Thus, a forensic accountant may also be involved in civil litigation cases, which do not necessarily involve fraud.

But what is that standard? Generally, the forensic standard involves considering all the relevant evidence that could affect the professional's opinion and yet withstand rigorous cross-examination from counsel who is keen to undermine or disprove the professional's opinion so that the professional can properly assist the court reach its decision. It also involves a strong understanding of the legal system.

It follows then, that *forensic accounting* is a discipline involving accounting to a standard required by the court—the criminal and civil courts, as well as arbitration, mediation, and other forms of business dispute resolution that require expert evidence to a similar standard. It involves the application of financial skills and an investigative mentality to unresolved issues, conducted within the context of the rules of evidence. As a discipline, it encompasses financial acumen and a strong knowledge and understanding of business reality and the workings of the legal system. In the context of a fraud case, extensive fraud investigation expertise is essential. Its development has been primarily achieved through on-the-job training, as well as experience with investigating officers (in fraud cases), legal counsel and in the courts.

Accounting practitioners who concentrate their professional practice on matters requiring them to testify in court as to the findings from an investigation of accounting and financial evidence are termed *forensic accountants*. The ultimate test for the forensic accountant is acceptance by the courts of law—both criminal and civil—of him or her as an expert witness providing testimony in the area of accounting and financial matters.

While the American Institute of CPAs and the state Boards of Accountancy currently do not prescribe any standard specifically related to forensic accounting, it is clear that the standards for this practice are determined in the first instance by the courts of law. At the same time, a CPA is required to meet the general standards of professional practice as stipulated by the governing State Board of Accountancy and American Institute of CPAs.

9.2 THE FIVE-STEP INVESTIGATIVE APPROACH

Typically, there are five major steps in the forensic accounting and fraud investigation process:

1. Planning.
2. Gathering evidence.
3. Analyzing and testing.
4. Reporting and testifying.
5. Case Resolution.

For a more detailed checklist, see the table at the end of this chapter.

9.2.1 Planning

As with almost all endeavors, planning is critical. A well-planned investigation maximizes the chances of success; poor planning can lead to disaster. In the early stages of a forensic accounting or investigative engagement, it's especially important to (1) establish the scenario, (2) identify areas of concern and uncertainty, and (3) define the nature and scope of the investigation.

Establishing the Scenario

The amount of information available during the earliest phase of an engagement will vary from case to case. Establishing what is known is of special importance. This is true because it has a direct impact on the nature and scope of the investigation.

A known or suspected fraud almost always comes to light through one of the following three broad scenarios:

1. *Accounting irregularities.* One of the most common irregularities is a discrepancy between the book value of an asset and its value as determined through physical counts or confirmations. For example, a physical inventory count may reveal a major shortage compared to the perpetual inventory records, or accounts receivable confirmations may reveal much lower values than the accounts receivable subledger. Other common examples include bank reconciliations that do not balance, and complaints from customers that their statements are incorrect. Any irregularity that comes to light during an internal or external examination would also fall into this category. The common theme in all of these examples is that the company's records—its information system—have raised a red flag that signals the possibility of fraud.
2. *Immediate physical evidence.* Physical evidence may be readily apparent or uncovered upon inspection. Obvious examples include the aftermath of sabotage or arson. Human or electronic surveillance techniques might also yield immediate evidence (for example, with respect to employee theft or the diversion of inventory).
3. *After-the-fact incriminating information.* Incriminating information is a grab-bag category that comes in various incarnations: outright confessions brought on by guilt, anonymous tips, memos in brown envelopes, whistle-blowing employees, irate spouses looking to get back at their fraud-perpetrating husband or wife, honest citizens just trying to do the right thing, and so on.

In any fraud investigation the first step is to establish which of these three scenarios exists, and the nature and scope of the related evidence.

Identifying Areas of Concern and Uncertainty

The next step in the planning phase is a blending of the Boy Scout motto: *be prepared* and Murphy's Law: *whatever can go wrong, will*. Immediate areas of concern depend on the scenario identified in the previous step. Dealing with sabotage requires the immediate beefing up of security at other likely targets to prevent further damage. Dealing with a specific employee who is suspected of fraud—such as an accounts receivable clerk who might be perpetrating a lapping scheme, or a shipping department employee misappropriating inventory—you would want to secure all possible evidence and remove the suspect employee from the scene. Removing the employee from the scene need not be

done in a direct, accusatory way. For example, if the fraud red flag is not common knowledge among the work force, the employee could be sent on a week's training course.

Beyond the immediate concerns of asset protection and evidence preservation, it's important, to the extent possible, to identify the uncertainties in the investigation—any pieces of the puzzle that are missing, so to speak. What are the major strengths and weaknesses of the existing evidence and supporting material? What additional evidence is likely to be available? What additional research, investigation and analysis are likely to be required to obtain any needed additional evidence and make it useful? Without at least a rough idea of where you're going, you most likely will not arrive at any valid conclusions.

Perhaps most important, you should think of any constraints, obstacles and pitfalls you are likely to encounter along the way. Obviously, forensic accountants and investigators need to be concerned about legal constraints in conducting their investigation. For example, as a general rule, only law enforcement authorities in possession of a valid search warrant can legally search a residence or a vehicle. (There are several exceptions, but for practical purposes none of them would apply to a fraud investigation.)

Less clear may be situations such as searching employee lockers. Judicial authorities have established that if employees have been put on notice all along that their lockers are subject to inspection, they probably can be searched. If this notice is lacking, legal counsel should be consulted, which should be the rule followed in all cases. Other concerns of investigators include lawsuits for false accusations or wrongful dismissal, and constraints imposed by collective bargaining agreements. The point is that a fraud investigation can be a legal minefield that must be navigated very carefully and deliberately, not haphazardly. To keep from hitting a mine, the safest course to set is early consultation with appropriate legal counsel and an experienced forensic CPA.

In addition to legal constraints, factors such as the company's reputation and relationship with its employees must be considered. For example, you would not want to alienate all your employees through hasty implementation of draconian investigative or security measures, just because of one bad apple.

Defining the Nature and Scope of the Investigation

The last step in the planning phase is to define the nature and scope of the investigation. This should be a fairly simple and straightforward process if the first two steps—establishing the scenario and identifying areas of concern and uncertainty—were properly thought out.

The nature and scope of the investigation are defined by several interrelated attributes including—

- The nature of the main objective—for example, prevention of further incidents, dismissal of the perpetrator, proving the case for criminal prosecution, establishing a loss claim, and so on—and the ranking of the objectives when there is more than one.
- If a criminal prosecution is envisaged, the point at which to involve the police.
- The level of secrecy or *cover* required in conducting the investigation.

For example, if the scenario involves an anonymous but seemingly credible tip implicating a purchasing employee in a kickback scheme, the objective may be to prove the case for criminal prosecution. The nature of the investigation will be fairly secret, because the

parties involved are unlikely to confess and you would not want to alert them to the investigation. Because kickback (that is, secret commission) cases can be difficult to establish, the scope of the investigation could become extensive, including background investigations of both the bribe giver and bribe taker, surveillance, and possibly even setting up a sting operation.

9.2.2 Evidence Gathering

Once the planning phase is complete, the general objectives of the investigation must be translated into specifics, for example, identifying the documents and other information to analyze, conducting interviews, and obtaining third-party information required for corroboration.

Throughout the process, two important questions to keep in mind are what logical alternative interpretations exist for the evidence, and what eventual use will be made of the evidence. In particular, the forensic accountant must be able to understand the difference between relevant and irrelevant information, and must be willing to apply the standards of evidence required by the court.

Information Gathering Techniques

The forensic and investigative accountant is not a police officer. He or she does not have the resources of a police officer and, even when working to assist the police, must work within his or her own expertise, and within the rules governing professional conduct. Among the most important investigative tools are those that enable the forensic accountant to gather and analyze information available in the public domain in conjunction with other information gathered during the investigation.

For example, in investigating an individual, it may be possible to gather background information concerning certain aspects of an individual's financial circumstances (for example, mortgages and other secured debts, old court judgments, and so on), educational and employment references, professional qualifications, and other details such as whether he or she has taken his or her annual vacation. Also worth exploring is corporate information such as jurisdiction of incorporation, authorized share capital, and the identity of all officers and directors since incorporation can often be obtained from the appropriate state office, usually the Secretary of State of the jurisdiction where the incorporation took place. In some jurisdictions, shareholder identities can be obtained. In many instances, private offshore corporations have less information available than publicly traded North American companies.

Public domain information may also provide critical clues or evidence. For example, comparison of a company's statistics and trends to others in its industry, that is, benchmarking, may identify unexplained variances that alert the forensic accountant to possible questionable activities or that warrant further investigation. At the very least, the background data will provide context for the detailed findings from the examination of nonpublic data.

There are many sources of public information about organizations, industries, and institutions. Very often a university reference library or a government resource center can provide access to documents, reference textbooks, computerized databases, and other sources of information that can assist in understanding and analyzing a case.

Documentary Evidence

At the beginning of any case involving documentary evidence, there are two key questions. What documents should be obtained? And where will they come from? These questions are usually resolved after discussions with available witnesses and an initial assessment of the findings to date. Depending on the circumstances, it may be necessary to involve the authorities to obtain a search warrant or begin legal proceedings so that a court could order the seizing of documents.

The main goal is to gather all documents that might be useful, bearing in mind that irrelevant documents can always be returned to their proper place. It is necessary to decide, in consultation with legal counsel, whether to be selective (that is, review all documents but take only those deemed necessary), or whether to remove or secure all of the documents from the premises by taking the filing cabinets, and so on. It is difficult to lay down hard and fast rules, but clearly the primary purpose is to obtain all documents that might be relevant without resorting to a *fishing expedition*.

The minimum requirements for financial documentation, for the period under investigation, are likely to be the following:

- Books and records, management reports, and statistical analyses pertaining either to the management of the company or to an individual.
- Documentation pertaining to the movement of assets into and out of a company.
- Relevant correspondence.
- Personal documentation, such as bank-account records.

Documents, including seized documents, should be properly identified and catalogued. Documents must be handled carefully. They should not be written upon, altered, stapled or unstapled during the course of the investigation. The investigating accountants, in particular, should bear this in mind.

Documents should be examined in detail and categorized as follows:

1. Documents required for evidence.
2. Documents required for rebuttal of the defense arguments.
3. Documents required for other reasons.
4. Documents that can be returned.

Once the documents have been sorted into these groups, photocopies can be made to provide working copies for the investigating accountant to use when preparing schedules, and in general for the working paper files.

Documents will subsequently be selected, from among those photocopied, for use in the presentation of evidence in a court of law. They should be compiled and assembled into a document brief.

Admissibility of Accounting Evidence

It is important during the evidence gathering stage to consider the two forms of documentary accounting evidence that may be presented in a court of law:

1. *Primary*, that is, the original, individual accounting documents obtained from the parties concerned or other sources.
2. *Secondary*, that is, summaries and schedules based on the original documents, which are produced by an accountant after examining the primary evidence.

The issue of whether secondary accounting evidence should be admissible has been argued in the courts for many years. Two opinions that allowed secondary accounting evidence, are described below.

In the first case, the court ruled, and was upheld on appeal, that a summary of documentary evidence was admissible. The court said, however, that the summary was in itself not evidence of the underlying facts; rather, it was strictly an aid to understanding primary evidence that had already been established. The judge made the following observations about the use of secondary evidence:

1. No more reliance could be placed on the survey than was placed on the primary evidence it was intended to summarize.
2. The summary did not prove the veracity and content of the primary evidence.
3. Any summary of primary evidence must show every weakness previously determined as existing within the primary evidence.

In the second case, the court ruled that an exhibit prepared by an accountant, based on the documentation before the court, be introduced into evidence because it helped to simplify and trace the many transactions previously discussed in the court. The defense was concerned that the exhibit expressed the independent opinions of the accountant who prepared the material and, therefore, was not objective. However, the judge ruled that any opinions reflected in the exhibit were opinions that were readily ascertainable from the documents themselves—the primary evidence.

Interview Techniques and How to Conduct Them¹

CPA practitioners—whether they stop to realize it or not—use interviews extensively in the routine performance of their tasks. Some of these interviews are long and complicated, such as when an auditor is learning about and documenting a company’s internal control structure. Still others are simple and direct. But the point is that audits and other such examinations are conducted through observation *and* inquiry.

Knowing how to conduct a proper interview will help improve a CPA practitioner’s overall effectiveness, regardless of whether or not these interviews involve possible fraud. As a matter of fact, the interview techniques described herein can be used in virtually any situation. For all purposes, the types of questions that can be asked are broken down into five types: (1) introductory, (2) informational, (3) closing, (4) assessment, and (5) admission seeking. The last two categories are used only when the interviewee’s truthfulness and complicity is suspect.

¹ Adapted from *Fraud Investigation Methods* (self-study CPE course) by Joseph Wells, CFE, CPA, Austin, TX: Association of Certified Fraud Examiners, 2003.

Interview Preparation

Before embarking on an interview, the practitioner should review appropriate working papers and other documents in order to ensure that important information that has not been overlooked.

The practitioner should determine what type of information can be supplied by each of the potential witnesses. Generally, the most vulnerable witness should be interviewed after the more reluctant witnesses. This provides a broader base of information that can be used to formulate future questions. However, the timing of interviews is at the discretion of the examination team.

Characteristics of a Good Interview

Good interviews share common characteristics. The interview should be of sufficient length and depth to uncover relevant facts. Most interviewers tend to get too little, rather than too much, information. The interview should be conducted as closely as possible to the event in question, because with the passage of time, memories of potential witnesses and respondents become faulty, and critical details can be lost or forgotten. A good interview is *objective* in scope and it should be aimed at gathering information in a fair and impartial manner.

Characteristics of a Good Interviewer

All good interviewers share certain characteristics. Above all, they are “people persons,” and are talented at human interaction. Successful interviewers are the types of people with whom others are willing to share information. The good interviewer does not interrupt the respondent with unnecessary questions since during an interview, much pertinent information results from volunteered information, as opposed to responses to a specific question. The good interviewer displays interest in the subject, and in what is being said. If the respondent perceives that the interviewer is biased or is attempting to confirm foregone conclusions, the respondent will be less likely to cooperate. Accordingly, the interviewer should make every effort to demonstrate a lack of bias.

Professionalism in the interview often involves a state of mind and a commitment to excellence. The interviewer should be on time, be professionally attired, and be fair in all dealings with the respondent. It is absolutely vital that the interviewer not appear to be a threat, for if persons perceive they are the target of an inquiry, they will be less likely to cooperate. An organization's dress code should be considered when attending an interview. For example, in some situations, a tie could be viewed as a threat.

Interview Rules

Interview One Person at a Time. One of the basic rules of interviewing is to question only one person at a time since the testimony of one respondent will invariably influence the testimony of another. There are few hard and fast rules with regard to interviewing, but this is one of them.

Privacy. Another basic rule is to conduct interviews under conditions of privacy. The interview is best conducted out of the sight and sound of friends, relatives, or fellow employees since people are very reluctant to furnish information within the hearing range of others.

1. Introductory Questions

One of the most difficult aspects—perhaps the hardest part—of conducting an interview is getting started. In many instances the interviewer and the respondent have not previously met. The interviewer has a tall order: meet the person, state a reason for the interview, establish necessary rapport, and get the information. The introduction is accomplished through questions rather than statements. Questions allow the interviewer to assess feedback from the respondent. This is an important aspect of the introduction. If the respondent is reluctant to be interviewed that fact will become established through the introductory questions.

Establish the Purpose of the Interview

The purpose of the interview must be established during the introductory phase. Obviously, when the interviewer makes official contact with a respondent some reason must be given. The reason or purpose of the interview should be general, not specific. The specific interview purpose will be related to the respondent later in the interview process. The stated purpose for the interview should be one that is logical enough for the respondent to accept and easy for the interviewer to explain. Normally, the more general the reason that is given, the better.

If the CPA is conducting interviews under the auspices of the attorney-client privilege (see Legal Section), it is normally appropriate to announce that to the respondent. Under those conditions, the person being interviewed should be told that the results of his/her interview may be disclosed to third parties.

Ask Non-Sensitive Questions

Sensitive questions should be scrupulously avoided until well into the interview, and then such questions should be asked only after careful deliberation and planning. During the introductory phase, emotive words of all types should generally be avoided. Since they normally put people on the defensive and make them less reluctant to answer and to cooperate.

Example. Generally, during the introductory phase of an interview, it is best not to use emotive words. You should try to use “softer” words as shown by the following examples:

| | Instead of | Use |
|--|--------------------------|---------------------------------------|
| | Investigation | <i>Inquiry</i> |
| | Audit | <i>Review</i> |
| | Interview | <i>Ask a few questions</i> |
| | Embezzlement/steal/theft | <i>Shortage or paperwork problems</i> |

2. Informational Questions

Informational questions are non-confrontational, non-threatening, and asked for the purpose of gathering information. The great majority of the interviewer’s questions fall into this category. Types of questions include the following:

- Conducting an interview to gain an understanding of accounting control systems.
- Interviews concerning documents.

- Gathering information regarding business operations or systems.
- Pre-employment interviews.
- Background information, if not known.

Informational questions seek to elicit unbiased factual information. The interviewer will be alert to inconsistency in facts or behavior. Informational questions—as well as others—fall into several general categories:

- Open
- Closed
- Leading
- Double-negative
- Complex
- Attitude

Open Questions

Open questions are those questions worded in such a way that “yes” or “no” answers become difficult. Furthermore, the answer is not dependent on the question. The typical open question calls for a monologue response, and it can be answered in several different ways. During the information phase of the interview, the interviewer should endeavor to ask primarily open questions in order to stimulate conversation. Some of the best open questions are subtle commands.

Example. Open questions typically start with “**what,**” “**what about,**” “**how,**” “**could it be,**” etc.

- “*What were your job duties as assistant controller?*”
- “*How do you normally process these types of invoices?*”
- “*What types of payments required Mrs. Smith’s approval?*”

Closed Questions

Closed questions are those questions that require a precise answer, usually “yes” or “no.” Closed questions also deal with specifics such as dollar amounts, dates, and times. As much as possible, closed questions should be avoided in the informational part of the interview, but used extensively in completing the interview, described later.

Leading Questions

Leading questions contain the answer as a part of the question. Most commonly, they are used to confirm facts that are already known. Although leading questions are usually discouraged in court proceedings, they can be used effectively in interview situations.

Double-Negative Questions

Negative questions or statements are confusing and often suggest an answer opposite to the correct one. They should not be used. Example: “How could it not be that you do not know?”

Complex Questions

Complex questions and statements are too complicated to be easily understood when they cover more than one subject or topic, require more than one answer, and/or require a complicated answer. They should be avoided.

Attitude Questions

The attitude of the interviewer can be conveyed by the structure of a question or statement and the manner in which a question is asked. When the interviewer wishes to establish a friendly mood, for instance, “attitude” questions can be employed.

Question Sequences

As a general rule, questioning should proceed from the general to the specific; that is, it is best to seek general information before seeking details. A variation is to “reach backward” with questions, by beginning with known information and working toward unknown areas. An efficient method of doing this is to recount the known information and then frame the next question as a logical continuation of the facts previously related.

It is common, especially in accounting and fraud-related matters, for figures or numbers to be critical. Unfortunately, some witnesses are unable to recall specific amounts. The interviewer can jog the memory of the respondent by comparing unknown items with items of known quantity.

Example. To jog interviewee’s memory regarding numbers or figures, try the following:

Interviewer. “Was the amount of money involved more than last year’s figure?”

Controlled Answer Techniques

Controlled answer techniques or statements may be used to stimulate a desired answer or impression. These techniques direct the interview toward a specific point. For example, it may be possible to get a person to admit knowledge of a matter by phrasing the question as follows: “*I understand you were present when the internal controls were developed, so would you please describe how they were constructed?*” This phrasing provides a stronger incentive for the respondent to admit knowledge than does: “*Were you present when the internal controls were developed?*”

To stimulate the person to agree to talk or provide information, you may use an example such as, “*Because you are not involved in this matter, I am sure you would not mind discussing it with me?*” This provides a stronger incentive to cooperate than: “*Do you have any objection to telling me what you know?*” Avoid negative construction, such as: “*I don’t guess you would mind answering a few questions?*”

Free Narratives

The *free narrative* is an orderly, continuous account of an event or incident, given with or without prompting. It is used to get a quick summary of what is known about a matter. Be sure to designate specifically the occurrence you wish to discuss.

Sometimes the respondent must be controlled to prevent unnecessary digression. Otherwise, use a minimum of interruptions, and do not stop the narrative without good

reason. The respondent will sometimes provide valuable clues when talking about things only partially related to the matter under inquiry.

Informational Question Techniques

Below are suggestions to improve the quality of the interview during the information-gathering phase.

- Begin by asking questions that are not likely to cause the respondent to become defensive or hostile.
- Ask the questions in a manner that will develop the facts in the order of their occurrence or in some other systematic order.
- Ask only one question at a time, and frame the question so that only one answer is required.
- Ask straightforward and frank questions, and generally avoid shrewd approaches.
- Give the respondent ample time to answer. Do not rush.
- Try to help the respondent remember, but do not suggest answers. Be careful not to imply a particular answer through facial expressions, gestures, methods of asking questions, or types of questions asked.
- Repeat or rephrase questions, if necessary, to get the facts.
- Be sure that you understand the answers. If they are not perfectly clear, have the respondent interpret them at that time instead of saving this for later.
- Provide the respondent with an opportunity to qualify his/her answers.
- Separate facts from inferences.
- Have the respondent give comparisons by percentages, fractions, estimates of time and distance, and other such comparisons to ascertain accuracy.
- Get all of the facts. Almost every respondent can give you information beyond what was initially provided.
- Once the respondent has given a narrative account, ask questions about every item that has been discussed.
- Upon conclusion of the direct questioning, ask the respondent to summarize the information given. Then summarize the facts, and have the respondent verify that they are correct.

Note-Taking

The interviewer will need to take notes frequently during the interview. Start each interview on a separate sheet of paper. This procedure can be especially helpful should documents from a particular interview be subpoenaed. Do not try to write down all the information you are given during an interview, only the pertinent facts. Taking too many notes will make the interview process cumbersome and may inhibit the respondent. If a quote is particularly relevant, try to write it down verbatim. Enclose all direct quotes in quotation marks.

Do not slow down the interview process for note-taking. Instead, jot down key words or phrases, then go back over the details at the end of the interview. In general, it is better to err on the side of taking too few notes rather than too many.

Maintain Eye Contact. Maintain eye contact with the respondent as much as possible during note-taking. Just as eye contact personalizes all human communication, it creates a more comfortable environment and facilitates the flow of information during the interview process.

Opinions. Avoid making notes regarding your overall opinions or impressions of a witness. Such notes can cause problems with your credibility if they are later produced in court. Be careful not to show excitement when taking notes. During interviews of targets and adverse witnesses, take notes in a manner that does not indicate the significance of the information; that is, never allow note-taking to “telegraph” your emotions.

Writing down Questions. Whenever possible, do not write down a list of interview questions. Let the interview flow freely. Inadvertently allowing the respondent to read a written list of questions can provide an opportunity for him/her to fabricate an answer. Certainly, writing down key points the interviewer wants to discuss may be appropriate.

Documenting Results. Expand the notes from the results of questioning as soon as possible after concluding the interview—preferably immediately afterward. If this procedure is followed, the fraud examiner will not have to take copious notes during the interview. Law enforcement officials are generally required to maintain notes. In the private sector, notes can usually be destroyed once a memorandum has been prepared summarizing the interview.

Observing Interview Reactions

The interviewer must be knowledgeable about the behavior of individuals during an interview situation. Most nonverbal clues to behavior fall within one of the following categories: *proxemics*, *chronemics*, *kinetics*, or *paralinguistics*.

- *Proxemic communication* is the use of interpersonal space to convey meaning.
- *Chronemic communication* is the use of time in interpersonal relationships to convey meaning, attitudes, and desires.
- *Kinetic communication* is the use of body movement to convey meaning.
- *Paralinguistic communication* is the use of volume, pitch, and voice quality to convey meaning.

Interview Methodology

Make a Transition from the Introduction. Once the introduction has been completed, the interviewer needs a transition to the body of the interview. Usually this is accomplished by asking the person an easy question about themselves or their duties.

Begin with Background Questions. Assuming the respondent does not have a problem answering the transitional question, the interviewer should then ask a series of easy, open questions designed to get the respondent to talk about him/herself.

Observe Verbal and Nonverbal Behavior. When the respondent is talking about him/herself, the interviewer should discreetly observe verbal and nonverbal behavior. Observing behaviors during the initial stages of the interview serves as a baseline for observing later reactions.

Ask Non-Leading (Open) Questions. Open questioning techniques are used almost exclusively in the informational phase of the interview. The questions must be inquisitory and not accusatory. Remember, the most effective questions are constructed as a subtle command. Once the respondent has answered open questions, the interviewer can go back and review the facts in greater detail. If the answers are inconsistent, try to clarify them. But the interviewer should not challenge the honesty or integrity of the respondent at this point.

Approach Sensitive Questions Carefully. Words such as “routine questions” can be used to minimize the significance of the inquiry. It is important for information gathering purposes that the interviewer does not react excessively to the respondent’s statements. The interviewer should not express shock, disgust, or similar emotions during the interview. Examples of ways to discuss fraud within a company follow. The questions are posed in a hypothetical way to avoid being accusatory.

Example: Examples of non-accusatory questions:

Interviewer:

- “Part of my job is to prevent and uncover waste, fraud, and abuse. You understand that, don’t you?”
- “Please tell me where you think the company is wasting assets or money.”
- “What, in your opinion, can we do in your department to save more money for the company?”
- “Where do you think the company is vulnerable to someone abusing his/her position?”

3. Closing Questions

Closing the interview on a positive note is a must in informational interviews. The closing serves several purposes. First, it is not unusual for the interviewer to have misunderstood or misinterpreted statements of the respondent. Therefore, the interviewer should review key facts to ensure that they have been understood. Secondly, the closing questions phase also seeks to obtain facts previously unknown. It provides respondents additional opportunity to say whatever they want about the matter at hand. If appropriate, the interviewer can ask if there are other documents or witnesses that would be helpful to the case. Do not promise confidentiality; instead say, “*I’ll keep your name as quiet as possible.*” Finally, the interviewer should leave the discussion on a positive note.

Persons being interviewed often do not volunteer additional information regarding other witnesses or evidence. Therefore, provide the respondent an opportunity to furnish further relevant facts or opinions. At the conclusion, attempt to determine which facts provided by the respondent are the most relevant. Do not attempt to go over all the information a second time.

Example. Before ending the interview, go over each of the key facts given by the witness in summary form. This gives the respondent an opportunity to provide additional facts or opinions.

Interviewer: “Ms. Jones, I want to make sure that I have my information straight. Let me take a minute and summarize what we’ve discussed.”

Go over each of the key facts, in summary form. The questions should be closed, so that the witness can respond either “yes” or “no.” To obtain additional facts, ask respondents if there is something else they would like to say. This gives the correct impression that the interviewer is interested in all relevant information, regardless of which side it favors. Try to actively involve the respondent in helping solve the case—*“If you were trying to resolve this issue, what would you do?”*

Ask if the respondent has anything else to say. This gives the respondent one final chance to make any statement. Also, ask if the interviewer may call at a later time with any additional questions, thus leaving the door open for additional cooperation.

Leave the respondent a business card or a telephone number. Invite the respondent to call with anything else relevant. In some cases the interviewer should attempt to obtain a commitment that the respondent will not discuss the matter. This step is not recommended with adverse or hostile respondents.

Physiology of Deception

It is said that everyone lies and does so for one of two reasons: to receive rewards or to avoid punishment. In most people, lying produces stress. The human body will attempt to relieve this stress (even in practiced liars) through verbal and nonverbal clues.

Conclusions concerning behavior must be tempered by a number of factors. The physical environment in which the interview is conducted can affect behavior. If the respondent is comfortable, fewer behavior quirks may be exhibited. The more intelligent the respondent, the more reliable verbal and nonverbal clues will be. If the respondent is biased toward the interviewer, or vice versa, this will affect also behavior.

Persons who are mentally unstable, or under the influence of drugs, will be unsuitable to interview. Behavior symptoms of juveniles are generally unreliable. Racial, ethnic, and economic factors should be carefully noted. Some cultures, for example, discourage looking directly at someone. Other cultures use certain body language that may be misinterpreted. Because professional pathological liars are often familiar with interview techniques, they are less likely to furnish observable behavioral clues.

4. Assessment Questions: Norming or Calibrating

Norming or *calibrating* is the process of observing behavior before critical questions are asked, rather than during questioning. Norming should be a routine part of all interviews. Persons with truthful attitudes will answer questions one way; those with untruthful attitudes will generally answer them differently. Assessment questions ask for agreement with matters that are against the principles of most honest people. In other words, dishonest people are likely to agree with many of the statements, while honest people will not. Assessment questions are designed primarily to elicit a verbal or nonverbal reaction from the respondent. The interviewer will then carefully assess each reaction. Suggestions for observing the verbal and physical behavior of the respondent include the following:

- Use your senses of touch, sight, and hearing to establish a norm.
- Do not stare or call attention to the person’s behavior symptoms.

- Be aware of the respondent's entire body.
- Observe the timing and consistency of behavior.
- Note clusters of behaviors.

On the basis of a respondent's reaction to assessment questions, the interviewer then considers all the verbal and nonverbal responses together (not in isolation) to decide whether or not to proceed to the admission-seeking phase of the interview. The presence of several verbal and/or nonverbal clues is usually necessary to conclude deception on the part of the respondent.

Verbal Clues

Changes in Speech Patterns. Deceptive persons often speed up or slow down their speech, or speak louder. There may be a change in the voice pitch; as a person becomes tense, the vocal chords constrict. Deceptive persons also have a tendency to cough or clear their throats during times of deception.

Repetition of the Question. Liars will frequently repeat the interviewer's question, in order to gain more time to formulate an answer. The deceptive individual will say, "*What was that again?*" or use similar language.

Comments Regarding Interview. Deceptive persons will often complain about the physical environment of the interview room, such as, "*It's cold in here.*" Or sometimes they will ask how much longer the interview will take.

Selective Memory. In some cases the deceptive person will have a keen memory for insignificant events, but when it comes to the important facts, the person, "*just can't seem to remember.*"

Making Excuses. Dishonest persons will frequently make excuses about things that look bad for them, such as, "*I'm always nervous; don't pay any attention to that.*"

Oaths. Dishonest persons often will add what they believe to be credibility to their lies through emphasis. Expressions such as "*I swear to God,*" "*Honestly,*" "*Frankly,*" or "*To tell the truth,*" are frequently used.

Character Testimony. A liar often will request that the interviewer, "*Check with my wife,*" or "*Talk to my minister.*" This is often done to add credibility to a false statement.

Answering with a Question. Rather than deny allegations outright, the liar may answer with a question such as, "*Why would I do something like that?*" As a variation, the deceptive person will sometimes question the interview procedure by asking, "*Why are you picking on me?*"

Overuse of Respect. Some deceptive people will go out of their way to be respectful and friendly. When accused of wrongdoing, it is unnatural for a person to react in a friendly and respectful manner.

Example. Overuse of respect may be a sign of deceit:

Respondent: "I'm sorry, sir. I know you're just doing your job, but I didn't do it."

Increasingly Weaker Denials. When an honest person is accused of something he/she did not do, that person is likely to become angry or forceful in making the denial. The more the person is accused, the more forceful the denial becomes. The dishonest person, on the other hand, is likely to make a weak denial. Upon repeated accusations, the dishonest person's denials become weaker, sometimes to the point of complete silence.

Failure to Deny. Dishonest persons are more likely than honest persons to deny an event specifically. An honest person may offer a simple and clear "no," while the dishonest person will qualify the denial: "No, I did not steal \$43,500 from the Company on June 27." Other qualified denial phrases include: "To the best of my memory," "As far as I recall," or similar language.

Avoidance of Emotive Words. A liar will often avoid emotionally provocative terms such as "steal," "lie," and "crime." Instead, the dishonest person frequently prefers "soft" words such as "borrow," and "it" (referring to the deed in question).

Refusal to Implicate Other Suspects. Both the honest respondent and the liar will have a natural reluctance to name others involved in misdeeds. However, the liar will often refuse to implicate possible suspects, no matter how much pressure is applied by the interviewer because the culpable person does not want the circle of suspicion to be narrowed.

Tolerant Attitudes. Dishonest persons typically have tolerant attitudes towards miscreant conduct. The interviewer in an internal theft case may ask, "What should happen to this person when he/she is caught?" The honest person usually will say, "They should be fired/prosecuted." The dishonest individual, on the other hand, is much more likely to reply, "How should I know?" or, "Maybe he/she is a good employee who got into problems. Perhaps he/she should be given a second chance."

Reluctance to Terminate Interview. Dishonest persons generally will be more reluctant than honest ones to terminate the interview. The dishonest individual wants to convince the interviewer that he/she is not responsible, so that the investigation will not continue. The honest person, on the other hand, generally has no such reluctance.

Feigned Unconcern. The dishonest person will often attempt to appear casual and unconcerned and therefore adopt an unnatural slouching posture, reacting to questions with nervous or false laughter or feeble attempts at humor. The honest person, on the other hand, will typically be very concerned about being suspected of wrongdoing, and will treat the interviewer's questions seriously.

Nonverbal Clues

Full Body Motions. When asked sensitive or emotive questions, the dishonest person will typically change his/her posture completely, as if moving away from the interviewer. The honest person will frequently lean forward toward the interviewer when questions are serious.

Anatomical Physical Responses. Anatomical physical responses are those involuntary reactions the body has when frightened, such as increased heart rate, shallow or labored breathing, or excessive perspiration. These reactions are typical of dishonest people accused of wrongdoing.

Illustrators. Illustrators are the motions made primarily with the hands to demonstrate points when talking. In response to nonthreatening questions, the illustrators may be done at one rate, while during threatening questions, the use of illustrators may increase or decrease.

Hands over the Mouth. Frequently, a dishonest person will cover his/her mouth with the hand or fingers during deception. This reaction goes back to childhood, when many children cover their mouths as they tell a lie. Such gestures are done subconsciously to conceal the statement.

Manipulators. Manipulators are those motions such as picking lint from clothing, playing with objects such as pencils, or holding one's hands while talking. Manipulators are displacement activities to reduce nervousness.

Fleeing Positions. During an interview, dishonest people will often posture themselves in a "*fleeing position*," where the head and trunk face the interviewer and the feet and lower portion of the body point toward the door in an unconscious effort to flee from the interviewer.

Crossing the Arms. Crossing one's arms over the middle zones of the body is a classic defensive reaction to difficult or uncomfortable questions. A variation is crossing the feet under the chair and locking them. These crossing motions occur mostly when the interviewee is being deceptive.

Reaction to Evidence. While attempting to be outwardly unconcerned, the guilty person will have a keen interest in implicating evidence. The dishonest person will often look at documents presented by the interviewer, attempt to be casual about observing them, and then shove them away, as if wanting nothing to do with the evidence.

Most actions that are designed to interrupt the flow of speech are stress related. Examples include

- Closing the mouth tightly.
- Pursing lips.
- Covering the mouth with the hand.
- Lip and tongue biting.
- Licking the lips.
- Chewing on objects.

Genuine smiles usually involve the whole mouth; false ones are confined to the upper half. Persons involved in deception tend to smirk rather than to smile.

Crossing. The body or legs may be crossed to reduce stress. When the hands are crossing the body, it is a defensive gesture to protect the "soft underbelly."

5. Admission-Seeking Questions

CPAs are rarely required to directly challenge the honesty or complicity of individuals, but it does happen. Imagine, for instance, a situation where, during a normal audit, you discover a material asset misappropriation that appears to have been committed by the chief financial officer. It becomes obvious that someone will have to question the CFO for

more details. Should that be you, the practitioner? Should it be a private fraud examiner? A law enforcement official? An attorney?

The answer, of course, depends entirely on the circumstances. Today's CPA practitioner, unlike two generations ago, is responsible for helping to detect fraud. As a result, you should clearly understand how experts get suspects to confess. To police officials, this is often known as *interrogation*. In the private sector it is more common to call the process an *admission-seeking interview*. Since this process is fraught with legal pitfalls, it should be conducted with extreme care by qualified individuals.

The interviewer should ask accusatory or admission seeking questions only when there is a reasonable probability that the respondent has committed the act in question. An assessment of culpability may be based on verbal and nonverbal responses to interview questions, as well as documents, physical evidence, and other interviews.

Conducting an Admission-Seeking Interview

The interview should be scheduled when the interviewer can control the situation. Normally it should not be conducted on the accused's turf and is best conducted by surprise.

Interview Room

The location should establish a sense of privacy. The door should be closed but not locked, and there should be no physical barriers preventing the target from leaving. This helps avoid allegations of *custodial interrogation*. Custodial interrogation is generally considered to occur when the suspect is being held against his/her will.

Distractions should be kept to a minimum. Ideally, there should be no photographs, windows, or other objects in the room. Chairs should be placed about six feet apart, and the accused should not be permitted to sit behind a desk. This is to prohibit a psychological barrier for the accused to "hide behind." Note taking during the interview should be done in a way that does not reveal their significance.

Presence of Outsiders

Do not suggest to the accused that he/she should have counsel present although, this right cannot be denied. If counsel is present, you should have an understanding that he/she will be strictly an observer. Attorneys should neither ask nor object to questions. A CPA practitioner must be very careful in questioning a witness whose lawyer is present. In fact, it is discouraged in most instances. If the situation cannot be avoided, consider having your own lawyer on standby. Other than the accused and two fraud examiners, no other observers should usually be permitted in the admission-seeking interview. If the accused is in a union, a representative may have the right to attend. However, this could present legal problems in "broadcasting" the allegation to a third party. It is very difficult to obtain a confession with witnesses present. The fraud examiner should, therefore, consider whether the case can be proven without the admission-seeking interview.

Miranda Warnings

As a general rule, Miranda warnings are not required by CPA practitioners unless there is some form of *state action* involved. However, if it is likely that the results of the investigation will be turned over to law enforcement for prosecution, it is wise to consult legal counsel to

ensure that subsequent prosecution is not tainted by failure to follow the proper procedures.

6. Steps in the Admission-Seeking Interview

Direct Accusation. The accusation should not be made in the form of a question, but a statement. Emotive words such as “steal,” “fraud,” and “crime” should be avoided during the accusatory process. The accusation should be phrased so that the accused is psychologically “trapped” with no way out.

Example. The accusation should usually be in the form of a clear statement. However, experts usually avoid emotive words such as “crime,” “fraud,” and so forth.

Wrong:

- “We have reason to believe that you...”
- “We think [suspect] you may have....”

Right:

- “Our investigation has established that you
 - Made a false entry. (Avoid “fraud.”)
 - Took company assets without permission. (Avoid using “theft,” “embezzlement,” or “stealing.”)
 - Took money from a vendor. (Avoid “bribe” or “kickback.”)

Observe Reaction. When accused of wrongdoing, the typical guilty person will react with silence. If the accused does deny culpability, those denials will usually be weak, and in some cases the accused will almost mumble the denial. It is common for the culpable individual to avoid outright denials. Rather, the person will give reasons why he/she could not have committed the act in question. The innocent person will sometimes react with genuine shock at being accused. It is not at all unusual for an innocent person, wrongfully accused, to react with anger. As opposed to the guilty person, the innocent person will strongly deny carrying out the act or acts in question.

Repeat Accusation. If the accused does not strenuously object after the accusation is made, it should be repeated with the same degree of conviction and strength.

Interrupt Denials. Both the truthful and untruthful person will normally object to the accusation and attempt denial. It is very important in instances where the fraud examiner is convinced of the individual's guilt that the denial be interrupted. An innocent person is unlikely to allow the interviewer to prevail in stopping the denial.

It becomes extremely difficult for the accused to change a denial once it is uttered. If the person denies the accusation and later admits to the same accusation, he/she is admitting to lying. This is very hard to do. The interviewer's job is to make this task easier. Several techniques can stop or interrupt denials. A guilty person more than an innocent one is likely to stop short of an outright denial (“*I didn't do it.*”), and more apt to furnish the interviewer with explanations as to why he/she is not the responsible party.

It is important to emphasize that both the innocent and culpable will make an outright denial if forced to do so. Accordingly, the interviewer should not solicit a denial at this stage of the admission-seeking interview.

Delays. One of the most effective techniques to stop or interrupt the denial is through a delaying tactic. The interviewer should not argue with the accused, but rather attempt to delay the outright denial.

Usually, the innocent person will not “hold on,” or let the interviewer continue to develop the theme.

Reasoning. If these techniques prove unsuccessful, the interviewer may attempt to reason with the accused, and employ some of the tactics normally used for defusing alibis. Present the accused with evidence implicating him/her. Normally, the interviewer should not disclose all the facts of the case, but rather small portions here and there.

Establish Rationalization. Once the accusation has been made, repeated, and denials are stopped, it is time for the interviewer to establish a morally acceptable rationalization that will allow the accused to square the misdeed with his/her conscience. It is not necessary that this theme be related to the underlying causes of the misconduct. It is common and acceptable for the accused to explain away the moral consequences of the action by seizing any plausible explanation other than being a “bad person.”

If the accused does not seem to relate to one theme, the interviewer should go on to another until one seems to fit. Thereafter, that theme should be developed fully. Note that the theme development explains away the moral—but not the legal—consequences of the misdeed. The interviewer is cautioned not to make any statements that would lead the accused to believe he/she will be excused from legal liability by cooperating.

Rather than being confrontational, questions posed should constantly seek agreement from the accused. The interviewer must strike a balance between being in control of the interview and still appearing compassionate and understanding. No matter what the accused has supposedly committed, the interviewer should not express shock, outrage, or condemnation.

Example. If the person being interviewed feels that the interviewer empathizes or understands the situation, it may cause the person to be more candid and ultimately confess to the crime.

Interviewer:

“All of us have done things that we’re not proud of. I’ve done things that I’m not proud of, but that doesn’t mean I’m a bad person. However, there comes a time when we have to admit our mistakes and make amends.”

“When people get in desperate circumstances, sometimes they do things they wouldn’t otherwise do.”

“If my boss had done that to me, I would’ve been angry too. I can see that you might have wanted to get back at him.”

Diffuse Alibis. Even if the accused is presented with an appropriate rationalization, it is likely that he/she will continue to deny culpability. Once the interviewer is successful in stopping denials, the accused will normally turn to various reasons why he/she could not

have committed the act in question. The purpose of this stage is to convince the accused of the weight of the evidence against him/her. Miscreants usually express a keen interest in evidence that tends to implicate them. Alibis can generally be diffused by using one of the methods listed below.

Display Physical Evidence. It is common for most guilty persons to overestimate the amount of physical evidence. The interviewer wants to try and reinforce this notion in the way the evidence is presented to the accused. The physical evidence, usually documents in fraud matters, generally should be displayed one piece at a time in reverse order of importance. In this way the full extent of the evidence is not immediately known by the accused. When the accused no longer denies culpability, the interviewer should stop displaying evidence.

Each time a document or piece of evidence is exposed to the accused, its significance should be noted by the interviewer. During this phase, the accused tries to accept that he/she has been caught. The interviewer should, therefore, expect that the accused will attempt to lie his/her way out of the situation. Like denials, the interviewer should stop the alibis and other falsehoods before they are fully articulated.

Once alibis are diffused, the interviewer should return to the theme being developed. The following is an example of this technique: A purchasing agent has established a fictitious company and embezzled money by approving payments from his employer to a shell corporation.

Example.

Respondent: "I couldn't have done this. I am required to have invoices approved by my supervisor."

Interviewer: "Here is one of the invoices in question (display document). You have signed your supervisor's name." (Do not mention whether or not you have talked to the supervisor or whether you have subjected the invoice to document analysis.)

"Look Bob, it is useless for you to try to deny the truth. We have lots of evidence. Let's just try to work this out, but you've got to help me, O.K.?" (Do not accuse the person of lying. This just prolongs the process.)

Discuss Witnesses. Another technique for diffusing alibis is to discuss the testimony of witnesses. The objective is to give enough information about what other persons said without providing too much. Ideally, the interviewer's statement will create the impression in the mind of the accused that many people are in a position to contradict his/her story.

The interviewer should not furnish enough information to the accused so that he/she can identify witnesses. This may place witnesses in a difficult position, as the accused could contact the witness in an effort to influence testimony. The accused could seek reprisal against potential witnesses, although this rarely occurs.

Discuss Deceptions. The final technique is to discuss the accused's deceptions with the purpose of appealing to his/her logic, not to scold or degrade. Lacking physical evidence, this technique is sometimes the only one available. As with other interview situations, the word "*lying*" should be avoided.

Present Alternative. After the accused's alibis have been diffused, he/she normally will become quiet and withdrawn. Some people in this situation cry. If so, be comforting. Do not discourage the accused from showing emotion. In this stage the accused is deliberating whether or not to confess at this point, the interviewer should present an alternative question to the accused. The alternative question forces the accused to make one of two choices: one alternative allows the accused a morally acceptable reason for the misdeed, while the other paints the accused in a negative light. Regardless of which answer the accused chooses, he/she acknowledges guilt.

Benchmark Admission

Either way the accused responds to the alternative question, either "yes" or "no", he/she has made a culpable statement, or *benchmark admission*. Once the benchmark admission is made, the miscreant has subconsciously decided to confess. Alternative questions are structured so that the negative alternative is presented first, followed by the positive alternative. In this way the accused only has to nod, or say "yes," for the benchmark admission to be made. The accused will also commonly answer in the negative.

Should the accused still not respond to the alternative question with the benchmark admission, the interviewer should repeat the questions, or variations thereof, until the benchmark admission is made. It is important for the interviewer to get a response that is tantamount to a commitment to confess. Because only a commitment is sought at this point, the questions for the benchmark admission should be constructed as leading questions, so they can be answered "yes" or "no," rather than requiring any sort of explanation. That will come later.

Reinforce Rationalization

Once the benchmark admission is made, the interviewer should reinforce the confessor's decision. Then the interviewer should make the transition to the verbal confession, where the details of the offense are obtained. Reinforcing the rationalization developed earlier will help the confessor feel comfortable, believing that the interviewer does not look down on him/her.

Verbal Confession

Transition to the verbal confession is made when the accused furnishes the first detailed information about the offense. Thereafter, it is the interviewer's job to probe gently for additional details, preferably including those that would be known only to the miscreant. As with any interview, there are three general approaches to obtaining the verbal confession: chronologically, by transaction, or by event. The approach taken should be governed by the circumstances of the case.

During the admission-seeking interview, it is best to first confirm the general details of the offense. For example the interviewer will want the accused's estimates of the amounts involved, other parties to the offense, and the location of physical evidence. After these basic facts are confirmed, the interviewer can then return to the specifics in chronological order. It is imperative that the interviewer obtain an early admission that the accused knew the conduct in question was wrong. This confirms the essential element of intent.

Because of the nature of the psychology of confessions, most confessors will lie about one or more aspects of the offense, even though confirming overall guilt. When this happens

during the verbal confession, the interviewer should make a mental note of the discrepancy and proceed as if the falsehood had been accepted as truthful.

Discrepancies should be saved until all other relevant facts are provided by the accused. If the discrepancies are material to the offense, then the interviewer should either resolve them at the end of the verbal confession or wait and correct them in the written confession. If not material, such information can be omitted altogether from the written confession. The following information should be obtained during the verbal confession:

The Accused Knew the Conduct Was Wrong. Intent is required in all matters involving fraud. Not only must the confessor have committed the act, he/she must have intended to commit it.

Facts Known Only to Confessor. Once the intent question is solved, the questioning turns to those facts known only to the confessor. These facts include, as a minimum, the accused's estimates of the number of instances of wrongful conduct as well as the total amount of money involved. The questions should not be phrased so that the confessor can answer "yes" or "no."

Especially in fraud matters it is common for the accused to underestimate the amount of funds involved as well as the number of instances, no doubt because of a natural tendency of the human mind to block out unpleasant matters. Take the figures with a grain of salt. If the accused's response is "I don't know," start high with the amounts and gradually reduce them.

Establishing the Motive for the Offense. Motive is an important element in establishing the offense. The motive may be the same as the theme the interviewer developed earlier, or it may not. The most common response is "I don't know." The interviewer should probe for additional information, but if it is not forthcoming, then attribute the motive to the theme developed earlier.

When Offense Commenced. The interviewer will want to know the approximate date and time that the offense started.

When/If Offense Was Terminated. In fraud matters, especially internal fraud, the offenses are usually continuous. That is, the miscreant seldom stops before he/she is discovered. If appropriate, the interviewer should seek the date the offense terminated.

Others Involved. Most frauds are solo ventures, committed without the aid of an accomplice.

By asking who else "knew," the interviewer is in effect not only asking for the names of possible conspirators, but also about others who may have known what was going on but failed to report it. This question should be leading, not "did someone else know?" but rather "who else knew?"

Physical Evidence. Physical evidence, regardless of how limited it may be, should be obtained from the confessor. In many instances illicit income from fraud is deposited directly into the bank accounts of the perpetrator. The interviewer will typically want to ask the confessor to surrender his/her banking records voluntarily for review. It is recommended that

- A separate written authorization, or
- Language be added to the confession noting the voluntary surrender of banking information.

A separate written authorization is generally preferable. If other relevant records can be obtained only with the confessor's consent, permission to review those should be sought during the oral confession. In some instances it may be advisable to delay this step until the written confession is obtained.

Disposition of Proceeds. If not discussed previously, the interviewer should determine what happened to any illicit income derived from the misdeeds. Typically, the money is used for frivolous or ostentatious purposes. It is important, however, that the confessor sees his/her actions in a more positive light. The interviewer should avoid comments or questions relating to "high living."

Location of Assets. In appropriate situations the interviewer should find out if there are residual assets that the confessor can use to reduce losses. Rather than ask the accused, "*Is there anything left?*" the question should be phrased as, "*What's left?*"

Specifics of Each Offense. Once the major hurdles are overcome, the interviewer should then return to the specifics of each offense. Generally, this starts with the first incident and works in chronological fashion.

Because these questions are information seeking, they should be open phrased so that the answer is independent of the question. It is best to seek the independent recollections of the confessor first before displaying physical evidence. If the confessor cannot independently recall incidents, documents can be used to refresh his/her recollection. Generally, it is best to resolve all issues on each incident before proceeding to the next.

Example. In determining the specifics of the offense, the interviewer should usually ask,

"Who has knowledge of this transaction?"

"What does this document mean?"

"When did this transaction occur?"

"Where did the proceeds of the transaction go?"

Interviewing is difficult, and seldom mastered without considerable practice. The preceding techniques, when properly employed, can serve to develop truthful, reliable, legally valid information.

Private Investigators

It may also be necessary to engage private investigators to conduct surveillance of suspected perpetrators, for example, to observe their activity and record their presence at various locations and times, including meetings with certain individuals.

Forensic accountants who regularly work with private investigators as part of their team should be consulted for a recommendation regarding how to use investigators effectively, and whom to use.

Search and Seizure Mechanisms

In criminal matters, law enforcement agencies often obtain a search warrant to obtain documentary evidence. The forensic accountant may assist them in specifying on the search warrant those accounting, banking and other records that are to be seized as evidence of fraudulent activity. Depending on the jurisdiction, the forensic accountant may also be named on the warrant to attend its execution at the premises to be searched, in order to help identify those documents that are to be seized as evidence.

In civil matters, depending on the jurisdiction, different search and seizure mechanisms may also be available. The forensic accountant could provide assistance in obtaining evidence through the use of a seizure order, granted pursuant to a court application. Under the court's supervision, an order would permit counsel to recover documentary evidence from the other party. This evidence could otherwise have been destroyed or concealed.

Similarly if there is a concern that the assets of an individual under investigation may be dissipated, an injunction may be obtained from a court. This injunction would prohibit the individual under investigation from conducting his or her affairs in a manner that would financially prejudice the other party in a case prior to the court rendering its decision.

The rules governing civil suits in most jurisdictions allow discovery proceedings, which include answering either orally or in writing questions under oath and the production of documents, or some equivalent process. During discovery, the forensic accountant can

(Text continued on page 11)

assist counsel in requesting documents to be produced by the other party and in determining questions to be put to the witnesses for the other party.

The Role of Computers

Over the years, the role of computers in investigations has increased exponentially; for example, the use of the Internet as a research tool and the development of faster, more efficient software to assist in the investigative process.

Investigative software now includes many packages that are designed to assist the forensic accountant, investigator or lawyer with his or her work. For instance, scanners can be used to scan in huge volumes of paper evidence that can then be searched via keywords or phrases and organized using a database for quick reference later in the case. Queries can be generated in a matter of minutes, which search through databases of millions of transactions, to identify the proverbial needles in the haystack. Similarly, specialized software is now readily available for procurement fraud investigation and to recover file fragments from personal computers.

The work product of the forensic accountant is also generated by computers and generally includes a written report accompanied by various supporting information—for example, document briefs, chronologies of events, accounting schedules (either summaries or analytical schedules), graphs and charts.

9.2.3 Analyzing and Testing

During the analysis stage, the financial issues being investigated are evaluated in detail. Appropriate conclusions are drawn, either in terms of a finding of fact (for example, whether a particular transaction or event took place) or the resulting quantification of the alleged fraud. If the investigation has been properly planned and appropriate evidence is available and has been gathered, this step should go fairly smoothly.

The ultimate test of the evidence may come when the perpetrator is confronted with it. A trained interviewer in possession of all the facts can often elicit an immediate confession from an unprepared suspect. In many cases, the suspect is relieved that the matter is finally over because he or she no longer has to endure the stress of covering up the fraud.

Of course, there are many cases that are not resolved as quickly, proceeding instead to lengthy civil or criminal court challenges. The planning, evidence gathering, and analyzing and testing phases of the investigation must yield a product that, in the end, can withstand the court challenges.

9.2.4 Reporting and Testifying

The forensic accountant must be able to present his or her findings in a way that is understandable, and must do so in an appropriate format. The *American Institute of CPA Practice Aids* should be referred to when preparing the final report. In general, however, the appropriate format might be one of the following:

- A reporting letter, for example, a communication to counsel outlining the scope of the review and findings.
- An affidavit or deposition, that is, a sworn statement of findings with supporting documentation.

- A formal communication to the court, such as a report that sets out the forensic accountant's opinions and underlying findings, and that provides details as to how those findings are substantiated.

Often the findings must be communicated through oral testimony in court. Once again, that is why every phase of the investigation up to this point must be conducted with the legal evidence standards in mind. Forensic accountants must be prepared for examination under oath about all their activities. This examination can come at any time and in any form, for example, as an affidavit, a deposition, or oral testimony at the actual trial. They must be able to qualify as an expert witness based on their education, experience and knowledge. Finally, they must be prepared to respond to cross-examination and to the submission of different financial evidence and alternatives by the other side.

Keep in mind that conventional accounting evidence is only one part of a much larger pool of evidentiary material, which includes one or more of the following:

- Testimony of witnesses.
- Police witness interview notes.
- Statements of claim.
- Statements of defense and counterclaim.
- Examinations or production of documents relating to a civil matter or search warrants.

Additionally, the forensic accountant may carry out research to identify any precedents that may assist in reporting and presenting evidence.

Preparing and Presenting Accounting Evidence

Certain guidelines should be considered when preparing and presenting accounting evidence. Although set out primarily from the point of view of the investigator or legal counsel, forensic accountants (especially those who act as expert witnesses) should also be aware of these guidelines, which include:

1. Make yourself fully aware of the evidence, or lack of it, from an accounting standpoint:
 - a. Be aware of the strengths and weaknesses of the case based on the available documents.
 - b. Be aware of any investigation that may be needed to complete the accounting picture.
2. Thoroughly familiarize yourself with the final *accounting picture* as set out in the accountant's report, schedules, and document brief.
3. Decide what accounting evidence to call, if any.
4. Prepare evidence for the court:
 - a. Request that the accountant prepare the appropriate report, schedules, and document brief.
 - b. Request that the accountant prepare appropriate visual or other aids.
 - c. Make available, as required by the rules of procedure, to the other side accounting material including the report, schedules, and document brief.

- d. Accomplish the following at the meeting with the other side.
 - Explain the accounting material.
 - Ensure that there is an opportunity for explanation and production of documents by the other side.
 - Consider the admissibility of accounting material without formal proof.
5. Conduct a final pretrial witness interview of the accountant:
 - a. Ensure that all documentation is introduced as exhibits.
 - b. Confirm that the accounting schedules are properly cross-referenced to the document brief.
 - c. Review the format of the examination of expert witnesses, including:
 - Areas to be covered.
 - Sequence of examination.
 - Exact nature of opinion evidence, if any.
 - Use of visual aids.
6. Make final preparations for tendering the accountant's evidence in court:
 - a. Place exhibits in proper numerical order.
 - b. Index the accountant's document brief with exhibit numbers.
 - c. Confirm the logistics of using visual aids.
 - d. Confirm the availability and legibility of copies of accounting schedules and visual aids.

Qualifying as an Expert Witness

The simulated testimony reproduced below shows how a CPA's qualifications as an expert witness can be established.

Examination—of Mr. I.M. Sleuth, CPA by Jim Jones, Esq. (Prosecutor)

Q. Mr. Sleuth, where do you reside, sir?

A. I live in Bigtown, Megaplace.

Q. And what is your occupation?

A. I am a CPA and a Certified Fraud Examiner.

Q. And do you practice on your own or with someone else?

A. I practice in partnership with other CPAs under the firm name of Sleuth & Company.

Q. And how long have you been operating the accounting partnership?

A. Close to twenty-two years now.

Q. And prior to that were you associated with any other firm?

A. Yes, prior to that I worked for a period of six years with a national firm following my graduation from school.

Q. And in what year did you qualify as a CPA?

A. In 1972.

Q. And since that date have you had occasion to testify in court with respect to accounting matters?

A. I have.

Q. And approximately how many occasions would that have occurred on?

A. An estimate of some fifty occasions.

Mr. Jones: Your Honor, I offer Mr. Sleuth as an expert witness on the basis of his qualifications that I have elicited.

Mr. Green (Defense Counsel): No objection, Your Honor.

His Honor: Thank you.

Q. Mr. Sleuth, I understand that you have prepared a number of documents relating to various transactions dealing with Acme Manufacturing?

A. Yes, I have.

Q. Mr. Sleuth, I show you a document, a rather large document, marked Exhibit A. I would ask you to look at that document and tell me if you recognize it?

A. Yes, I do.

Q. And did you prepare that document yourself?

A. Yes, I did, with the assistance of staff under my direct supervision.

Q. And I wonder if you would hold it in such a way that the jury will be able to see the structure of that document itself. It appears to consist of a number of columns, vertical columns, am I correct?

A. That's correct.

Q. And the document is headed what?

A. It's headed, *Analysis of Sales for the Period August 1, 1998 to October 5, 1998.*

Observing the Accountant Witness: A Positive Approach

The following list presents the ideal a CPA should, under the direction of legal counsel, strive for when giving oral testimony.

- The answers given should be responsive to the questions and as brief as possible, without losing sense.
- The statement of qualifications as an expert witness should be well outlined, factual, and not overly laudatory.
- There should be no show of bias when describing the scope and purpose of the services.
- The accountant should indicate the source of all documentation and acknowledge that all documents used to support his or her findings are currently before the court.
- The accountant should be prepared to consider new evidence provided it is relevant to the case.
- The accountant should be specific about the time period covered and the dollar amount of his or her findings.
- The accountant should be able to articulate the basis for his or her opinion in an organized and logical fashion that is easy for the judge (and if it is a jury case, a lay jury), to follow.
- The accountant should make good use of visual aids.
- The accountant should speak slowly and deliberately, leaving sufficient time for the judge (and jury) to absorb his or her evidence.
- The accountant should periodically check that the judge (and jury) is following his or her evidence.
- The accountant should direct his or her answers to the judge (and jury) rather than to the lawyer conducting the examination or cross-examination.
- The accountant should make a clear presentation.
- The accountant should be certain that the terms of the engagement are well organized and clearly set forth.
- The accountant should see to it that the accounting schedules are well referenced, including the visual aids, and can easily be tied to the supporting documents.
- The accountant should be calm and collected.
- The accountant should demonstrate knowledge of the documents and the case, and an understanding of the testimony of the other witnesses preceding him or her; that is, there should be a positive demonstration and total commitment and understanding of the matter before the court.

The Accountant Witness—A Negative Approach: What Not to Do

The following list presents the negatives an accountant can exhibit when giving testimony:

- Confusion.
- Lack of preparation.
- Self-described expert (that is, self importance: impressed with himself or herself and his or her credentials).
- The accountant demonstrates bias in the presentation and explanation of the scope and purpose of his or her services.
- Failure to present findings or conclusions.
- Lack ready notes in his or her file.
- Findings convey no definite time period.
- Findings convey no definite dollar amount.
- Poor visual image.
- Poor posture.
- Incomplete supporting documents.
- Argumentative and belligerent.
- Openly nervous.
- Off-hand answers to questions.

9.2.5 Case Resolution

Fraud is a crisis for an organization and its employees. Good crisis management demands that the investigative process not end with the reporting of findings or the giving of testimony. Briefly, this means the victim organization should—

1. Seek or enforce restitution from the perpetrator (for example, seize any assets pursuant to a court order).
2. Learn and adjust from the experience—in particular, ensure that controls are implemented to prevent a recurrence.
3. Keep channels of communication open between the crisis survivors—that is, the organization and its employees—to ensure the crisis does not damage their relationship or impair the organization's ability to function effectively and efficiently.
4. Implement regular, diligent monitoring and follow-up on the above points.

9.3 FORENSIC ACCOUNTANTS

Forensic accountants must possess a range of skills in order to carry out their investigations in a professional manner. These skills include not only thorough accounting knowledge but also knowledge of business and an awareness of the legal process. With these skills, the forensic accountant can investigate, analyze, document, report on, and testify as to the financial aspects of an investigation into a fraud or other so-called white-collar crimes.

In many instances, the forensic accountant may be requested to quantify the amount of a fraud loss in a criminal matter or the financial damages in a civil matter. While a criminal

matter must be proven beyond a reasonable doubt, a civil matter must be proven by a preponderance of the evidence. Both require a demonstration of similar techniques and skills from the forensic accountant.

9.3.1 Professional Skills and Attributes

The seven major categories of a forensic accountant's professional skills and attributes are:

1. Accounting and audit knowledge, including good business knowledge.
2. Fraud knowledge.
3. Law and rules of evidence knowledge.
4. Investigative mentality and critical skepticism.
5. Psychology and motivation awareness.
6. Communication skills.
7. Computers and information technology comprehension.

A closer inspection of each category follows.

Accounting and Audit Knowledge

Professional training in accounting and auditing provides not only accounting and audit knowledge but also a practical understanding of business operations, business finance, corporate structure, industry practices, and standards of conduct.

The majority of those who identify themselves as forensic accountants are CPAs. These individuals have sought and found careers for themselves in an area that allows them to use their skills as CPAs, together with other personal attributes that are necessary in investigating business fraud and commercial crimes.

Audit skills are an important foundation for a forensic accountant. Due to the sensitivity of the work involved, forensic accountants must be able to focus on the need for a 100 percent substantive examination of all documentation related to a particular matter.

The accountant with good audit skills must have the ability to prepare and use complete and accurate documentation; thus the accountant must know how to catalog the available information. He or she must also be able to determine the other existing information sources, which initially may not be available but which can, with research and diligence, be uncovered, obtained, and utilized. With his or her accounting and audit skills, the accountant can inquire about, locate and identify investigation-related documents—whether they are present initially or obtained during the course of the investigation.

For most CPAs, audit experience includes both audit and nonaudit engagements covering a wide cross-section of business enterprises and their operations, from small sole proprietorships to large multinational corporations, both public and private. This familiarity with business enterprise is an important element in the forensic accountant's investigation of business frauds and similar matters.

Fraud Knowledge

In addition to professional training in accounting and auditing, the most important aspect of the forensic accountant skills mix is exposure to and knowledge of many different kinds of

fraudulent transactions. This will allow the forensic accountant to identify red flags and to piece together patterns and theories that may otherwise elude an accountant who has not had the same degree of exposure to fraud.

Forensic accountants do not merely compute, they analyze. The analytical process is not an easy one, as each case is unique and therefore calls upon the forensic accountant's experience, formal training, and other important attributes. Specifically, he or she must be able to identify accounting problem areas, prioritize these problem areas or issues as required, and refine or change the focus of the investigation as new information is obtained and assessed. Often, an original theory may be only the beginning of an investigation, or it may be refined to a specific issue warranting further review. In providing assistance to the courts, this ability to properly focus the investigation is important.

The importance of experience cannot be overemphasized. The forensic accountant must also be able to look beyond the form of the documentation, to understand its substance and foundations, and to assess whether it is consistent with other business realities. The forensic accountant must understand the nature of the documents that he or she is reviewing and question their business reality. More than anything, a forensic accountant is distinguished by having "been there before." Knowledge of many different kinds of fraud, based on first-hand investigative experience, means a more effective plan of investigation, knowing when, how, and who to interview as well as the format for communicating findings in reports to clients and if necessary to the court.

Law and Rules of Evidence Knowledge

It is important for the forensic accountant to be knowledgeable about both criminal and civil laws, since these laws have a direct impact on matters involving the forensic accountant. Specifically, a forensic accountant must be able to understand both criminal and other statutes that may have been contravened, in order to identify possible issues. There is also a need to understand the rules of evidence to ensure that all findings are admissible in court, if necessary. Specifically, investigative accountants must have an understanding of the rules of evidence—for both civil and criminal matters—which consist of:

- What evidence is.
- How it is obtained.
- How it is preserved.
- How it is presented before the courts.
- How the forensic accountant's own work can become part of the evidence brought before the courts or before some other tribunal responsible for determining what has occurred.

To provide accounting assistance in a matter involving fraud, the forensic accountant must possess a general understanding of the issues by which the courts can judge an act to be fraudulent. He or she must be knowledgeable as to the court's tests for fraud—for example, the presence of dishonest intent as seen in the perpetrator's actions, or more particularly, the *mens rea* or criminal intent of the perpetrator at the time the act occurred. He or she must review and analyze accounting, banking, financial and other business records, and

identify both specific acts and patterns of conduct that are suggestive of dishonest intent to deprive a victim of an asset.

Investigative Mentality and Critical Skepticism

The forensic accountant must possess an investigative outlook, tenacity, and the ability to identify indicators of fraud. Collectively, these attributes could be termed as the investigative mentality. This mentality encourages the forensic accountant to seek substance over form—to identify and analyze data and to conduct interviews to determine what has actually occurred in a business transaction, rather than what simply appears to have happened.

The investigative mentality is sometimes manifested by the *smell* test—the ability to assess relevant transactions or events to determine their reasonableness and to the extent possible, their veracity. In other words, in light of all the known facts, does a particular action appear reasonable and logical? Is the action or pattern of behavior plausible in the circumstances, or is there an *odor* that begs for further investigation?

The investigative mentality can also be thought of as professional, critical skepticism. It is not a shotgun approach; rather, it is a specific and precise set of judgmental procedures suitable for the circumstances that allows the forensic accountant to identify and assess all relevant facts and develop hypotheses. These hypotheses can then be researched further and tested more extensively as the investigation proceeds. The forensic accountant never discounts any aspect of an investigation on face value: Only after examining all available evidence and weighing its totality will he or she determine an item to be irrelevant to the issues at hand.

Another analogy—that of the watchdog-bloodhound—further illustrates the forensic accountant’s investigative mentality attribute. A CPA is more akin to a watchdog—he or she looks for material misstatements in financial statements caused by error or fraud, but will respond affirmatively if warning signs of fraud appear through audit procedures. The forensic accountant, however, is more of a bloodhound—actively seeking out the presence of evidence, all of which when viewed together may indicate the occurrence of a fraudulent act.

While the investigative mentality requires a disciplined approach and a methodology, it also requires creativity in being able to identify and seek out further sources of evidence and to analyze this new information. Attention to detail is critical as the success or failure of the case may depend on the identification of evidence that, on initial review, may appear insignificant or irrelevant. The issues of materiality or sampling relevant in an audit assignment do not restrict a forensic investigation. Those restrictions may cause fraudulent acts to be overlooked, and they are inadequate in establishing evidence.

Psychology and Motivation Awareness

Another attribute of the forensic accountant is an understanding of the human element. Documents do not commit fraud; computers do not commit fraud; rather, people commit fraud. In assessing information, documentation and accounting records, one of the seasonings that the forensic accountant can apply to the mix is his or her understanding of individuals, including what motivates an individual to commit fraud and the attributes of an individual who commits fraud. This understanding, together with the ability of the forensic

accountant to examine information not just from an accounting viewpoint, but also within the context of the overall picture or business reality, is important.

In general, it can be said that individuals react to satisfy needs. The forensic accountant must recognize the presence of such needs during his or her investigation, whether it is the need of an employee for greater income to maintain an extravagant lifestyle or the need of a sales manager to maintain sales volumes in a declining market so as to ensure his or her continued employment. Such needs often provide the motivation for acts that an employee may label differently but which are, in essence, fraud.

In a situation where an individual has both the need and the opportunity, a fraudulent act may be the result.

Communication Skills

Forensic accountants, as expert witnesses to the court in findings of fact, must be able to clearly and effectively communicate information. This means that they must be able to communicate without bias in written form, including the use of accounting schedules, charts, and exhibits. They must also be able to communicate to others the nature and extent of the work undertaken and the findings that have evolved from that work so that it can be understood both in a court of law and in other forums.

When the forensic accountant testifies as an expert witness in court, he or she must be able to explain the procedures, analyses, and findings of the investigation in such a way that the basis for his or her expert testimony—both facts and, if necessary, opinion—is understood by the judge and, if there is one, the jury. The forensic accountant's knowledge of the available evidence and possible alternate explanations of the events must be as complete as possible, to ensure that the findings are not compromised on cross-examination.

Understanding Computers and Information Technology

Today's computers have replaced yesterday's ledgers, and in fraud investigation it is important to be as up-to-date as the alleged perpetrators of fraud. Thus, the skills of a forensic accountant should include the ability to understand the opportunities computers provide to potential perpetrators of fraud as well as the ability to use computers in analysis and documentation of an alleged fraud.

Because succinct presentation to the judge and jury is so critical, knowledge of computer graphics is also helpful. The forensic accountant's findings often include quantitative analyses that are conducive to presentation in the form of graphs and charts that depict and summarize the information. Typical graphs and charts include summaries of the source and use of funds, as well as flow charts showing the movement of assets at various times.

9.3.2 Ethics

Independence and Objectivity

Independence and objectivity are integral concepts in the ethical training of CPAs. While the need for these attributes is well established in the audit area, they are extremely important in investigative work. The forensic and investigative accountant is not an advocate; rather, he or she provides the skills and input of an independent expert. Even a bias with respect to a single, small matter—whether actual or perceived—may call into

question in the eyes of the court other unbiased evidence presented by the forensic accountant. He or she must therefore report objectively at all times.

Respect for Access to Information and Privacy Laws

One factor that must not be overlooked in the role of investigator is that the information that is gathered must be collected in an ethical and legal manner. One cannot misrepresent one's self when gathering information, nor can the process of collecting information be abused.

Most important, the rights of an individual whose activities are being reviewed must not be abused.

9.3.3 Kinds of Services Offered

Proactive versus Reactive Services

Forensic accounting services can be proactive or reactive. Proactive services include training on fraud awareness and fraud prevention measures, presented elsewhere in this Handbook. Reactive services are investigative and analytical in nature and are rendered after the event. Much of the information in this chapter addresses reactive services.

Civil versus Criminal Services

Another way to identify the kinds of services that a forensic accountant renders is to consider the forum in which a dispute is finally resolved. For example:

- A criminal forum must establish guilt beyond a reasonable doubt.
- A civil case has a less onerous burden of proof than a criminal case. The trier of the facts must reach his or her conclusion based on the preponderance of the evidence.
- A nonjudicial tribunal, for instance, an alternative dispute resolution proceeding (arbitration) can differ from a court of law by being either stricter or more lenient.
- Finally, if the circumstances are such that no reference is made to an outside tribunal, but rather two parties are to resolve a matter on their own, then the level of proof required is only what the other side will accept.

Other Categorizations

Services of a forensic accountant can also be categorized in other ways, for example by the type of procedures performed. These procedures can include—

- Performing an initial review of documentation to determine whether further research or investigation is required or necessary.
- Providing an affidavit or deposition outlining the results of a review of documentation.
- Providing a report identifying the scope of the work performed and findings.
- Assisting counsel in obtaining a search warrant (that is, in a criminal case).
- Providing expert testimony in court.

The nature of the industry in which a forensic accountant is performing an investigation can be another method of classification. For example:

- Service industries could include transportation, banking, securities brokerage, retail, real estate, construction, professional services (such as services of CPAs and lawyers), mortgage brokerage, and telecommunications.
- Manufacturing industries could include construction, farming, food processing, all forms of manufacturing, mining, petroleum, and publishing.

The above classifications could then be further refined, and others added. For example, government and nonprofit sectors are other areas where forensic accountants are called upon to provide their services.

9.4 CHECKLIST: DEALING WITH A KNOWN OR SUSPECTED FRAUD

CPAs can use the following checklist when dealing with a known or suspected fraud in their organizations or in those of their clients. *No* answers may require investigation and follow-up, the results of which should be documented. Use the *Ref* column to cross-reference the checklist to the appropriate work papers.

The checklist is intended for general guidance and information only. If fraud is of vital concern to an organization or if serious fraud is suspected, seek the advice of legal counsel and a CPA experienced in fraud investigation.

TABLE 9.1 DEALING WITH A KNOWN OR SUSPECTED FRAUD CHECKLIST

| Dealing With a Known or Suspected Fraud Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| 1. Planning | | | | |
| a. Has the main scenario of the fraud been established, including the sources of information pointing to fraud (that is, accounting irregularities, physical evidence, or incriminating information)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | --- |
| b. Have immediate areas of concern been identified, such as the need to protect assets from further damage (for example, by boosting security) and to preserve key evidence for further investigation (e.g., by removing the key suspect from the scene, through a leave of absence or other appropriate means)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | --- |
| c. Have legal and other constraints been identified, (that is, the provisions of any collective bargaining agreement) and has legal counsel been consulted? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | --- |
| d. Has a preliminary assessment been made to determine: | | | | |
| • The quality of the information currently available | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | --- |
| • Additional information that is needed | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | --- |
| • How to obtain the information | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | --- |
| e. Have the nature and scope of the investigation been defined, including: | | | | |

TABLE 9.1 (continued)

| Dealing With a Known or Suspected Fraud Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| <ul style="list-style-type: none"> ● The main objective(s) ● Whether (and when) to pursue criminal charges ● The level of secrecy required ● Administrative matters (for example, engagement letters; or if external forensic accountants are used, budgets) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. Evidence Gathering | | | | |
| a. Has a detailed list been prepared of the evidence that is to be obtained or seized? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Have all sources of evidence been considered (for example, books and records, documents, correspondence, public domain information, background financial information and personnel history, etc.)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. When evidence is obtained, is it assessed for: | | | | |
| ● Relevance | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Alternative interpretations (for example, simple error) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Eventual use and admissibility (for example, as court evidence) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Are proper evidence-handling procedures in effect, (for example, taking photocopies; not writing on, altering, stapling or unstapling originals)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Especially for larger investigations, has evidence been categorized in a way that will facilitate its future retrieval and use? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. Has the nature, timing and scope of any interviews (especially of suspects) been carefully considered? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| g. Are interviews conducted by or with trained and experienced interviewers, with appropriate safeguards to prevent bogus harassment or other charges (for example, safeguards could include leaving the door ajar during interviews and having assistants interrupt at predetermined times)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| h. When appropriate, has the use of reputable private investigators been considered? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| i. For any evidence to be seized, does the search warrant or court order have the proper scope so that all of the required evidence falls within its reach? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 9.1 (continued)

| Dealing With a Known or Suspected Fraud Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| j. Especially for larger investigations, have computer databases and other appropriate tools been used to store and cross-reference evidentiary materials? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| k. Has security over all evidence been established, including, if appropriate, off-site storage of copies (electronic, paper, or both) for key evidence and documents? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Analyzing and Testing | | | | |
| a. Has all evidence been systematically analyzed? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Were appropriate conclusions drawn? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Has the evidence been thoroughly checked and tested and reviewed with legal counsel to ensure it is up to court standards? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 4. Reporting and Testifying | | | | |
| a. Has a forensic accountant prepared a well-organized, unambiguous report, summarizing the findings of the investigation? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Has the report undergone a quality-control review? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Has adequate preparation been done for testifying in court, including a full run-through? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Is the person giving the testimony experienced, and if necessary, has he or she previously qualified as an expert? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. For expert witnesses, have fairness and impartiality, and the appearance of such, been present throughout the process (for example availability to both sides)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 5. Case Resolution | | | | |
| a. Has a plan and process been put into effect to seek and enforce restitution from perpetrators? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Have controls and procedures been put into place to prevent a recurrence? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Have channels of communication been kept open and other appropriate steps taken to maintain good employee relations and mitigate any other adverse effects of the crisis? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Has a program been established to monitor the results of the above on an ongoing basis? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

CHAPTER 10:

Reducing the Risk of Financial Statement Fraud

| | | |
|--------|--|----|
| 10.1 | The Pervasive Nature of Financial Statement Fraud..... | 3 |
| 10.1.1 | Introduction | 3 |
| 10.1.2 | Overview | 3 |
| 10.1.3 | What Constitutes Financial Statement Fraud?..... | 3 |
| 10.1.4 | SEC Definition of Fraud | 4 |
| 10.1.5 | Common Methods of Committing Financial Statement Fraud | 5 |
| 10.2 | Kinds of and Motives for Financial Statement Fraud | 5 |
| 10.2.1 | Earnings Manipulation..... | 5 |
| 10.2.2 | Earnings Management | 6 |
| 10.2.3 | Balance-Sheet Manipulation..... | 12 |
| 10.2.4 | Falsification of the Income Statement | 13 |
| 10.2.5 | Reducing the Risk of Fraud in Closely Held Companies..... | 23 |
| 10.3 | Special Areas of Financial Statement Fraud | 25 |
| 10.3.1 | Failure to Record Loss Contingencies and Asset Writeoffs | 26 |
| 10.3.2 | Manipulation of Acquisition Reserves..... | 33 |
| 10.3.3 | Cost Shifting to Improve Current Operating Results | 37 |
| 10.3.4 | Recognizing Fictitious Revenues | 39 |
| 10.3.5 | Improper Disclosures and Material Omissions | 50 |
| 10.3.6 | Special Purpose Entities: The Enron Case..... | 51 |
| 10.3.7 | Methods to Conceal Financial Statement Fraud From Auditors | 55 |
| 10.4 | Predictors of Financial Statement Fraud | 56 |
| 10.4.1 | Quantitative Predictors | 57 |
| 10.4.2 | Qualitative Predictors..... | 59 |
| 10.4.3 | A New Fraud Profile (1997–2002)?..... | 62 |
| 10.5 | Regulatory Responses to Financial Statement Fraud | 64 |
| 10.5.1 | Public Company Accounting Oversight Board..... | 64 |

| | | |
|--------|--|-----|
| 10.5.2 | SEC Initiatives and Staff Accounting Bulletins (SABs)..... | 65 |
| 10.5.3 | New Statements on Auditing Standards..... | 70 |
| 10.5.4 | The Paradigm: COSO's <i>Internal Control—Integrated Framework</i> | 73 |
| 10.5.5 | Preventive and Detective Controls Under Sarbanes-Oxley..... | 78 |
| 10.5.6 | Enforcement of Section 10A of the Securities Exchange Act of 1934..... | 81 |
| 10.6 | Audit Deficiencies and Audit Failures..... | 83 |
| 10.6.1 | The Top 10 Audit Deficiencies (1987–1997)..... | 83 |
| 10.6.2 | Audit Failures (1997–2002)..... | 84 |
| 10.6.3 | Lessons Learned..... | 86 |
| 10.7 | Guidance for Auditors..... | 86 |
| 10.7.1 | Risk Assessment..... | 87 |
| 10.7.2 | Analytical Procedures..... | 87 |
| 10.7.3 | Targeted Substantive Testing..... | 88 |
| 10.7.4 | Scope Limitations and Qualified Audit Opinions..... | 88 |
| 10.7.5 | Typical Frauds Related to Misappropriation of Assets, Example Audit Procedures, and Internal Control Questions..... | 89 |
| 10.8 | Checklist: Detection of Financial Statement Fraud..... | 107 |
| 10.9 | Checklist: Sarbanes-Oxley..... | 119 |

CHAPTER 10:

Reducing the Risk of Financial Statement Fraud

10.1 THE PERVASIVE NATURE OF FINANCIAL STATEMENT FRAUD

10.1.1 Introduction

Allegations of financial statement fraud have dominated the headlines early in the new millennium. Once prominent companies such as Enron, Xerox, Rite Aid, Adelphia, Tyco, and WorldCom now symbolize corporate disgrace. The Securities and Exchange Commission (SEC), federal law enforcement agencies and Congress have been investigating financial statement fraud throughout corporate America. Fear that financial statements might be concealing rather than revealing information has driven frightened investors from the public marketplace. In this atmosphere, it is more important than ever for financial professionals to understand financial statement fraud and how it might be used to deceive boards of directors, senior management, auditors, and investors alike.

10.1.2 Overview

Financial statement fraud involves the alteration of financial statement data, usually by a firm's management, to achieve a fraudulent result. These altered financial statements are the tools then used by a company's managers to obtain some reward. The reward may consist of direct compensation such as receiving a bonus that otherwise would not be paid without using altered, incorrect financial data to embellish management's operating performance. On the other hand, the compensation may be direct in that managers avoid being fired for failing to achieve promised results. Compensation may also be indirect; for example, management may use fraudulent financial statements to raise additional capital that in turn allows a firm to expand and presumably enhance the value of shares held by management.

10.1.3 What Constitutes Financial Statement Fraud?

What constitutes financial statement fraud has been the subject of much debate because the line between fraud and discretion is not always clear. It is easy to define fraud as a conscious effort by management to produce financial statements with materially wrong account data. It is almost as easy to identify as fraud misleading accounting entries that management cannot justify under any applicable accounting standards. Fraudulent acts become less obvious, however, when cloaked in the mantle of accounting standards that are incorrectly applied. For example, the applicable accounting standard in the United States is generally accepted accounting principles (GAAP), principles that may allow management some discretion as to when to recognize revenue or expenses.

Honorable people can debate the most appropriate use of a principle when looking at the gray or more broadly permissive areas of GAAP. Less-than-honorable people, however, might make use of these gray areas to produce financial statements that mislead. This

practice is found most often in concert with other misleading applications of GAAP. Fraudsters almost always fail to discuss this choice of GAAP principles in the notes to financial statements.¹ Without knowledge of the impact of GAAP gray-area judgments on the financial statements, unsuspecting readers may mistakenly assume that revenues and expenses were accrued in a manner consistent with prior financial statements when, in fact, they were not. The end result may be that continuing operations appear to be profitable while, in reality, there may be serious problems that the misuse of GAAP gray areas can cover up for a short period of time. Thus, when accounting decisions purportedly in conformity with GAAP produce financial statements intentionally² designed to mislead the reader, those decisions cross the line into fraud.

10.1.4 SEC Definition of Fraud

These concepts are codified in the United States securities laws, especially SEC Rule 10b-5³, which states the following:

It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or the mails, or of any facility of any national securities exchange,

- (a) to employ any device, scheme, or artifice to defraud,
- (b) to make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
- (c) to engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.

Publicly traded companies must conform to GAAP and to the rules and regulations promulgated by the SEC under United States securities laws. The SEC drew heavily on accounting literature when it recently addressed the issue of accounting gray areas. SEC standards (discussed below) that have their origin in GAAP will provide substantial guidance to determine financial statement fraud not only for publicly traded companies but also for all firms issuing financial statements in conformity with GAAP.

¹ In this chapter, the term *company* refers to any legal or business entity that prepares financial statements, including partnerships, limited liability companies, and corporations.

² Failure to disclose is probably a GAAP violation; therefore, while the accounting for a certain transaction may appear to be supported by GAAP, failure to disclose so as not to make the financial statements misleading takes the company out of GAAP compliance. As with proving any type of fraud, one must show that the fraudster was *scienter* or knowingly aware that his or her actions were designed to mislead.

³ Promulgated under Section 10(b) of the Securities Exchange Act of 1934.

10.1.5 Common Methods of Committing Financial Statement Fraud

Research carried out for the Committee of Sponsoring Organizations of the Treadway Commission⁴ (the *COSO Report*), a voluntary private sector organization dedicated to improving the quality of financial reporting, found the most common kinds of fraud were:

1. Overstatement of earnings
2. Fictitious earnings
3. Understatement of expenses
4. Overstatement of assets
5. Understatement of allowances for receivables
6. Overstatement of the value of inventories by not writing down the value of obsolete goods
7. Overstatement of property values and creation of fictitious assets

The following sections will discuss the various kinds of financial statement fraud and the corresponding motives for each kind, the early indicators of financial statement fraud (both quantitative and qualitative) and the means to detect some of the most difficult-to-find kinds of fraud. At the end of this chapter, there is a checklist that addresses internal control issues designed to provide early detection of financial statement fraud.

10.2 KINDS OF AND MOTIVES FOR FINANCIAL STATEMENT FRAUD

We will approach financial statement fraud looking at three broad areas:

1. Earnings manipulation
2. Earnings management
3. Balance-sheet manipulation

Financial statement fraud generally falls into one or more of the above categories.

10.2.1 Earnings Manipulation

Earnings manipulation is the direct alteration of accounting data for the purpose of fraudulently changing reported net income. For example, booking a sale that clearly does not meet the requirements for revenue recognition increases revenues. Conversely, capitalizing marketing costs as an asset, contrary to guidance in GAAP, decreases current-period expenses. Notice also that both examples affect the balance sheet as well: Recognizing fictitious sales probably inflates accounts receivable; deferring marketing expenses creates some type of amortizable asset. Since the primary intent of these manipulations is, however, to increase earnings rather than create assets, these practices are classified as “Earnings Manipulation.”

⁴ Mark S. Beasley, Joseph V. Carcello, and Dana R. Hermanson. *Fraudulent Financial Reporting 1987–1997: An Analysis of U.S. Public Companies*. COSO, 1999. See also *Top 10 Audit Deficiencies*, Beasley, Carcello, and Hermanson. *Journal of Accountancy*, April 2001.

Motives for Earnings Manipulation

The motives for earnings manipulation usually stem from the need to report higher net income. Management compensation agreements, for instance, may require the achievement of some absolute level of net income or an increase in net income over some benchmark in order to trigger bonus payments. Pressure to increase “shareholder value” may provide another motive to create earnings increases. Because stocks are valued at some multiple of price to earnings, an increase in earnings usually increases share price even if the multiple stays constant. When earnings are growing rapidly, the multiple is more likely to expand.

Earnings manipulation may also help support the share price of a publicly traded company while management and insiders sell their holdings. Such a reprieve may be important if time restrictions prevented the granting or sale of those shares at an earlier date. Examples of stock granting or sale restrictions include:

1. Vesting provisions in employee stock ownership plans that postpone ownership
2. Stock option exercise restrictions that prevent managers from acquiring shares until specified dates or the occurrence of specific events
3. SEC Rule 144A restrictions that limit the number of shares that can be sold on United States securities exchanges on a given trading day
4. Income tax provisions that afford more favorable treatment to capital gains in shares held for a sufficient period of time to qualify as long-term capital gains (the restriction being that the government would receive more of the sale proceeds if the share sales were classified as short-term capital gains)
5. Corporate control requirements that necessitate holding significant blocks of stock past some event such as an annual shareholders meeting before they can be sold

Finally, earnings manipulation may help a company obtain or retain its listing on a stock exchange. The initial and continued listing requirements of many exchanges provide for some type of net income test. Although companies failing this test may qualify for initial or continued listing under other tests such as overall market capitalization, companies whose share prices have declined sharply in a weak market may find net income manipulation to be their only hope. Losing an exchange listing may relegate the company to the over-the-counter market where there are no requirements for the presence of a minimum number of market makers, that is, the securities firms that stand ready to buy or sell shares to maintain an orderly market in the company's stock. Without a minimum number of market makers, investors face the prospect of greatly reduced liquidity. A shareholder wishing to sell his shares risks having to wait a long time for a buyer to come into the market. Therefore, a listing on a recognized exchange that mandates a minimum number of market makers is an important benefit to a publicly traded company, a benefit that unscrupulous management may implement earnings manipulation to retain.

10.2.2 Earnings Management

A subtler variant of earnings manipulation is earnings management. Although both involve the orchestration of accounting data, the latter attempts to exploit the interpretive opportunities inherent in GAAP to produce reported earnings that conform to outside expectations. Earnings management stops just short of outright fraud while earnings manipulation crosses the line.

Corporate managements are under more pressure today than ever before to increase “shareholder value,” that is, the price of the stock. Superstar analysts raise performance expectations by generating earnings estimates that strongly influence stock prices. Management may believe that if the company does not “massage” the numbers to meet analysts’ expectations, the stock price may decline and decline precipitously if analysts feel compelled to scale back their growth estimates.

In this environment, the moral issue of reporting earnings that truly measure the company’s economic activity is a matter of management intent. The very nature of accrual accounting leaves open the possibility that management judgment, even within GAAP, may be colored by the intent to show the company in the best possible light. Accrual, deferral, and allocation procedures designed to permit the relation of revenues and expenses, and gains and losses across periods, also allow management considerable leeway as to when to declare any monies are earned. When within this process does discretion become the intent to deceive? Within what limits should management be acting to permit investors to price the company’s securities in the market? How much earnings “smoothing” actually misrepresents the trend of economic performance as opposed to the irregularities of cash flows? Earnings management is fraudulent when it uses improper accounting to hide true company performance. Arthur Levitt, chairman of the SEC, expressed the Commission’s concern about this subject in a speech given in 1998:

Flexibility in accounting allows it to keep pace with business innovations. Abuses such as earnings management occur when people exploit this pliancy. Trickery is employed to obscure actual financial volatility. This, in turn, masks the true consequences of management’s decisions.⁵

He expressed his concern about where this could lead:

As a result, I fear that we are witnessing an erosion in the quality of earnings, and therefore, the quality of financial reporting. Managing may be giving way to manipulation; integrity may be losing out to illusion.

In Staff Accounting Bulletin (SAB) No. 99, *Materiality*⁶ the SEC reviewed the United States accounting literature and presented the staff’s findings on earnings management.

Failure to Perform Punishes the Stock Price

Within this range of discretion, managements of publicly traded companies, especially growth and high-tech companies, have been under tremendous pressure to perform, from both analysts and investors. Failure to report continued profit growth can result in dramatic punishment to the stock price even when the shortfall is by only a few cents per share. Even performances that are good by historical standards can cause a price decline when they are below analysts’ expectations. This kind of market reaction has been an incentive for companies that are just meeting analysts’ forecasts or even falling slightly below to show a modest increase in reported profit.

⁵ Arthur Levitt, “The ‘Numbers Game,’” a speech presented to the New York University Center for Law and Business, Sept. 28, 1998. Available at <http://www.sec.gov/news/speech/speecharchive/1998/spch220.txt>.

⁶ SAB No. 99, *Materiality*, is available at <http://www.sec.gov/interp/account/sab99.htm>

Companies reporting consistently rising earnings are rewarded with high price/earnings (P/E) multiples. As the chain of good quarters extends, the multiple tends to increase and vice versa. P/E multiples are effectively inverted capitalization rates that have built-in assumptions for future discount rates applied to expected future cash flows. If earnings grow steadily from period to period, analysts are better able to predict future earnings. The market tends to reward a company having such a record with a lower discount rate that reflects a lower level of uncertainty about future earnings. This lower discount rate then increases the present value of future earnings and thus makes the stock or claim on those earnings more valuable.

Managements Regularly Meet Analysts' Forecasts

Recent academic studies have shown the regularity with which managements meet analysts' forecasts quarter after quarter and the small number of shortfalls. Managements themselves can influence analysts' estimates through meetings and other contacts with the result that the whole earnings estimation process seems to be manipulated. It has also been observed that analysts with underwriting houses tend to make higher growth forecasts than independent analysts.

It is hard to resist the conclusion that managements are often driven to rework the earnings components. Their bonuses are tied to operational performance and their stock options are tied to stock price performance. In addition, their overall performance will determine accessibility of capital for their companies. A good earnings report can improve the terms of a security offering to the benefit of both the firm and its management. The fact that shares of firms making seasoned equity offerings underperform during the years immediately following the offering suggests that accruals were maximized in the year of the offering and earnings were allowed to deteriorate immediately thereafter.

Discovery of earnings manipulation can lead to the dismissal of senior executives, lawsuits by shareholders, and sharp declines in the price of the company's stock. There is also a decline in the number of analysts following the company and an increase in the number of short sellers.⁷

Four Main Kinds of Earnings Management

SEC Chairman Levitt focused on four main fraudulent practices used to enhance earnings:

1. "Big-Bath" restructuring charges
2. Writeoffs
3. "Cookie-Jar" reserves
4. Materiality

⁷ For an excellent survey, discussion, and bibliography of the academic and practitioner literature on this broad topic, see Patricia M. Dechow and Douglas J. Skinner, "Earnings Management: Reconciling the Views of Accounting Academics, Practitioners and Regulators," *Accounting Horizons*, June 2000, pages 235–250.

Big-Bath Restructuring Charges

These are large one-time charges associated with a restructuring. Management may take a big-bath charge on the assumption that the company stock price will get pummeled whether the restructuring charge is large or small. Using that logic (which may actually be correct), management opts for the big charge by establishing large reserves for shutting down operations or shifting operations to other areas. If the reserve estimates are too big and actual expenses do not consume all the reserves, management can later reverse the unused portion back into income. As an added bonus, the reversal back to income may occur at a time when earnings need a boost because of disappointing current operating results. Hence, Chairman Levitt observed that overestimation can leave charges that are “miraculously reborn as income when estimates change or future earnings fall short.”

Sunbeam Case Study

At the end of fiscal 1996, the Sunbeam Corporation took a \$338 million restructuring charge that included various operating costs actually chargeable to future periods. In October 1998, the SEC required Sunbeam to reduce the restructuring charge to \$239 million. As a result, the company’s 1996 earnings were restated upward, while its 1997 earnings were restated downward by 65 percent to \$38 million from \$109. New management who had joined the company in 1996 took the big-bath restructuring charge to create the appearance of a turnaround. When the big-bath charges had been washed out, however, the so-called turnaround was largely nonexistent.

In May 2001, the SEC brought fraud charges against five former executive officers of Sunbeam as well as Sunbeam’s former engagement partner.

Writeoffs

After one company acquires another, research and development (R&D) work performed in one or both of the companies may be redundant because of a change in corporate direction under the new management. For that reason, companies may write off some in-process R&D projects that have yet to be expensed because they do not fit into the new corporate plans. Some companies, however, have taken advantage of the opportunity to write off substantial amounts of in-process R&D, by applying a principle similar to the big-bath restructuring charge. Management believes that the company can take a large, one-time hit to earnings without further hurting its stock price when the financial community is already expecting some writeoffs because of the acquisition. By taking the writeoff at the time of the acquisition, these R&D expenses will not weigh on future earnings.

MCI WorldCom Case Study

In August 1998, WorldCom disclosed an expected in-process R&D charge of \$7 billion in connection with its acquisition of MCI. In September 1998, after the transaction closed and following discussions with the SEC, the charge was reduced to \$3.1 billion. When such charges were no longer available, WorldCom used reserves in 1999–2000 and the improper capitalization of current period expenses in 2001–2002, to manage its reported financial results.

3Com Acquisition of US Robotics Case Study

During the first quarter of fiscal 1998, 3Com recorded an accounting combination and merger restructuring charge of \$426 million for the June 1997 merger of 3Com and U.S. Robotics. Shortly thereafter, the SEC required 3Com to reduce the charge to \$270 million. In its Form 8-K disclosing the reduction, 3Com indicated that the adjustments were intended to reflect three factors: a change in the timing and costs associated with product swaps, a more accurate reporting of costs associated with the elimination of duplicate facilities, and a revision of goodwill writeoffs relating to premerger acquisitions. These changes were made in deference to the SEC's position that the cost of replacing discontinued products should be reflected not at the time of the merger but at the time the cost is actually incurred.

Cookie-Jar Reserves

Fraudulent managers like to cloak their deception in an accounting rule, although in reality the accounting rule is not properly applied or other accounting rules are broken. The use of loss reserves is a good example of the abuse of a GAAP principle in order to manage the final earnings figure.

Cookie-jar reserves are reserves set aside during periods of strong financial performance and used to increase earnings or make up revenue shortfalls in periods of weak financial performance. They may take a variety of forms such as sales returns, loan losses, warranty costs, tax cushions, or inventory adjustments.

When financial performance is strong, earnings may be reduced by overstating reserves, overaccruing expenses, or taking excessive one-time writeoffs. In later periods of weak financial performance, reversing the accruals and reserves to reduce current-period expenses increases earnings. In a calendar quarter in which a company expects to outperform market expectations, it might create a reserve for future losses on such items as long-term contracts to create the effect of lowering earnings closer to the market consensus forecast. Then, in a future quarter, after the company has predicted that it will not make enough income to meet market expectations, management can reverse out some of the reserves on the grounds that future contract losses no longer appear probable.

On the surface and viewed in isolation, the creation and reversal of the loss reserves may appear unrelated to earnings expectations. GAAP provides for the booking of loss contingencies in Financial Accounting Standards Board (FASB) Statement of Financial Accounting Standards No. 5, *Accounting for Contingencies*, if the loss contingencies are both quantifiable and probable. In reality, however, the possibility of losses on future contracts most likely existed prior to the establishment of the reserve and continued to exist after the reserve was reversed into income. The reserves then become an accounting artifice used by management to manage earnings to meet market expectations. Moreover, management violated GAAP, in this example, either by creating the reserve without justification or reversing the reserve without any change in the degree of likelihood that the loss would in fact occur. Such reserves are known as cookie-jar reserves because management can reach into the cookie jar and pull them into income whenever the need arises.

W.R. Grace Case Study

In June 1999, the SEC accused W. R. Grace of manipulating the reported earnings of its primary health care subsidiary National Medical Care, Inc. Management had established reserves for unanticipated health care reimbursements and used them in subsequent periods to reduce expenses and show a steady growth rate in its health care subsidiary. But, contrary to GAAP, there were no liabilities to justify the reserves. When the SEC uncovered the scheme, the agency sued the company, its management, and auditors. The Commission also required Grace to establish a \$1-million education fund for earnings management training.

Materiality

Underlying the discussion of financial statement fraud to this point is the assumption that the accounting manipulations cited are all material in that the manipulations significantly change the information presented in the financial statements. Much of the accounting literature contains provisions that except immaterial amounts from a given accounting standard. However, the evolution of the definition of materiality has introduced another element of judgment into determining whether or not there is fraud.

Fortunately, the SEC decided to weigh in on this matter when it issued SAB No. 99, which helped clarify some of the key materiality concepts. One of the issues addressed head-on by the SEC was the use of quantitative materiality to waive accounting violations. A blind application of quantitative materiality essentially looks at the monetary amount of an accounting entry (or series of entries) that was indefensibly improper. If the amount was less than some arbitrary standard such as five percent of net income, neither management nor company auditors would insist on changing that entry even though it blatantly violated accounting standards. The SEC said that although quantitative standards may serve as a starting point for investigating potential accounting irregularities, relying exclusively on an arbitrary percentage to avoid application of appropriate accounting standards has no basis in accounting literature (or in U.S. securities laws).

The FASB in 1980 issued Statement of Financial Accounting Concepts No. 2, *Qualitative Characteristics of Accounting Information*, which addressed materiality as follows:

The omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.

In other words, materiality is viewed from the standpoint of the reader of financial statements. If the correction of an erroneous accounting item would probably cause the reader to come to a conclusion different from the conclusion reached upon reading the uncorrected statement, then the item is material. Prior to the release of FASB Concepts Statement No. 2, the United States Supreme Court, in reviewing a securities case involving materiality issues, ruled that a fact is material if there is "a substantial likelihood that the . . . fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."⁸ Therefore, both accounting literature and the Supreme Court look to the reader or user of the financial statements and ask whether it is probable or substantially likely that the reader would have come to a different conclusion. If the answer is yes, then the item in question is material.

ABS Industries Case Study

In October 1999, the SEC brought an action against ABS and four of its former officers and employees for engaging in a scheme to manage earnings. ABS' financial results overstated sales by 3.21 percent and overstated income before taxes by 2.48 percent. The SEC determined that although these amounts were not quantitatively material, they were, however, qualitatively material given management's intent.

10.2.3 Balance-Sheet Manipulation

In addition to the creation of fictitious accounts receivable and improperly capitalized expenses as discussed above, management can also manipulate assets. By recording as purchases certain transactions for which title has not passed, by using improperly extended depreciation of useful lives, and by failing to write down or write off useless assets, the value of a company can be misrepresented. Management may inflate inventory by failing to bring the correct amount into the cost of sales, a practice that has the added fraudulent benefit of inflating gross profit and earnings as well. Finally, management may manipulate capitalized acquisition costs through improper purchase price accounting.

Management manipulates liabilities by failing to record amounts owed to others or by keeping debts off the books. Management can also attempt to classify liabilities, especially loans to shareholders, as equity.

⁸ *TSC Industries v. Northway, Inc.*, 426 U.S. 438, 449 (1976).

The motives for balance-sheet manipulation usually relate to reporting requirements established by lenders and regulators who tend to focus more heavily on balance-sheet items. A bank loan covenant, for example, may require a certain amount of shareholders' equity, a maximum debt-to-equity ratio, and/or a minimum current ratio. If the borrowing company's balance-sheet accounts violate the loan covenants, the company may be in default under the terms of the loan and be subject to accelerated repayment of the loan or be precluded from any future loan advances. To make matters worse, a publicly traded company probably would have to report to securities regulators that it was in default under its loan covenants and, as a consequence, suffer a decline in its stock price. Similarly, companies in regulated industries such as insurance and banking must maintain certain amounts of capital to meet regulatory requirements. Failure to do so may result in sanctions or even closure by the regulators. Therefore, motives for balance-sheet manipulation, while perhaps being more case-specific than those discussed previously for earnings fraud, nonetheless pose a real threat to accounting integrity.

Comparator Systems Case Study

In May 1996, the SEC suspended trading in the securities of Comparator Systems, a Southern California company that claimed to be in the business of producing fingerprint identification technology. The SEC was concerned about the adequacy and accuracy of publicly disseminated information as well as about the valuation of certain assets reported in Comparator's financial statements. Shortly thereafter, the SEC obtained a permanent injunction against the company and its principal executive officers on evidence that Comparator's assets provided no future economic benefit, had been recorded improperly, or simply did not exist. Comparator's purported assets included patents and licenses, investments, accounts receivable, and prepaid fees. The patents, however, had expired or passed into the public domain, the investments represented interests in private companies not engaged in business activities, the accounts receivable balance reflected the company's claim for stock allegedly stolen by a former employee, and the prepaid fees consisted of stock issued to Comparator's officers and consultants. These bogus assets were substantially overstated but allowed Comparator to maintain its listing on the National Association of Securities Dealers automated quotation system (NASDAQ) SmallCap exchange and sell its worthless stock to unwitting investors.

10.2.4 Falsification of the Income Statement

Falsification of the income statement may be accomplished by overstating revenue, understating expenses, or some combination of the two, during a specified time period. Using either method, the effect will be to overstate net income on the income statement, overstate owners' equity on the balance sheet, and thereby increase reported earnings per share; or to overstate expenses and understate results of operations during one period with the intent of artificially overstating net income in future periods.

Overstatement of Revenue

Under GAAP, revenue should not be recognized until it is both realized (or realizable) and earned. FASB Concepts Statement No. 5, *Recognition and Measurement in Financial Statements of Business Enterprises*, states that revenue is realizable when a product is “exchanged for cash or claims to cash” and revenue is earned “when the entity has substantially accomplished what it must do to be entitled to the benefits represented by the revenue.”

If revenue has not been realized and earned, revenue recognition is improper. Examples of improper revenue recognition include:

1. Fictitious revenues
2. Premature revenue recognition
3. Sales of development stage products
4. Conditional sales
5. Sales with a right of return
6. Consignment sales
7. Channel stuffing
8. Vendor rebates
9. Barter transactions
10. Reciprocal exchange transactions (swaps)

Revenue recognition remains a leading source of financial statement misstatement, so much so that Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 316), states that revenue ordinarily should be presumed to be a fraud risk area (AU 316.41) and suggests that audit procedures such as confirmations of terms with customers and trend analyses by product line be directed toward this area. In 2004, 2005, and 2006, the area of revenue recognition has been a focus in Public Company Accounting Oversight Board (PCAOB) inspections of public company auditors.

Fictitious Revenues

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Report found that the most common method of revenue recognition fraud resulted from recording fictitious revenues. Fictitious revenues are revenues recorded on the sales of goods or services that never took place. Fictitious revenues may involve fictional or legitimate customers. In either case, transactions may be recorded in the sales journal and inventory records without adequate documentation. In some cases, false invoices and shipping documents are prepared to conceal the fraud and product may be sequestered in the warehouse, shipped off-site, or stored with freight forwarders.

Kurzweil Applied Intelligence Case Study

From 1992 to 1994, Kurzweil Applied Intelligence engaged in a fraudulent revenue recognition scheme that inflated Kurzweil's revenues and earnings reported in financial statements accompanying its initial public offering (IPO), as well as its

annual and periodic reports filed with the SEC. Among other things, Kurzweil senior executives forged signatures on sales quotes, executed side letters that negated its customer's obligation to purchase product, and recognized revenue from distributorship agreements where the distributor did not have the intent or ability to pay without resale. To perpetuate the fraud, goods were shipped to and stored at an off-site independent warehouse to create the false appearance that products had been sold and shipped to customers, and invoices were held for fraudulent sales where the customer would not expect to receive an invoice.

As a result of this fraudulent scheme, Kurzweil's CEO and senior vice president of sales were able to sell securities in the IPO at prices they knew to be artificially inflated and received annual bonuses based upon overstated sales. Given their personal stake in the scheme, Kurzweil's executives went to great lengths to conceal the fraud from its independent auditors.

In July 1995, the SEC filed civil charges against the company and its officers for overstating revenue and earnings. Those charges were settled in administrative proceedings against the company, four executive officers, and three mid-level employees in Kurzweil's accounting function. In December 1996, Kurzweil's CEO and senior vice president of sales were sentenced to federal prison terms of 33 and 18 months, respectively, based upon convictions for conspiracy, securities fraud, and falsification of corporate books and records.

Premature Revenue Recognition

The COSO Report found that the second most common technique to inflate revenue involves premature recognition. Unlike fictitious revenues, for which there is no evidence to support a sale, premature revenues are recorded on sales expected to occur but are not yet completed. Revenue is recognized prematurely on incomplete sales in which title has not yet passed from the seller to the buyer. Since the transfer of ownership completes the sale, it is not final until all the obligations associated with the sale have been completed. A classic example of premature revenue recognition results when revenue is recorded on a sale expected to close in the next quarter.

Historically, premature revenue recognition cases involved new public companies. The reason is that when a company goes public, analysts from a number of Wall Street firms will initiate coverage and begin to track the company's performance relative to management's projections for the year. That coverage creates considerable pressure on financial management to meet the expectations of Wall Street. This pressure is what gets a lot of companies into trouble. In order to meet analysts' expectations, some companies apply aggressive accounting techniques in order to increase the bottom line. If those techniques fall short of the target, the sales function is directed to "do whatever it takes" to enable the company to make its numbers.

Today, revenue recognition improprieties occur in well-established companies. However, the motive is often the same: Financial management may inflate reported revenue in order to meet analysts' consensus earnings estimates.

Financial management is not always aware of schemes within the company to inflate revenue, often because documents are fabricated and the conduct is concealed from the accounting function, which may not have adequate internal controls in place to detect the fraud. In other cases, internal controls may not keep up with the company's growth. In still other cases, the internal controls that do exist are circumvented by the individuals directing the fraud.

Most of the time, schemes to inflate revenue are intended to be short-term fixes. For companies seeking to establish credibility in the market, it may begin by holding the quarter open a few days to enable the sales function to close just a few more additional sales, or, sales that are expected to close the following quarter may be pulled ahead into the current quarter. In these types of cases, the rationalization is, "It's just a few, we'll make it up next quarter." The same rationalization is used to justify earnings management in well-established companies.

The problem is the shortfall is not easily recouped. As companies pull in potential sales that are further and further out into the future, it becomes less and less likely that the company will be able to make up the shortfall. As one sales manager involved in this type of predicament described it, "it's like robbing Peter to pay Paul." As time goes on, there is no way out—other than devising new schemes to prop up the numbers.

California Micro Devices Case Study

One example of a revenue recognition case that spiraled out of control involved California Micro Devices. Cal Micro made semiconductor components, which it sold to a number of blue-chip companies, including IBM, Motorola, and Kodak. The company went public in 1986. Within two years of its public offering, its auditors at the time detected revenue and expense cutoff errors and proposed \$2 million in adjustments. The company listened to its auditors and restated its earnings—only to do the same thing all over again the next year.

There were several motives to manipulate reported earnings. For example, the company was under pressure to meet analyst expectations, attract strategic partners, and increase the value of a secondary stock offering. To accomplish these goals, the company engaged in nearly a dozen revenue recognition schemes. For example, the company recorded revenue on sales that shipped in later quarters, on shipments before the customer agreed to accept delivery and on shipments held at the freight forwarder or in sales representative's houses until customers agreed to accept delivery.

To conceal this scheme, senior executive officers altered the company's books and records and lied to its auditors. For example, the company prepared two accounts receivable reports. One was a real report that listed actual receivables, and the other was for its board of directors and the marketplace. In addition, management told the board that the high number of receivables resulted from the high number of shipments at quarter-end—a phenomenon known as a "hockey stick" sales pattern. Management also told the board that many of the receivables resulted from

arrangements with distributors who had 180 days to pay. Of course, management neglected to mention that the customers had unconditional rights of return.

By the time of the fiscal 1994 year-end audit, more than \$8 million of those receivables were uncollectible, but Cal Micro managed to get a clean bill of health from its auditors, a then Big Six accounting firm. Just under \$1 million was written off as bad debt, and the remainder (around \$7 million) was written off as a nonproductive technology acquisition.

In October 1994, the company disclosed the accounting irregularities and shortly thereafter terminated its CEO and CFO. In January 1995, forensic auditors determined Cal Micro had recorded \$38 million in bogus revenue. In September 1997, the CEO and CFO were indicted on criminal charges for their knowledge of the fraud and for their sales of substantial amounts of Cal Micro stock while revenue was artificially inflated. In July 1998, they were convicted of securities fraud.

Sales of Development Stage Products

Revenue may also be overstated through the recognition of sales on development stage products that require further development or product refinement. Even if products are accepted by customers who agree to serve as a “beta-test” site for the new product, such arrangements are typically made on a trial or evaluation basis. Therefore, revenue recognition is inappropriate. Likewise, revenue recognition is inappropriate if a vendor delivers an incomplete or dysfunctional product that will require repair or maintenance after delivery to the customer.

The premature recognition of revenue on development stage products often occurs in the software industry. Revenue recognition on software licenses is governed by AICPA Statement of Position (SOP) 97-2, *Software Revenue Recognition*. Under SOP 97-2, revenue may be recognized from software sales only if persuasive evidence of an agreement exists, delivery has occurred, the vendor’s fee is fixed or determinable, and collectibility is probable. If the software sale contains other elements, such as software upgrades or other enhancements that are integral to the functionality of the software license, then revenue must be recognized in accordance with contract accounting, which delays revenue recognition.

MicroStrategy Case Study

In December 2000, the SEC filed charges against three senior executive officers of MicroStrategy Inc., its CEO, CFO, and COO, for materially overstating revenue and earnings on sales of software and information services during the period 1998 through 2000. The Commission alleged that, among other things, MicroStrategy improperly recognized material amounts of revenue, up front, on certain multiple element deals in which MicroStrategy had a continuing obligation to provide significant services or future products which were not separable from the sale of a license to the Company’s existing software products. Several of these deals had a development component that required MicroStrategy to develop additional or customized applications of the product. Despite its continuing obligation to provide

additional software, licenses, and services, MicroStrategy improperly recognized the revenue up front by mischaracterizing the transactions as the sale of software product, contrary to SOP 97-2. As a result of these and other errors, MicroStrategy overstated revenues by approximately \$66 million. In the settlement of the ensuing civil action, the defendants received substantial sanctions, including an order to pay \$10 million in disgorgement and \$1 million in penalties. In a separate settled order, MicroStrategy's corporate controller and accounting manager were also sanctioned for their roles in the fraudulent scheme.

Conditional Sales

Conditional sales are sales with terms that have not yet been completed. As in the case of premature sales, recognizing revenue from conditional sales is improper because the risks and rewards of ownership have not passed from the seller to the buyer. Examples of conditional sales include sales subject to funding contingencies or performance conditions. Even if delivery has occurred, and the customer has physically accepted delivery, the sale is not complete until the contingencies have been removed.

Kendall Square Case Study

In the mid 1990s, Kendall Square Research Corporation, a Cambridge, Massachusetts, manufacturer of specialized computer systems for research applications, overstated approximately 50 percent of its reported revenues over an eighteen-month period by improperly recognizing revenue on conditional sales to universities and research institutions. Because these organizations were dependent upon grants from the government and from private foundations to support their activities, Kendall Square routinely sold its computer systems subject to funding contingencies, pursuant to which the customers were not obligated to pay until they received funding. Recognition of revenue on these sales violated GAAP because the revenue was not realizable until the funding contingency expired and because payment was not reasonably assured, as required by FASB Concepts Statement No. 5 and Accounting Research Bulletin (ARB) No. 43, *Restatement and Revision of Accounting Research Bulletins*.

Sales With a Right of Return

In the ordinary course of business, there is nothing wrong with giving purchasers a right of return, as long as an appropriate reserve has been established. However, return rights are not always properly reserved, and may be concealed in side letters with other contingencies to create the false appearance that revenue has been realized and earned.

Under GAAP, it is improper to recognize sales with a right of return unless the seller has estimated the likelihood of returns and booked an appropriate reserve. More specifically, FASB Statement No. 48, *Revenue Recognition when a Right of Return Exists*, provides that to recognize revenue when a right of return exists, "the amount of future returns [must] be

reasonably estimated.” Based upon this estimate, sales must be offset by expected returns to report revenues accurately. The recognition of sales that do not meet the requirements of FASB Statement No. 48 results in the overstatement of revenue.

Consignment Sales

A consignment sale is a type of contingent sale that is subject to acceptance by a third party. A distributor, for example, may take product on consignment and agree to pay for the product when it is resold to a third-party customer. Revenue may not be recognized on consignment sales until the third-party customer accepts the product. Consignment sales are fraudulent if material terms are not reflected in the consignment contract and instead appear in side letters or oral communications reflecting the true nature of the sale.

Channel Stuffing

Channel stuffing occurs when a distributor agrees to accept more product than is needed, typically in exchange for substantial discounts or other inducements. Although the practice is not improper, *per se*, material terms are often concealed in side letters or oral agreements that provide significant discounts and/or the right to exchange or return unsold product. If this occurs, the distributor is, in effect, accepting product on consignment without accepting the risks of ownership. Revenue recognition under these circumstances violates GAAP.

Vendor Rebates

The two primary types of vendor rebates are transaction rebates and incentive rebates. A *transaction rebate* is a discount or refund from the manufacturer on each product purchased. Transaction rebates are normally recorded immediately as a reduction to cost of goods sold because the rebate is earned at the time the product is purchased from the manufacturer. *Incentive rebates*, by contrast, usually require the purchaser to meet specified purchase levels. Under FASB Statement No. 5, incentive rebate income may not be recognized until the required purchase levels have been met. The recognition of incentive rebates before meeting the requisite purchase levels overstates income.

Barter Transactions

Most commercial transactions involve the exchange of monetary assets or liabilities for goods or services. The amount of the monetary asset or liability exchanged typically provides the basis for measuring the value of the transaction.

Barter transactions involve the exchange of noncash assets or liabilities. There are two types of barter transactions. One involves an exchange of nonmonetary assets or liabilities with another entity (reciprocal exchanges), and the other involves a transfer to another entity of a nonmonetary asset for which for which no assets are received or relinquished (nonreciprocal transfer).⁹

Reciprocal Exchange Transactions (Swaps)

Revenue may be recorded in reciprocal exchange transactions if certain requirements are met. There must, however, be economic substance to the transaction. So-called “round-trip” deals, which typically involve a swap of assets or services without any real gains, lack economic substance.

⁹ APB Opinion No. 29, *Accounting for Nonmonetary Transactions*.

The SEC is investigating whether telecommunications and energy companies conducted swaps of network capacity to improperly inflate reported revenue. For example, Global Crossing agreed to buy \$18 million in services from Enron to be paid over a period of eight years, and simultaneously agreed to sell \$18 million in services to Enron and be paid immediately. Although Global Crossing recorded the liability on its balance sheet, it recorded the entire revenue amount in its income statement. The accounting for these transactions is under scrutiny. The SEC and the Justice Department are conducting similar investigations into the restatement of \$1.1 billion in revenue by Qwest Communications resulting from its improper accounting of capacity swaps in 1999, 2000, and 2001.

Understatement of Expenses

Another method used to falsify the income statement involves the understatement of expenses. Under GAAP, the matching principle requires that revenue and its related expenses be recorded in the same accounting period. If the costs associated with revenues recorded in one period are deferred to a later period, net income is overstated for the period the revenue is recognized and understated for the period the expenses are recorded.

Examples of the understatement of expenses to artificially inflate net income include the following:

1. Deferral of operating expenses
2. Understatement or omission of sales discounts and allowances
3. Improper capitalization of current period expenses

Deferral of Operating Expenses

Expenses may be improperly deferred in order to meet budget projections or consensus earnings estimates. If costs are expensed during periods subsequent to the period in which the cost was incurred, the expenses are not properly matched against the income they helped produce. The recording of expenses in the wrong period often signals a lack of internal accounting controls.

Livent, Inc. Case Study

Livent, Inc. was a Canadian theater company that produced a number of successful Broadway Shows, including *Phantom of the Opera*, *Showboat*, and *Ragtime*. In January 1999, the SEC brought enforcement proceedings against nine former employees of Livent, for their involvement in a scheme to inflate income by falsifying expenses, among other things. This scheme operated for a period of eight years, from 1990 through 1998. The Commission's complaint also alleged kickbacks from customers and a revenue recognition component. This discussion will focus on the expense items.

Livent manipulated reported expenses by:

1. Transferring preproduction costs for the shows to fixed assets such as the construction of theaters
2. Simply removing certain expenses and related liabilities from the general ledger

3. Transferring costs from shows currently running to other shows that had not yet opened

The scheme was pervasive. It involved the CEO, president, CFO, senior vice president of finance, COO, and three controllers. Five of these individuals traded in Livent securities while earnings were artificially inflated. In 1998, the company restated its financial results. The restatement totaled nearly 100 million dollars.

Of the nine individuals the SEC charged with civil fraud, two were indicted in a parallel criminal proceeding, and two others pled guilty to violations of federal securities laws. In addition, in a civil injunctive action, the Commission charged Livent's general counsel, who had been aware of the scheme and participated in drafting revenue generating contracts subject to side letters, which were concealed from the outside auditors.

Understatement or Omission of Sales Discounts and Allowances

The easiest way to understate expenses is to simply omit them altogether. The omission of expenses artificially inflates net income and owners' equity. For example, the omission of sales discounts and allowances will overstate revenue and net income on the income statement, and understate liabilities and overstate owners' equity on the balance sheet.

Aurora Foods, Inc. Case Study

In January 2001, the SEC brought charges against three former senior officers and five employees of Aurora Foods, Inc., a producer and marketer of branded food products, for underreporting trade marketing expenses and thereby inflating reported earnings in 1998 and 1999. Specifically, Aurora was found to have underreported more than \$43 million in trade marketing expenses, the expenses incurred to induce grocery stores to purchase its products. Examples include case discounts and similar incentives. Rather than properly recording these expenses, Aurora's senior management attempted to conceal them from the company's auditors by directing subordinates to make false entries in various accounts on Aurora's books. For example, Aurora employees were directed to move trade promotion expenses into accounts receivable through false entries in the accounts receivable ledger and subsidiary ledgers and through manual adjustments in the trade promotion accrual. Although one division manager objected to these practices, she, too, was sanctioned for following the inappropriate instructions of her superiors.

Improper Capitalization of Current-Period Expenses

Capital expenditures are costs that benefit the company over more than one accounting period. Accordingly, capital expenses are amortized over a period of years. Cost of goods sold or cost of sales, by contrast, directly correspond to the generation of current revenue

and only provide benefits during the current accounting period. As a result, these costs are expensed immediately. If period expenses are improperly capitalized, net income is improperly overstated.

WorldCom, Inc. Case Study

In June 2002, the SEC brought charges against WorldCom, Inc., the second biggest U.S. long-distance telephone and data services provider, for fraudulently overstating income before taxes and minority interests by \$3.8 billion during fiscal 2001 and the first quarter of fiscal 2002. The SEC's complaint alleges that WorldCom falsely portrayed its financial condition through the improper capitalization of "line costs," which were WorldCom's costs of leasing space on competitors' telephone lines. Under GAAP, these costs must be expensed in the period incurred and may not be capitalized. In contravention of GAAP, WorldCom's senior management is alleged to have directed the transfer of line costs to capital accounts in amounts sufficient to enable the company to meet Wall Street analysts' consensus earnings estimates. Among other things, this fraudulent scheme allowed the company to avoid reporting losses in 2001 and 2002. Investigations by the SEC, the Department of Justice and various Congressional committees are continuing.

Some Comments on Financial Statement Frauds

Some financial statement misstatements are "self-correcting" in that misstatements in one period will likely be reversed in the next period. For example, an overstatement of ending inventory increases income in the year of the overstatement, but next period the misstatement rolls into Cost of Sales and unless there is a significant additional profit in that year, the misstatement often has to be matched or increased to meet earnings goals in the next period. Often such schemes fall apart soon after they start to involve material amounts, and physical counts and book records become increasingly divergent. Some misstatements self-correct after longer periods such as depreciation or amortization misstatements. Fictitious sales often lead to detection when cash flows and aging receivables raise questions, but the brazen Parmalat fraud seemed to escape detection for a long time because of the manufacturing of false balance sheet assets and the offloading of liabilities to related entities.

In other cases, the issue may continue until detected or until reversed. For example, excess or deficient accruals of one sort or another may provide a source of future management manipulation of income, or may just sit on the balance sheet for a long time if they are not distorting overall financial results.

Another example of misstatements that do not self-correct is misstatements in valuing the compensation from stock option grants. In 2006, misdating of stock options (spring-loading or backdating) to maximize the executive award value was discovered and the scheme involved a large number of companies that should have known that this was both a fraudulent and deceptive process and it caused a misstatement of the proper compensations

expense for stock option awards. In as much as stock options began being expensed just a short time ago, the related compensation expense is now part of the income statement and not just a footnote disclosure. The SEC and IRS are conducting an increasingly wide investigation on this issue. The PCAOB Staff issued an Alert in July 2006 reminding auditors to include the controls surrounding the stock option granting and expensing practices into the scope of the Sarbanes-Oxley required reporting on internal controls.

10.2.5 Reducing the Risk of Fraud in Closely Held Companies

Much of this chapter focuses on publicly traded companies both because information about frauds committed by these entities is readily available and because regulators have been in the forefront of fraud detection and prevention. Nevertheless, every type of fraud discussed here can occur in closely held private companies; only the motives and timing are slightly different. Although the managements of closely held companies might not have to worry about securities analysts' expectations, there may be outside shareholders demanding better earnings performance. These demands might lead management to employ any of the earnings manipulation schemes discussed above. Of course, if management bonuses are a function of increased earnings, there is a motive for earnings manipulation regardless of whether the company is publicly traded or not. If the outside investors are passive, the moment of performance assessment will most likely be the end of the fiscal year. Management of public companies, on the other hand, may feel pressure to hit targets quarterly if they have to report to regulators.

Family businesses with nonparticipating owners are particularly vulnerable to frauds by management family members. Although the notion of "family" conjures the exact opposite of this risk, the reality is that jealousy and rivalry can generate rationalizations that motivate the fraudulent shifting of cash flows to the management family member. Indeed, audits are critically important in such situations and provide the kind of oversight deterrence that can dissuade a tempted fraudster. By focusing on related party transactions and considering fraud as required in SAS No. 99, there is some assurance that the common practices of misappropriation are subject to detection.

The need to value shares in a closely held company may also give rise to earnings management. If shares are being valued for sale or any other purpose such as collateral for a bank loan to a major shareholder, earnings management may be employed to achieve the appearance of a steady rise in earnings. This misleading rise in earnings could induce an appraiser or stock valuations specialist to assign a higher growth rate to projected earnings. It is just as likely, however, that the appearance of consistently rising earnings could suggest the use a lower firm-specific risk premium to calculate the present value of that projected earnings stream since earnings would appear to be less volatile. The end result of earnings management in a closely held company is thus similar to the effect of earnings management on the P/E multiple of publicly traded companies.¹⁰

¹⁰ To learn more about the issues in private company valuations, in 2004, the AICPA published a practice aid entitled *Valuation of Privately-Held-Company Equity Securities Issued as Compensation*.

For a closely held company, the prevention of fraud in the financial statements starts with requiring that financials presented to the board of directors and to outsiders be in conformity with GAAP. The timing of cash flows in cash-basis accounting can lead to the manipulation of financial statements.¹¹ Accrual-basis accounting looks to economic events to determine whether a debt is incurred or whether revenue is earned; the time of the occurrence of those events may be quite different from that at which cash is paid or received. What limits the possibility for fraud in accrual-basis accounting is the reduced opportunity to hide a debt or record unearned revenue since the standards of recognition are more explicit than those for cash-basis accounting.

Although GAAP is not required for private companies, it is difficult for those companies to communicate with outsiders, such as lenders and investors, without producing GAAP-based financial statements. In a sense, GAAP is the common financial language of the United States because it contains a set of rules and standards developed and tested over many years that are known to readers of financial statements. Certain foreign firms whose shares are not traded on U.S. exchanges may use local accounting standards or International Accounting Standards (IAS) for domestic reporting but would find raising capital in the United States problematical without translating those statements into GAAP.

Additional fraud prevention measures include implementation of the internal controls discussed in Section 1.3, "Internal Controls and 'Fraudproofing,'" in Chapter 1 of this *Handbook* and promoting an ethical environment, as covered in Chapter 2, "Promoting an Ethical Environment." For middle-market firms,¹² i.e., those with annual revenues of \$10 million or more, the findings of the COSO Report are especially applicable since research concluded that smaller companies are more susceptible to fraud.

The importance of financial statement fraud prevention measures increases directly with company size. For a very small company, fraudulent financial statements that slightly inflate earnings or assets could be used to secure a bank loan or small investment but little else. Steps taken to prevent fraud at that level should reflect the potential for damages resulting from such misstatement. For larger, middle-market companies or small companies fraudulently representing themselves as larger companies, potential damages are more serious; steps taken to prevent fraud should therefore be more visible and systematic. For example, a middle-market company should implement reviews of internal controls at least once a year by outside auditors and more frequently by internal accounting staff. If budgets allow, a significant fraud-prevention measure should include hiring an internal auditor to assess the effectiveness of the controls of each business unit for a year. Assessments of the adequacy of internal controls would help significantly with early fraud detection.

The reporting of irregularities to independent board members is one of the most important fraud-prevention measures available to closely held companies. The opening of such a formal reporting channel increases the likelihood that corrective action will be taken. Without such a reporting channel, management, even if not directly involved in a fraud, might be inclined to sweep the problem under the rug for fear of reprisal or embarrassment. If the closely-held firm has no outside directors, a significant fraud-prevention step would be the appointment of such director(s).

¹¹ For that reason, U.S. tax law generally requires corporations to report on an accrual basis when gross receipts exceed an average of \$5 million per year over the prior three tax years.

¹² *Middle market* is a term used by bankers to segment their lending markets. The term is used here because closely held firms frequently interact with banks on matters involving their financial statements.

Under SAS No. 112, (a revision of SAS No. 60) *Communicating Internal Control Related Matters Identified in an Audit* starting with year-end 2006 audits, managements and “those charged with governance” will receive written reports annually on internal controls issues that are considered significant deficiencies or material weakness of which the auditor is aware. The presence of such conditions is often a strong indicator that an “opportunity” will be available to facilitate a misstatement or fraud. A minor fraud, because of its nature, is often considered a significant deficiency if not a material weakness that would be included in this communication.

It is worthwhile to say a few words about some other variables in private company financial reporting. Private companies do not have to engage auditors to perform an audit. Although other parties may require an audit (e.g., creditors, banks, venture capitalists, family members), lesser accountant services such as reviews and compilations are available, and are increasingly being considered by smaller entities as the bar continues to be raised on the requirements auditors should be performing on every audit. However, the services can provide vastly different protections than an audit. In a review, the accountant evaluates the reasonableness of the reported amounts and disclosures through inquiry, observation, and generally the application of analytical procedures. Fraud is considered, as the inquiries and considerations of SAS No. 99 are applicable, but the detailed tests that might reveal more issues are not required. Most importantly, the auditor is not responsible for understanding internal control. An “opinion” is not given, but matters coming to the auditor’s attention or any identified GAAP departures are communicated. In a compilation, the accountant often acts simply as a “compiler” of information in the accounting records into financial statements and performs no audit procedures and provides no assurance. Footnote disclosures need not be complete, provided the omission is not considered to be for deceptive purposes. The accountant need not even be independent of the entity to perform this service. Companies and owners need to understand the services and their potential implications and risks to the financial statement users.

Frauds and large losses need not be limited to companies publicly trading securities. A well publicized fraud that cost creditors a billion dollars (and later the auditors hundreds of millions of dollars) was Phar-Mor, a discount drug store chain with over 300 stores and 25,000 employees that inflated earnings by overstating inventory for several years in anticipation of an upcoming public offering. Although the inventory misstatement and fraud was detected before materially misstated financial statements were issued, the creditors were outraged that the fraud had not been detected earlier. Due to the strong growth record and profitability (false) of the company, its business risk to the audit firm was assessed as “low.” The unusual story of the flamboyant founder and COO of Phar-Mor, Michael Monus, convicted of 109 federal counts and sentenced to nearly 20 years in federal prison, is interesting reading and a mini-case study in the risks of strong entrepreneurial management and “tone at the top.” Filing for bankruptcy protection in 1992 and emerging in 1995, the company went out of business in 2002.

10.3 SPECIAL AREAS OF FINANCIAL STATEMENT FRAUD

Certain items on a firm’s financial statements appear to be especially vulnerable to fraud. The following discussion will highlight major fraud-prone areas and the steps that can lead to early detection. The seven areas identified are:

1. Failure to record loss contingencies and asset writeoffs

2. Manipulation of acquisition reserves
3. Cost shifting to improve current operating results
4. Recognizing fictitious revenues
5. Improper disclosures and material omissions
6. Special purpose entities; the Enron Case
7. Methods to conceal financial statement fraud from auditors

The common thread running through all these areas is that detection requires *the auditor to look for something not present in the financial statements*. Auditors are accustomed to beginning with a trial balance listing of all accounts and determining the procedures necessary to complete the audit. An item that does not show up on that trial balance at all, however, may never come to the attention of the auditor. For instance, in order to detect a failure to book a loss reserve for a contingent liability, one must first discover the existence of the contingency. From an auditing perspective, in the case of a failure to record a loss contingency, there is no loss contingency balance to audit; the accounting entry simply does not exist. Similarly, using acquisition reserves to hide current-period expenses means that the expense item or category is absent from the income statement and is buried in some balance-sheet account relating to a prior business combination.

Cost shifting, that is, the movement of expenses from one entity or period to another, is equally hard to find. When the auditor looks at the accounts for the one business as of a given date, he or she does not see expenses shunted over to another affiliate or to another time period. In the case of fictitious revenue, although the auditor at least has income statement revenue accounts to examine, the existence of side letters with customers which, for example, grant those customers the right to return product, does not show up as a contingency or in the footnotes. In practice, an auditor is not likely to be told that side letters exist.

Clearly, these are the toughest kinds of financial statement fraud to detect. Nevertheless, for each fraud discussed above, the auditor should look for warning signs. Those red flags may be small in dollar amounts but may nevertheless point to significant irregularities. The following discussion assumes that a certain subset¹³ of management has attempted to manipulate financial data and looks at these issues in the context of audit planning and execution to determine what additional steps an auditor could take that might lead to detection of the fraud.

10.3.1 Failure to Record Loss Contingencies and Asset Writeoffs

Loss Contingencies

A loss contingency is defined in FASB Statement No. 5 as “an existing condition, situation, or set of circumstances involving uncertainty as to possible . . . loss . . . to an enterprise that

¹³ If financial statement fraud is traceable to a significant number of senior managers, the auditor should consider taking additional steps. For internal auditors, those steps would include discussions with legal counsel. Outside auditors should consider issuing a qualified opinion or, more likely, resigning from the audit engagement altogether.

will ultimately be resolved when one or more future events occur or fail to occur.”¹⁴ FASB Statement No. 5 continues to state that the “[r]esolution of the uncertainty may confirm . . . the loss or impairment of an asset or the incurrence of a liability.”¹⁵

FASB Statement No. 5 lists examples of loss contingencies that include:

- Collectability of receivables
- Obligations related to product warranties and product defects
- Risk of loss or damage of enterprise property
- Threat of expropriation of assets
- Pending or threatened litigation
- Actual or possible claims and assessments
- Guarantees of indebtedness of others
- Agreements to repurchase receivables (or repurchase related property) that have been sold¹⁶

A firm is required to accrue a loss contingency when that contingency is both *probable* and *able to be estimated*. FASB Statement No. 5 states:

An estimated loss from a loss contingency . . . shall be accrued by a charge to income if both of the following conditions are met:

- a. Information available prior to issuance of the financial statements indicates that it is probable that an asset had been impaired or a liability had been incurred at the date of the financial statements. It is implicit in this condition that it must be probable that one or more future events will occur confirming the fact of the loss.
- b. The amount of loss can be reasonably estimated.¹⁷

A future event is probable if it is “likely to occur.”¹⁸

Having set the ground rules, we can examine some specific examples in the following sections:

1. Warranty and product claims reserves
2. Asset writeoffs

Warranty and Product Claims Reserves

If a manufacturer experiences postproduction problems with a certain product, it may begin to experience higher-than-expected returns or, more likely, claims for reimbursement

¹⁴ Statement of Financial Accounting Standards No. 5, paragraph 1.

¹⁵ *Ibid.*, paragraph 1.

¹⁶ *Ibid.*, paragraph 4.

¹⁷ *Ibid.*, paragraph 8.

¹⁸ *Ibid.*, paragraph 3. Footnote disclosure of the loss contingency may be required if the future event is less than probable but is “reasonably possible;” if the chance of a future event is more than remote but less than likely, FASB Statement No. 5, paragraph 10, requires disclosure in the financial statements of the nature of the contingency and an estimate of the potential loss.

or repair. Those claims may arise under a specific warranty, under product tort law or under consumer protection laws and regulations. At this point, the manufacturer must assess its overall cost exposure. It might be possible to estimate the extent of future claims as a percentage of production based on past experience with other products subject to similar problems. It might also be possible to estimate the cost of each claim, i.e., the cost of replacement or repair for each defective unit of product. If both an estimate of future claims and the cost of each claim are available, then the amount of loss can be reasonably estimated. FASB Statement No. 5 requires the booking of a loss contingency if the future claims are likely to occur. If, however, the manufacturer is already seeing large numbers of claims prior to or soon after the close of its financial reporting period,¹⁹ it is reasonable to assume that the likelihood of future claims is high and that a FASB Statement No. 5 reserve should be accrued with a charge to current earnings.

However, a manufacturer under pressure to achieve increased earnings may be very reluctant to accrue a warranty or product claims reserve. Management may take the position that the problem does not exist or cannot be quantified. But, an alert auditor may detect certain red flags that indicate a problem does indeed exist and that its extent can be estimated. The red flags that indicate the existence of a contingency include:

1. The incidence of claims prior to the issuance of financial statements (discussed above)
2. Discussions with (and bills from) outside legal counsel
3. Internal correspondence within production and research staffs as to the need to address a critical problem with a product already on the market
4. Internal correspondence among department heads of production, R&D, general counsel, and senior management about postproduction problems and product claims
5. External correspondence between the manufacturer and its customers about a given product concerning special price concessions or special return privileges
6. The incidence of special or overbudget freight charges to accommodate returns and/or the shipment of replacement product
7. Shifting of production schedules to manufacture replacement product
8. Halting manufacture of the product in question
9. Shifting of R&D staff away from planned research projects to applications engineering relating to redesign of existing products
10. Payments in sometimes seemingly immaterial amounts to customers on a regular basis over a period of weeks or months that indicate some arrangement to compensate for product defects

Once it has been established that a loss contingency exists or is likely to occur,²⁰ the next step is to determine whether the potential loss can be quantified. In this case, if the firm

¹⁹ Actually, FASB Statement No. 5 requires the assessment of contingencies arising from “information available *prior to issuance* of the financial statements” (emphasis added). Therefore, if claims relating to a prior period come to the attention of management during the preparation of financial statements for that prior period, management should consider booking a contingency as of the end of that period.

²⁰ For purposes of this discussion, we focus on failure to accrue a probable loss contingency. However, violations of GAAP (and securities laws if the company files with the SEC) may occur if the firm has a

itself does not have actual experience with product claims or if that experience is not relevant to the product in question, the auditor should look outside the firm. Industry statistics on product liability and the incidence of claims are generally available from trade associations, government regulators, or independent research organizations. In the course of examining internal correspondence between department heads and within departments, however, the auditor will likely find some internal estimates of the extent of the problem. This becomes especially obvious if the correspondents are attempting to justify the allocation of additional staff and financial resources to combat the problem or to explain why production was shifted or halted. In short, the members of management not directly involved in manipulating the financial statements may speak quite frankly about the loss contingency.

Asset Writeoffs

An asset is not always worth its balance-sheet carrying value. Even if an appropriate depreciation schedule is established when the asset is acquired, over time the needs of the business enterprise may change. Because of rapid changes in engineering and materials applications, for example, manufacturing processes may need to be updated to remain economically competitive. The machinery used in the old processes may become obsolete well before the machines themselves actually wear out and are depreciated down to salvage value. Similarly, changes in customer demand may force a manufacturer to discontinue a certain product line and render useless equipment specially designed to build that product. Firms operating in highly competitive markets may lose business to a low-cost competitor and be forced to idle production lines. Occasionally, in order to obtain or retain a customer relationship, a firm may even deliberately quote a price for its products that does not cover the cost of acquiring and operating the equipment used to produce those products. In all these cases, management should assess whether the equipment carrying value is impaired, especially if there are no reasonable prospects of finding an alternative use for the equipment. In the event an impairment loss should be taken, however, management may fraudulently postpone that charge if it causes earnings to fall below a managed earnings target.²¹

To detect this fraud, the auditor must be particularly adept at seeing through management's pretensions to get to the facts. The best place to begin is to review fixed assets with divisional or production personnel. FASB Statement No. 121, *Accounting for the Impairment of Long-Lived Assets and for Long-Lived Assets to Be Disposed Of*, provides a list of possible events that may give rise to an impairment:

1. A significant decrease in the market value of an asset
2. A significant change in the extent or manner in which an asset is used or a significant physical change in an asset
3. A significant adverse change in legal factors or in the business climate that could affect the value of an asset or an adverse action or assessment by a regulator

reasonably possible loss contingency, according to FASB Statement No. 5, paragraph 10, but fails to make the required disclosure of that contingency in its financial statements.

²¹ In this section, we are discussing asset writeoffs in the course of operations. Acquisition-related writeoffs are discussed in the preceding section entitled "Big-Bath Restructuring Changes."

4. An accumulation of costs significantly in excess of the amount originally expected to acquire or construct an asset
5. A current-period operating or cash-flow loss combined with a history of operating or cash flow losses or a projection or forecast that demonstrates continuing losses associated with an asset used for the purpose of producing revenue²²

The auditor may wish to draw questions for firm personnel from this list and look for evidence of changes in production and product demand to determine whether an asset is impaired.

Clearly, if equipment has been moved off the shop floor into storage and there are no plans for future use of that equipment, an impairment loss is highly likely. The more difficult issues arise if equipment is still in use but profitability is less certain. Profitability is at issue when assets may be impaired because FASB Statement No. 121 states that “[i]f the sum of expected future cash flows (undiscounted and without interest charges) is less than the carrying amount of the asset, the entity shall recognize an impairment loss. . . .”²³ Since most management reporting systems, however, measure profitability by product line or by customer, it is hard to imagine how a business could survive in today’s competitive environment without this information. Indeed, the activity-based costing initiatives begun in the 1980s were a direct result of the need for management to understand a product’s contribution to overall firm profitability. Although auditors may not be accustomed to reviewing product line profitability reports, these reports source revenues to the costs to produce them and can answer directly whether a given production process has been historically profitable.

Historical data are the basis of management plans and profitability forecasts. If the auditor can obtain such forecasts directly from the personnel with line responsibility for production, those personnel might be inclined to render a more accurate forecast since they are unaware of management’s earnings target. One should keep in mind that line managers may have an incentive to show as positive a picture as possible to avoid production shutdowns. Also, line managers may also receive hints or outright requests from management to produce an overly favorable forecast. In either case, however, if the forecasts are accompanied by written narratives, the narratives will generally list all the downside possibilities in order to provide political cover for the line manager should events not turn out as planned.²⁴ The auditor may be able to assess the reasonableness of the forecast, given the known conditions at the time and the likelihood of those downside possibilities.

Proving fraud in a forecast is difficult because a forecast is by its very nature a best-guess.²⁵ If that forecast, however, was based on facts known to be incorrect, such as a major customer’s known unwillingness to buy the product, then the forecast was fraudulently

²² FASB Statement No. 121, paragraph 5.

²³ *Ibid.*, paragraph 6.

²⁴ If there are no narratives, the auditor can probably obtain a list of potential downside possibilities simply by asking the line managers.

²⁵ For a definition of financial forecast, see the AICPA *Guide for Prospective Financial Statements*, Section 200.04.

constructed. A forecast may also become fraudulent if it is used at a later time to justify a management decision even though the management knows that significant facts have changed. For example, a forecast may accurately reflect that, at the time of preparation, there was a possibility that a certain major customer wanted to buy the product. If, however, by the balance-sheet date, management knows that the customer is not interested and there are no alternative buyers, it would be fraudulent to assert that the forecast is still accurate and then use it to justify not writing down the value of assets used to produce that product.

Another area of asset writeoff that can fall victim to fraud involves investments in securities of private companies. Such securities are difficult to value because transaction prices are not publicly available. If the security held is stock and there have been substantial historical operating losses with little hope of future profitability (i.e., the decline in value is other than temporary), that stock may be impaired according to FASB Statement No. 115, *Accounting for Certain Investments in Debt and Equity Securities*. Likewise, FASB Statement No. 115 states that for debt,

... if it is possible that the investor will be unable to collect all amounts due according to the contractual terms of a debt security not impaired at acquisition, an other-than-temporary impairment shall be considered to have occurred. If the decline in fair value [of any security] is judged to be other than temporary, the cost basis of the individual security shall be written down to fair value as a new cost basis and the amount of the write-down shall be included in earnings (that is, accounted for as a realized loss).²⁶

Without recent prices for the sale of stock and debt in a private company, the auditor might have to look at financial information from the investee company. The investor, if it holds a significant position in the investee, should have financial information on file (if not, this should be a red flag that something may be amiss). Those data would likely include results of operations that would give historical profitability. For future profit estimates, one should look to company forecasts and assess the validity of those forecasts based upon the known relationships, if any, between management of the investor and investee. If common representation within management or on the boards of both companies exists, further inquiry may be necessary to determine the validity of any forecast. Losses over several past years may be sufficient to establish impairment, as the following case study taken from a SEC Accounting and Auditing Enforcement Release demonstrates.

Windpower, Inc. Case Study

Windpower, Inc., a small private company, began doing research in windmill production and technology in 1978 with a view to later commercial development. The following year, the same group of investors established Breezy Valley Energy, Inc. and transferred Windpower's R&D work to Breezy Valley in 1980. Breezy Valley reimbursed Windpower \$31,308 for work done to date and from then on Windpower lent Breezy Valley money for R&D. In fact, these loans formed the primary source of funds for Breezy Valley.

²⁶ FASB Statement 115, paragraph 16.

According to Windpower's financial statements for the nine months ended March 31, 1981, loans outstanding to Breezy Valley at that date amounted to \$108,434. By the end of the following fiscal year, the aggregate loans totaled \$208,146 and by March 31, 1983, they reached \$321,725. In Windpower's financial statements for 1981 and 1982, the loans are accounted for as a receivable; during fiscal 1983, this receivable was exchanged for Breezy Valley preferred stock.

In September 1983, Windpower filed a Form S-1 in connection with a proposed \$4-million IPO. In this filing, Windpower's investment in Breezy Valley was carried as an asset valued at historical cost rather than written down as Breezy Valley's prospects dimmed. Windpower's investment as reported in its various forms, represented 62 percent, 77 percent, and 80 percent of the total assets at the end of fiscal 1981, 1982, and 1983 respectively while cumulative operating losses increased at Breezy Valley from \$118,420 in fiscal 1981 to \$265,542 in 1982, and reached \$437,092 by the end of fiscal 1983. Revenues for Breezy Valley had declined such that it was bringing in only \$1 for every \$7 going out in expenses; future earnings prospects were unattractive because Breezy Valley seemed unable to market its products.

Conclusion and Analysis

On the grounds of its failure to write down its investment in Breezy Valley to net realizable value in accordance with GAAP, the SEC suspended the effectiveness of Windpower's registration statement for the \$4-million public offering. Since this case predated the issuance of FASB Statement No. 115, the SEC looked to FASB Statement No. 5 and found that Windpower should have applied the provisions of FASB Statement No. 5 which states in paragraph 8 that:

An estimated loss from a loss contingency . . . shall be accrued by a charge to income if both the following conditions are met:

- a) Information available prior to issuance of the financial statements indicates that it is probable that an asset has been impaired or a liability has been incurred at the date of the financial statements. It is implicit in this condition that it must be probable that one or more future events will occur confirming the fact of the loss.
- b) The amount of the loss can be reasonably estimated.

Windpower's financial condition met the requirements of paragraph a) since the investment in Breezy Valley was impaired and recovery was unlikely because of the growing losses and limited prospects of generating sales. The requirements of paragraph b) were also met since the amount of the loss was exactly equal to the known aggregate amount of the loans. Clearly, the impairment requirements of FASB Statement No. 115, if it had been in effect, were also met.

On the basis of this failure to take account of the reduced value of Windpower's investment and the slim prospects of recovery, the SEC instituted proceedings against Windpower's auditor and two of its partners for improperly certifying that Windpower's financial statements had been prepared according to GAAP and audited according to GAAS. The SEC accepted Offers of Settlement and Undertakings from the auditor and its two partners.

10.3.2 Manipulation of Acquisition Reserves

When one company acquires another using the purchase method of accounting for the transaction under Accounting Principles Board Opinion (APB) No. 16, *Business Combinations*, the purchase price paid is allocated to the assets of the acquired company using the fair value of those assets. Any excess of purchase price over the fair value of assets acquired is booked as goodwill. Liabilities can also be transferred or accrued; those liabilities assumed by the purchaser effectively increase the amount paid. If, as is usually the case, the cash portion of the purchase price covers the fair value of assets acquired, then liabilities assumed over and above the cash paid will increase goodwill.

One type of liability managers of an acquiring company may wish to set up are loss contingencies as provided under FASB Statement No. 5,²⁷ presumably for potential problems inherited or created when the target company was acquired. These loss contingencies or reserves, as they are more commonly known, typically increase the goodwill paid for the acquired company, i.e., the entry establishing the loss contingency is a credit to a reserve liability and a debit to goodwill. That goodwill is then amortized into income, usually over a forty-year period. Examples would include reserves for warranties on discontinued products or reserves for bad debts that would no longer be serviced as the acquiring company consolidates operations of the target, and closes or sells off unwanted segments. Management may also wish to set up severance reserves for employee layoffs. If those contingencies later materialize, the expense (debit) of performing the warranty work, writing off the debt or paying severance is then taken to the reserve as a credit balance on the liability section of the balance sheet.

Most important, the expense of a reserved item does not run through the income statement. Instead, since setting up the reserve itself created or increased goodwill from the purchase transaction, amortization of the goodwill attributable to the reserve comes into the income statement but only a small portion, perhaps as little as one-fortieth, is expensed in a given year. Therefore, establishing the reserve allows management to avoid taking the entire expense into income in the current period and, by the amortization of goodwill, to spread that expense over a much longer future time.

From this discussion, one can readily see that management has an incentive to reserve as much as possible when making acquisitions. Moreover, management does not need to attempt to set up all necessary reserves by the date of the acquisition; FASB Statement No. 38, *Accounting for Preacquisition Contingencies of Purchased Enterprises*, provides for a twelve-month period after the acquisition date to adjust the purchase price. It is here that management actions need to be carefully reviewed. Without restrictions on the booking of reserves after an acquisition, the current management of the acquiring company could constantly (and conveniently) create reserves to absorb current losses from acquired businesses.

²⁷ Other accounting literature discussing when and how contingencies can be incurred in connection with a business combination includes SEC SAB No. 100, *Restructuring and Impairment Charges* and Emerging Issues Task Force (EITF) Issues No. 94-3, *Liability Recognition for Certain Employee Termination Benefits and Other Costs to Exit an Activity (Including Certain Costs Incurred in a Restructuring)*, and No. 95-3, *Recognition of Liabilities in Connection with a Purchase Business Combination*.

At some point, however, current management must take responsibility for current period results. The twelve-month cutoff provided in FASB Statement No. 38 is the outside limit; the period for adjusting the purchase price should end when management “is no longer waiting for information that it has arranged to obtain and that is known to be available or obtainable”²⁸ at the time of the acquisition. Management crosses the line and commits fraud when it creates material purchase reserves for losses that were not foreseeable at the time of purchase, especially if management creates those reserves and adjusts the purchase price more than twelve months after the purchase date. Likewise, management also commits fraud when it uses reserves to absorb losses unrelated to the reasons for which the reserves were established.

Fabulous Deals, Inc. Case Study

As the divisional controller was about to go into a budget meeting, the Deal Club corporate CFO and corporate controller handed him new numbers inflating his revenue estimates by \$200 million. He was already staying up past midnight designing fictitious accounts under the corporate controller's instructions to create numbers that met analysts' estimates.

But this scene was not to be enacted until 20 years after Bill Battler, a wealthy Harvard MBA, had taken over Deal Club, a small discount-shopping club, in 1976 and went public with it in 1983 at 25 times sales despite losing \$2.5 million on only \$4 million in revenues the previous year. By 1997, Battler had built it into a business reporting \$2.3 billion in annual revenues. Battler had grown the business by persuading large credit card companies to promote the club to their cardholders. He also founded or acquired more than a dozen similar clubs in the travel and other industries and brought them under Deal Club's umbrella. Proud of a reported 70-percent membership renewal rate that provided what Battler called an “annuity-like” stream of predictable earnings, he saw the stock move to the \$25 area with a P/E of about 30.

Enter Carl Charise. A former tax lawyer, Charise founded Fabulous Franchises, Inc. in 1990 and went public with it in 1992 at \$4 a share. The company had the franchise rights to a number of hotel chains with a total of 500,000 rooms, real estate brokerages, rental cars, vacation time-sharing, and other businesses. Fabulous Franchises made money by charging a franchise fee and taking a percentage of earnings from its operators. Earnings were growing at an annual rate in excess of 60 percent because of Charise's good management and aggressive acquisition policy. The stock price hit a record \$79 in 1996 creating a return of 2,000 percent since going public. In addition to an office at company headquarters in North Carolina, he kept an office in Manhattan from which he constantly wooed Wall Street analysts with the Fabulous Franchises story.

As each company grew bigger, growth opportunities became fewer. Battler and Charise began telling the analysts to lower expectations since both companies

²⁸ FASB Statement No. 38, paragraph 4.b.

needed bigger and bigger acquisitions which were becoming harder and harder to find. In January 1997, Battler approached Charise proposing that Deal Club take over Fabulous Franchises. In the following months, discussions turned from acquisition by Deal Club to a merger of equals.

Superficially, the two companies seemed to make likely merger partners. The millions of well-to-do customers passing through Fabulous Franchises' operations were a natural market for Deal Club memberships and would create a new profit center. The merger would utilize the synergy of Fabulous Franchises' strong earnings and Deal Club's high multiple to add billions to market capitalization.

Trouble in Paradise began, however, when the two conflicting corporate cultures started to take a closer look at each other. Bill Battler proved to be an absentee visionary and the company ran itself in a casual manner that sometimes slipped into carelessness. Divisions were left to run things their own way; accounting systems were unsophisticated; financial reporting was slack and there seemed to be no long-term planning. These practices were defended as "entrepreneurial" and had, indeed, unarguably produced a business with \$2-billion-a-year in sales.

Carl Charise, on the other hand, was not only extremely charming to Wall Street, but also a very competent CEO who ran a tight ship. When his people demanded detailed nonpublic information including hard numbers, Deal Club executives backed off. In fact, instead of producing numbers for the new management team, the Deal Club President produced one for himself, namely, a \$25-million negotiated payout, to be paid in the event that he was not made COO of the merged company after two years. The whole situation made Fabulous Franchises nervous but Deal Club's outside auditors, Fiddle & Fakit, gave assurances that the books were in excellent condition. Nevertheless, in the midst of all this prickliness, Deal Club kept delivering spectacular quarterly earnings. Fabulous Franchises executives could not confirm any information, however, and therefore remained apprehensive.

After the two companies closed the merger under the name Fabulous Deals, Inc. in late 1997, more unusual behavior began to surface at Deal Club. Bill Battler insisted that the old Deal Club remain financially autonomous and that CFO Haggis McFudge and controller Patricia Candel remain in place. Deal Club's divisional controllers would not report to the merged company's chief accounting officer but to McFudge and Candel, who would consolidate results before passing them on. This arrangement was reluctantly agreed to, but the financial reports continued to come in slowly and, meanwhile, Fabulous Deals risked missing the 10-K filing deadline with the SEC. In the face of this problem and Charise's threats to take the matter to the board, Battler agreed to remove McFudge and Candel from the process.

More peculiar matters began to come to light when the new chief accounting officer had a meeting with McFudge, Candel, and others about the new reporting system. The former president of Deal Club asked him how to move \$165 million from merger reserves into income "creatively" for fiscal 1998. It was also revealed that earnings had actually been increased by \$100 million using the same trick in 1997. When Charise heard this news, he began to fear he would have to restate earnings with all that implied for the stock price which he had so assiduously worked to

support through his good relations with Wall Street. Former Deal Club executives tried to explain the matter away, and Fiddle & Fakit assured Charise that the restatement would not be necessary.

The biggest bombshell, however, exploded a few weeks later at a routine budget meeting when two mid-level Deal Club executives revealed that Deal Club's growth story was a complete fiction and that all the numbers had been fabricated. The story, as it came out that day and over the next few weeks, showed that under instructions from McFudge and Candel, more than 20 controllers at 17 of Deal Club's 22 divisions had committed fraud by creating \$511 million in phony pretax income that translated into a one-third increase in earnings for the three years ended fiscal 1997. The fraud had grown each year until 1997 net income was 61 percent fiction. As the former Deal Club executives told the story, McFudge and Candel had said the bogus numbers were necessary to meet analysts' forecasts.

When Charise publicly announced that Deal Club's 1997 earnings were being restated downward by \$115 million, Fabulous Deals' stock price plunged to \$19 from \$36 to reduce market capitalization by \$14 billion. At 108 million shares traded, the volume was the largest one-day turnover for any stock in the history of the New York Stock Exchange (NYSE) up to that time. Three shareholder lawsuits had been filed by the end of the day and about 70 more followed. By the time the stock price finally bottomed at \$7.50, more than \$29 billion in market capitalization had been vaporized.

Conclusion and Analysis

The scandal seems to have been driven by the perception by McFudge, Candel, and others that meeting analysts' expectations and maintaining the upward momentum of the P/E and stock price were more important than accepting the ups and downs, the good years and bad, of business and the impact such developments implied for the stock price. Externally perceived performance became more important than reality. The extent of Bill Battler's involvement remains an open question.

The scandal was only able to go on as long as it did because of the failure of Fiddle & Fakit to detect accounting irregularities of this magnitude. In the first three quarters of 1995, 1996, and 1997, the unaudited financial statements were doctored by adjusting revenues upward and expenses downward at the largest Deal Club subsidiary. These adjustments were \$31 million, \$87 million, and \$176 million, respectively. If the auditors had looked at these interim statements, they would have seen a pattern of unsubstantiated changes to income and expense items. At year-end, before Fiddle & Fakit arrived to do the audit, these irregularities were reversed and the fictitious earnings replaced by earnings converted from cookie-jar reserves. Fiddle & Fakit were so lax in their work that they failed to question this use of reserves. They even allowed a \$25-million transfer from reserves to be classified as "immaterial." Acquisition reserves were even used to pay for \$597,000 in expenses requested by Bill Battler for the operation of his private plane in years *prior* to the acquisition. These expenses, assuming they were properly reimbursable, should have been classified as operating costs.

This failure is even more troubling since Fiddle & Fakit had had the Deal Club account for years and McFudge, Candel, and others were former Fiddle & Fakit employees. Bill Battler had even fought to retain Fiddle & Fakit as auditors after the merger. Fiddle & Fakit paid \$335 million to settle a shareholder class action suit and is embroiled in other suits involving Fabulous Deals and Bill Battler. Fabulous Deals has agreed to pay \$2.85 billion in class action settlements.

10.3.3 Cost Shifting to Improve Current Operating Results

If management desires to improve earnings fraudulently, it can remove expenses from the current-period income statement to make operations appear more profitable. There are two ways in which expenses incurred by a firm can be shifted; they can be moved to the:

1. Balance sheet to be brought onto the income statement at a future period
2. Income statement of another related entity to remove the cost altogether

Shift to the Balance Sheet

The matching principle, which states that the timing of expenses should be related to the timing of revenues,²⁹ restricts the first shifting method. Under this principle, if the cost was incurred to earn revenue in the current period, as a general rule, the cost should be charged to that revenue in the current period. There are some expenses that offer the prospect of providing benefits to future periods, and management may attempt to justify capitalizing, and then amortizing them into income over future periods. This practice, however, may run afoul of specific accounting guidance and, if management intentionally ignores this guidance, it will create fraudulent financial statements. For example, to meet earnings projections, management may begin capitalizing the salaries of marketing personnel on the argument that the work performed by those personnel will benefit future-period sales.

Although there may be some conceptual merit to the argument, capitalizing sales personnel salaries runs directly counter to an example contained in FASB Concepts Statement No. 6, *Elements of Financial Statements*, paragraph 148, because it is difficult to determine the amount and length of time of future benefits.³⁰ Implementing the principle of conservatism, FASB Concepts Statement No. 6 states that such expenditures are “recognized as expenses in the period in which they are incurred because the period to which they otherwise relate is indeterminable or not worth the effort to determine.”³¹ Finally, even if capitalization is justified, the manipulation of financial statements may also occur when management switches from currently expensing costs to capitalizing them without proper disclosure. Failure to disclose may cause readers of financial statements to believe that profits have

²⁹ See FASB Concepts Statement No. 6, *Elements of Financial Statements*, paragraphs 145–149 for a summary of the issues regarding expense recognition.

³⁰ There is an exception that allows the capitalization of sales commissions paid to agents selling insurance policies under FASB Statement No. 60, *Accounting and Reporting by Insurance Enterprises*, paragraph 28 *et seq.* In the case of insurance sales, though, actuaries are able to establish estimates of how long those policies will remain in force and thereby generate premium income to the insurance carrier. Those estimates then provide a reasonable basis for amortizing the commissions and other acquisition costs over future periods.

³¹ FASB Concepts Statement No. 6, paragraph 148.

improved in the year of the policy change compared to previous periods when, in reality, the improved operating results may be solely attributable to shifting expenses to the balance sheet.

The Asset Quality Index, described in the discussion entitled “Quantitative Predictors,” below in section 10.4.1, is one of the early warning signs of this type of manipulation. This index looks at the percentage of noncurrent assets to total assets for the current year over the previous year. If the index is greater than one, management has increased the percentage of noncurrent to total assets. This type of behavior is frequently associated with the sale of stock, especially during the period leading up to seasoned equity offerings for a company whose stock is already publicly traded. (A seasoned equity offering consists of the sale of new, additional shares by a public company). A survey of academic research also found that management frequently got away with this type of manipulation.

Two recent studies provide evidence that managers manage earnings at the time of seasoned equity offerings (Rangan, 1998; Teoh, *et al.* 1998). It is well known that shares of firms that make seasoned equity offerings (SEOs) underperform the market in the years following the offering. These two papers show that:

1. The reported earnings of firms that make SEOs are unusually high at the time of the SEO.
2. These high reported earnings are attributable to unusually high accruals (including “discretionary” accruals).
3. These firms’ earnings performance is unusually poor in the years following the SEO.
4. There is a strong association between the extent of earnings management and subsequent stock price performance. Shares of firms with the highest accruals at the time of the SEO tend to perform worse in the years after the SEO than shares of other firms.

This evidence is consistent with the view that investors do not “see through” earnings management at the time of the SEO. Rather, as time passes after the SEO and the earnings management becomes apparent through subsequent earnings disappointments, the overpricing reverses and these stocks underperform the market.³²

Clearly, the incentive is to create a short-term illusion of higher profits to sell stock at an inflated price.

Shift to Related Entity

Sometimes fraudsters can deceive by moving costs from one entity to another under common control. This is useful to the fraudsters in situations in which investors or analysts are looking intently at the performance of a certain business segment, and management wants to show rising earnings in that segment to give the illusion of significant future growth. Events similar to this played out in the W.R. Grace case,³³ although that

³² Dechow and Skinner, *op. cit.*

³³ In the Matter of W.R. Grace & Co., Accounting and Auditing Enforcement Release No. 1140 (June 30, 1999). This case also raised materiality issues in that the manipulation of subsidiary earnings was less than a rule-of-thumb threshold of 5 percent of consolidated Grace earnings. But since the SEC found that management placed increased importance on the subsidiary’s earnings, the SEC determined that the manipulation was material.

management also used reserves as the tool to shift expenses. As outlined above, in June 1999, the SEC brought a managed earnings case against Grace for manipulating the reported earnings of its primary health care subsidiary, National Medical Care, Inc. Management had established reserves for unanticipated health care reimbursements and used those reserves in subsequent periods to reduce expenses and show a steady growth rate in its health care subsidiary. However, there were no liabilities to justify the reserves, which consequently were not in conformity with GAAP. Fraudsters may also want to improve a subsidiary's earnings in order to enhance it for sale by shifting costs to the parent or to affiliates and by using reserves, as illustrated in the example of Grace.

Another example of cost shifting was the previously discussed Livent case.³⁴ This scheme operated from 1990 through 1998. There were three areas of expense manipulation:

1. Livent transferred preproduction costs for the shows to fixed assets, such as set construction.
2. Livent removed certain expenses and related liabilities from the general ledger.
3. Livent transferred costs from one show currently running to another show that had not yet opened.

Livent shows that this type of cost shifting is especially hard to detect. Business downturns usually bring these schemes to the surface because, if the company overall is suffering, there is no place to hide the additional costs. To try to detect cost shifting before a downturn, auditors would be well served to look for credits appearing in expense accounts. Such credits may indicate that the entity incurring the cost accrued the expenses on its books as debits, and then transferred the expenses out with offsetting credits. It is not safe, however, to assume that the subsidiary incurring the expense initially recorded it as such. There may be a special reserve or liability account on the balance sheet set up to record the initial debits with the transfer credits appearing later. As the expenses are being booked, significant debit balances in the liability account will grow until the transfer is made. Such debit balances in a liability account should stand out. Also, if the transfers take place over time, there is likely to be some correspondence spelling out the procedures, especially if the initial debit is to an unusual account such as a liability reserve.

10.3.4 Recognizing Fictitious Revenues

The COSO Report found that more than half the financial reporting frauds in the period from 1987 to 1997 were attributable to overstating revenue. Revenue recognition issues have occupied the accounting profession for many years as well. In 2006 revenue recognition based audit deficiencies remain amongst the most noted deficiencies by the PCAOB.³⁵ In 1984, the FASB issued FAS Concepts Statement No. 5. That statement set out two basic requirements for recognizing revenue:

³⁴ In the matter of Livent, Inc., Accounting and Auditing Enforcement Release No. 1095, January 13, 1999.

³⁵ While this is true for large and small firms, the AICPA prepared a report entitled *Small Firm PCAOB Inspection Deficiency Analysis* in May 2006. This report analyzed the audit deficiencies referenced to firms with fewer than 100 public clients. Of the 242 reports examined, 43 revenue recognition issues were identified, more than twice the number of the next most frequent deficiency.

- a. *Realized or realizable.* Revenues and gains generally are not recognized until realized or realizable. Revenues and gains are realized when products (goods or services), merchandise or other assets are exchanged for cash or claims to cash. Revenues and gains are realizable when related assets received or held are readily convertible to known amounts of cash or claims to cash. Readily convertible assets have (i) interchangeable (fungible) units and (ii) quoted prices available in an active market that can rapidly absorb the quantity held by the entity without significantly affecting the price.
- b. *Earned.* Revenues are not recognized until earned. An entity's revenue-earning activities involve delivering or producing goods, rendering services or other activities that constitute its ongoing major or central operations, and revenues are considered to have been earned when the entity has substantially accomplished what it must do to be entitled to the benefits represented by the revenues. . . .³⁶

The staff of the SEC identified a long list of additional accounting pronouncements dealing with revenue recognition, including:

- FASB Statement No. 13, *Accounting for Leases*
- FASB Statement No. 45, *Accounting for Franchise Fee Revenue*
- FASB Statement No. 48, *Revenue Recognition When Right of Return Exists*
- FASB Statement No. 49, *Accounting for Product Financing Arrangements*
- FASB Statement No. 50, *Financial Reporting in the Record and Music Industry*
- FASB Statement No. 51, *Financial Reporting by Cable Television Companies*
- FASB Statement No. 66, *Accounting for Sales of Real Estate*
- APB Opinion No. 10, *Omnibus Opinion—1966*
- ARBs No. 43 and No. 45, *Long-Term Construction-Type Contracts*
- SOP No. 81-1, *Accounting for Performance of Construction-Type and Certain Production-Type Contracts*
- SOP No. 97-2, *Software Revenue Recognition*
- Emerging Issues Task Force (EITF) Issue No. 88-18, *Sales of Future Revenues*
- EITF Issue No. 91-9, *Revenue and Expense Recognition for Freight Services in Process*
- EITF Issue No. 95-1, *Revenue Recognition on Sales with a Guaranteed Minimum Resale Value*
- EITF Issue No. 95-4, *Revenue Recognition on Equipment Sold and Subsequently Repurchased Subject to an Operating Lease*³⁷

In SAB No. 101, the SEC set out its interpretation of the above literature and concluded that:

The staff believes that revenue generally is realized or realizable and earned when all of the following criteria are met:

- a. Persuasive evidence of an arrangement exists
- b. Delivery has occurred or services have been rendered

³⁶ FASB Concepts Statement No. 5, paragraph 83 (footnotes omitted).

³⁷ SEC SAB No. 101, Topic 13, A.1.

- c. The seller's price to the buyer is fixed or determinable
- d. Collectibility is reasonably assured.³⁸

With regard to a fixed or determinable selling price, the SEC staff amplified its position by looking to SOP 97-2 which defines a *fixed fee* as a "fee required to be paid at a set amount that is not subject to refund or adjustment."³⁹ Even though SOP 97-2 deals with software revenue recognition, the staff believed that the requirement of not being subject to refund or adjustment was applicable to all transactions. If the buyer retains a right to a refund of the purchase price, then collectibility *cannot* be assured. Indeed, it would be difficult to meet the FASB Concepts Statement No. 5 realization test if the cash or other payment tendered was subject to refund at the buyer's discretion. Yet, refund arrangements are a common area for revenue recognition fraud.

If company management wishes to inflate revenues by booking fictitious sales, in all likelihood one or more of the SEC's conditions will have been violated:

1. Lack of an agreement
2. Nondelivery
3. No fixed price
4. Receivables are not collectible

Lack of an Agreement

As the reporting quarter draws to an end, companies straining to achieve a revenue target face pressure to close sales by the last day. That pressure may lead to the fraudulent booking of premature or nonexistent sales. In the rush to close transactions by a certain date, sales personnel may represent to management that there is an oral agreement with a customer when, in fact, there is none. For this reason, the SEC standard requires "persuasive evidence," which generally means some written documentation from either the buyer or a third party such as a purchasing agent. If a company requires a written agreement in order to credit a salesperson with a sale, the agreement might be held up, perhaps under review in the buyer's legal department, at the end of the quarter. The salesperson may then represent (perhaps accurately) that the buyer has signed off on the sale; without a signed contract, however, recognition of the sale violates the company policy. Such a policy is put in place to assure the company conforms to GAAP. Violating that policy causes a GAAP violation if, in footnotes to the financial statements or elsewhere, management represents that sales are not recognized without a written agreement.⁴⁰ Such a violation might also point to an internal control issue for the auditors to consider.

Good sales cutoff procedures can generally detect lack of proper agreements. If written agreements are fabricated, detection is much more difficult. The random sampling of orders

³⁸ *Ibid.* (footnotes omitted).

³⁹ SOP 97-2, paragraph 8.

⁴⁰ See SAB No. 101, *Revenue Recognition in Financial Statements*, Question 1. The hypothetical situation posed in the SAB actually stated the normal and customary business practice was to obtain written agreements and did not mention the existence of a company policy to obtain written agreements. The staff's position was that companies could not book as revenue sales lacking written agreements when the normal and customary business practice for the industry was to obtain written agreements.

booked as revenue near the end of a quarter should provide a list of customers to call to verify that documents are authentic. For a document fabrication scheme to succeed over several quarters or years, however, the fabricated agreements must be replaced by authentic agreements and real sales or there will be significant reversals of prior period sales. Therefore, auditors can compare, perhaps on a random basis, contracts on file at the end of a given reporting period with contracts on file for the same transaction at later period. If the original (fake) contract has been switched, there probably was an attempt at fabrication. Conversely, if the authentic document does not appear, the sale may never have been completed, in which case there would be a reversal in the subsequent period. Numerous such reversals would point to revenue recognition problems.

Nondelivery

What constitutes delivery varies from industry to industry but generally occurs when title and risk of loss pass to the buyer. Delivery of some products require shipping documents that provide an auditable paper trail. Delivery of products such as software, though, may occur over the Internet at near instantaneous speed. But even here there should be some documentation or electronic receipt verification.

Attempts at achieving fraudulent deliveries usually involve some person or entity willing to hold the product until such time as its sale can be arranged. As part of the fraud scheme, the recipient executes documents or emails that appear to confirm delivery. This recipient is sometimes part of the scheme or can be a customer who inadvertently accepts delivery before completing the sale. The latter may be easier to detect because customers receiving products before they are wanted tend to complain to company management. The third-party recipients who park goods temporarily may be harder to detect but usually require some payment for their services. Payment may come in the form of above-average discounts if the third parties resell the products over future periods or there may be special terms allowing for product returns. An analysis of average product selling prices may point to one customer who stands out from the rest by receiving better deals. If returns from a given customer are abnormally high, that fact, too, may indicate special arrangements, especially if the returns occur in a later reporting period. If one customer receives such favorable treatment, the auditor should make additional inquiries as to why. In addition, delivery schemes involving resellers typically become more apparent when other resellers cannot sell the product as expected because of a change in market conditions. If a reseller is still taking substantial deliveries of product while many others are experiencing sales declines, the auditor should attempt to understand why that reseller's channels of distribution are clear when others are blocked.

No Fixed Price

Sometimes prices are difficult to determine, particularly if the product is to be combined with other products before being sold to an end user. Such sales may involve a royalty payment that is a function of the selling price. It would be inappropriate to book anticipated future royalties as current revenues until the amount of those royalties becomes fixed upon ultimate sale. Minimum royalties, however, may be booked when they become due. Fraud occurs when royalties are recognized on fictitious or anticipated ultimate sales. Such royalty arrangements, however, typically require the royalty payor to report to the royalty recipient

the quantity of ultimate sales on a periodic (usually quarterly) basis. This permits an accounting of the final sales that can be used to verify reported royalty income.

The more deceptive form of fraud used to circumvent the fixed price requirement is the clandestine use of side letters or arrangements that allow for refunds or discounts at the buyer's option or in certain circumstances. Under tight market conditions or perhaps because the product is new and untested, it may be necessary to use these side letters to make a sale. The most likely candidates for this type of fraud are sales personnel with some discretion and authority such as divisional managers and above. Implementation of such a scheme requires their authority to alter records or invent excuses should the buyer exercise his rights under the side agreement. As a general rule, side letters are the result of some type of internal control failure when the divisional manager is able to effect economic outcomes and alter accounting records. These side letters are quite hard to detect because the buyer usually realizes he is receiving a special deal and does not want to publicize it. Of course, the fraudsters in the selling company will attempt to keep such agreements secret.

These schemes must come to the surface when the buyer exercises his rights under the agreement. A more senior member of management is usually involved to cover up the refund with a fabricated reason or another transaction. Nevertheless, there is usually some documentation of the refund if corporate controls are in place. The auditor who suspects the existence of side letters can certainly look for refunds and discounts that are out of the ordinary. Keep in mind that the customer probably demanded the right to obtain a refund or discount in the course of negotiations for the sale. To catch the existence of side letters before refund demands are made, a suspicious auditor may review sales files for correspondence, notes, or other evidence of such demands from the prospective customer. If installing the product requires personnel such as engineers, those personnel not reporting to the fraudsters may know details of the side agreement but innocently believe there is no issue to report to senior management. It is also likely that if fraudsters used side letters with one customer, there might be side letters with other customers as well.

Receivables Are Not Collectible

Financially weak firms may not pay their bills. To prevent sales to firms in poor financial condition, some type of customer approval process independent of the sales function needs to be in place to assess customer health, especially if the customer is placing large orders. This review function should be integrated with the approval process for customer refunds and discounts to prevent the implementation of side letters, which also affect collectibility, as discussed above. From an auditor's point of view, an unusual concentration of orders from small or distressed customers, particularly near the end of a reporting period or a sales campaign, should raise concerns.

Buffalo Chips, Inc. Case Study

When the accounts receivable accountant tripped over a box on the Buffalo Chips loading dock in October 1993, she knew something was wrong at the company. From the packing slip, she recognized a \$250,000 order she had invoiced in the previous quarter. As it turned out, booking revenues before products were shipped

was only one of the fraudulent accounting practices used at Buffalo Chips to deceive its auditors and investors.

In 1979, Buffalo Chips was a small Silicon Valley startup with a promising patent for semiconductor chips but had burned through its venture capital without bringing a product to market. Soon after Jim Johnson, a former engineer with defense and electronic-component firms, took over the company for no salary but 20 percent of the stock, the company became cash positive and had sales of nearly \$2 million. Jim soon acquired the rest of the company. Mel Leeds was brought aboard in the accounting department and quickly became CFO. Johnson and Leeds had different personalities but shared a taste for expensive homes, cars and golf clubs.

Johnson had built up sales in specialty resistors and capacitors assembled on silicon chips by trading on his old connections in defense and electronics. Now he was successful in winning contracts to supply components to major American companies. Production capacity was increased by taking the company public and purchasing a microchip manufacturing facility from another producer. By 1987, revenues topped \$30 million and 215 people were on the payroll. As the company grew, management was under relentless pressure from analysts to expand the P/E multiple and raise the stock price with a string of quarterly earnings increases.

Johnson was an overbearing manager insisting on making decisions down to the level of \$25 purchases of office equipment. The turnover of senior management was high with the result that the average level of executive experience declined. As early as 1987, product ordered for subsequent quarters was being shipped to meet current revenue objectives. Phony packing documents were created and product was stored onsite in empty offices and offsite in garages and elsewhere. The external auditors forced the company to restate 1989 earnings to correct "revenue and expense cutoff errors" and recommended Leeds be fired. Johnson kept him on, however, but changed his title and some of his responsibilities, then raised his salary. In 1992, a new president tried to correct the situation but without success. He resigned after five months. The new CFO, Mario Innocente, who had been unemployed for nearly a year before joining Buffalo, did not.

Johnson told the executive in 1993 he wanted to see double-digit revenue growth every quarter because he wanted to attract new capital from a prospective partner and could raise another \$40 million through a secondary offering if the stock price rose from its current \$11 to \$20. In 1994, Banzai Alloys bought 10 percent of Buffalo, promised an infusion of \$24 million, and agreed to sell Buffalo's products overseas. The stock price jumped to \$21.25 per share and the value of Johnson's holdings increased to \$40 million. Leeds sold some of his holdings and netted more than \$500,000. In the meantime, company executives booked bogus sales to both real and fictitious companies, treated product returns as sales, and produced false financial reports to deceive auditors, bankers, and their own board of directors. False annual reports and 10-Q and 10-K filings were signed off and misleading information was given to analysts.

Accounts receivable was now bursting with phony sales. To cover up, Innocente prepared two accounts receivable reports, one for internal use and the other for the board and investment bankers. The internal report showed that 51 percent of receivables were actually current; the outside report showed 82.4 percent. Even

when a board member questioned the peculiar fact that receivables exceeded quarterly revenues, he was fobbed off with the answer that the Asian distributors had 180 days to pay and thus their receivable could be booked as current. He did not know that Asian sales were booked to distributors who had an unconditional right of return, that is, the products were, in effect, shipped on consignment. Cash collections fell to 25 percent of the quarterly target.

With the books in such bad shape, a secondary offering was now out of the question since the financial statements for the first nine months of fiscal 1994 could not survive an audit. It was initially suggested that \$3 million in uncollectable receivables be written off but, toward the end of the fourth quarter, the amount had ballooned to \$8.3 million. In consultation with Leeds, the new CFO decided to allocate the write-downs to product returns and bad debts. The writeoff would be offset by recognizing revenues of \$7 million from Banzai as nonproduct technology sales.

When the figures were published, analysts became suspicious of the \$8.3 million and \$7 million figures and began to ask questions about the accounting for receivables. The stock price dropped to \$13 from \$22 in one day and several shareholders filed lawsuits. A press release from the board of directors explained the accounting irregularities and the stock continued its downward path to \$6. Johnson, Leeds, and Innocente departed and new auditors restated a \$7.7-million profit as a \$16.6-million loss. Johnson and Leeds were indicted on the criminal charges of fraud and insider trading and received sentences of 36 and 32 months respectively and had to pay a fine of \$100,000 each. Johnson had to surrender his 1.5 million shares of Buffalo Chips valued at about \$2.5 million in restitution to shareholders.

Conclusion and Analysis

How did this happen? First of all, the company was led by Jim Johnson, an ambitious and overbearing CEO, who found a compliant CFO in Mel Leeds. This proved to be a potent mix of personalities. Johnson had indeed shown great drive and competence in turning the struggling start-up company into a profitable concern under his leadership. But as the company grew and went public in order to expand, it came under the scrutiny of Wall Street analysts. Management was now under pressure to meet analysts' earnings expectations. It was also necessary to keep revenues and earnings up in order to attract a new partner and raise additional capital through a secondary offering. Unfortunately, real revenues and earnings could not support these ambitions.

As revealed in court, the company concocted nearly a dozen revenue recognition schemes. These included recording revenue on:

- Sales shipped in subsequent quarters
- Sales shipped before the customer agreed to accept delivery
- Sales shipped to customers without receiving an order. These sales were not reversed when the goods were returned

- Shipments held at the freight forwarder or stored offsite, sometimes at the homes of employees (Company shipping staff had deals with the forwarders to sign off on the paperwork as if real deliveries had been made.)
- Sales shipped to fictitious customers
- Sales shipped to customers with unconditional rights of return, that is, goods were shipped on consignment and recorded as sales

This scheme was concealed by the creation of a false accounts receivable report for the board of directors and investment bankers. The bankers and the board were deceived by the explanation that the high levels of receivables reflected large shipments made at the end of a quarter. They were not told that some sales were to customers with unconditional rights of return. After the whole scheme collapsed, forensic auditors discovered that Buffalo Chips had recorded \$38 million in phony revenue.

The SEC later alleged the auditors had recklessly failed to comply with generally accepted auditing standards (GAAS) and had exercised improper professional conduct in the audit of accounts receivable, inventory, and property. Accounts receivable were overstated by \$10.6 million or 162 percent; inventory was overstated by \$10.2 million or 197 percent; property was overstated by \$3.0 million or 40 percent. When restated, accounts receivable reduced net income by \$9.7 million, inventory reduced net income by \$9.3 million and property and equipment reduced net income by \$2.7 million. The SEC alleged that the auditors had failed to exercise appropriate professional skepticism, obtain competent evidential matter or properly supervise audit personnel. For example, the auditors did not examine the writeoff of one-third of the accounts receivable balance, an act that should have signaled to the auditors that a material misstatement was possible. The SEC eventually brought Rule 102(e) proceedings against the engagement partner and manager on Buffalo Chips' 1994 audit.

Datatronix Inc. Case Study

Datatronix is a multinational database software company with shares traded over the counter. The company described itself in its press releases and advertising literature as the fastest growing company in the database software industry. In reality, the company was showing increased revenues and earnings by using a wide range of fraudulent accounting practices to produce the numbers on its own financial statements as well as those filed with the SEC. For the fiscal years 1994 to 1996 and for the first quarter of fiscal 1997, Datatronix salespeople, managers, and others fraudulently inflated quarterly and annual revenues and earnings in violation of GAAP. The violations included:

1. Backdating license sale agreements
2. Entering into side agreements granting rights to refunds and other concessions to customers
3. Recognizing revenue on transactions with reseller customers that were not creditworthy

4. Recognizing amounts due under software maintenance agreements as software license revenues
5. Recognizing revenue on disputed claims against customers

Managers later explained that the frauds occurred when the performance numbers failed to meet the internal revenue and earnings objectives which in turn had been established in order to meet analysts' forecasts. As the quarterly cutoff dates approached, the sales department tried to close as many sales as possible to meet the quarterly objectives. If license agreements could not be signed before the end of the quarter, they were frequently signed later and backdated to the quarter in violation of both GAAP for revenue recognition and written internal policy. This practice was possible because of slack internal controls. Salespersons, the very people under pressure to produce good revenue figures, were responsible for overseeing the dating of signatures on agreements. In one known case, an agreement was accepted a month after the end of the quarter.

Written and oral side agreements were also common means of juggling revenues and earnings. The agreements had a wide variety of provisions:

1. Allowing resellers to return and to receive a refund or credit for unsold licenses
2. Committing the company to use its own sales force to find customers for resellers
3. Offering to assign future end-user orders to resellers
4. Extending payment dates beyond twelve months
5. Committing the company to purchase computer hardware or services from customers under terms that effectively refunded all or a substantial portion of the license fees paid by the customer
6. Diverting the company's own future service revenues to customers as a means of refunding their license fees
7. Paying fictitious consulting or other fees to customers to be repaid to the company as license fees

These side letters allowed the sales staff to "park" software licenses with resellers and bring them into revenue without actually having sold anything to an end user, indeed, without having even found an end user. The most notorious reseller involved in this scheme was known as the "bank" and the "virtual warehouse." This reseller was, however, not very effective at moving Datatronix products. Nevertheless, it entered into purchase agreements for \$9.5 million in software licenses in fiscal 1995 but sold only \$2.8 million in that year. In the first half of fiscal 1996, it entered into purchase agreements for an additional \$5.9 million. During the *whole* of 1996, it sold only \$6.2 million of the remaining \$6.7 million in licenses purchased in 1995 and *none* of the \$5.9 million in licenses purchased in the first two quarters of 1996.

Datatronix created these sales through a series of side letters inducing this reseller to enter into quarter-end purchase agreements. The Datatronix sales staff offered the bait of allowing the reseller to book a sale *they* were negotiating with an end user. The same arrangement with the same end user was offered to two other resellers. The result allowed Datatronix to book the same end-user sale three times through the three resellers.

Other side letters allowed resellers to cancel purchase agreements while Datatronix continued to recognize the original sales as revenue. One agreement allowed a reseller to cancel \$6 million in licensing agreements in the third quarter of 1996. This figure represented 14 percent of pretax income for that quarter. Another side letter permitted a different reseller to cancel \$6.4 million or 11 percent of pretax income in the fourth quarter.

Additional GAAP violations occurred when service agreements were recognized as license sales and taken fully into revenue in a single quarter instead of being taken in ratably over the life of the contract. In the 1996 fourth quarter, three service agreement renewals totaling \$11.2 million or 25 percent of pretax income for the period were treated as license sales and taken into revenue.

In the last quarter of 1995, Datatronix invoiced a customer for \$5.4 million claiming the customer had used more copies of Datatronix software than had been permitted under its license agreement. Finance staff thought the claim would be settled at a discount to the list price; the customer was told the \$5.4 million could be applied against future purchases. The claim was settled in the first quarter of 1996 for \$3.8 million but Datatronix improperly recognized the claim as fourth-quarter 1995 revenue and increased pretax income for the period by 13 percent. The remaining \$1.8 million should have been written off in first-quarter 1996 but was instead improperly characterized as an unbilled maintenance fee receivable that was eventually written off over the last three quarters of fiscal 1996.

Revenue was recognized from end users with whom no contract had been signed and from whom no formal acceptance had been received. Policies for recognizing creditworthiness were disregarded and revenues were booked from undercapitalized and new customers. Both these actions are in clear violation of the GAAP that clearly states that "until persuasive evidence of the agreement exists and an assessment of the customer's creditworthiness has been made," no revenues can be recognized. Such improperly recognized revenues amounted to \$3.3 million in the 1996 first quarter, \$9.1 million in the second, and \$8.2 million in the third.

At the end of the fourth quarter of fiscal 1996, Datatronix sold \$9.2 million worth of software to a computer manufacturer for resale installed on its computers. Datatronix, however, failed to deliver the software code before the end of the fiscal year. Early in fiscal 1997, Datatronix delivered a so-called "beta" version that did not work on the purchaser's hardware. Usable software was not, in fact, delivered until more than half way through 1997. Revenue from the sale was improperly recognized, however, in the fourth quarter of 1996 and increased pretax income for the period by 13 percent.

In 1996, Datatronix decided to open so-called Megastores where it would team up with hardware providers to sell hardware-software solutions. So-called "partnerships" were formed with hardware providers whereby Datatronix would buy computers for the stores while the hardware providers would buy licensing agreements of equal or greater value than the hardware purchases. The hardware purchasers were also asked to buy licenses for the software installed in the demonstration computers in the Megastores. The hardware purchases and license sales were in cash and structured so the hardware purchase would give the providers cash flow at about the time the license agreement payments were due. All

these transactions were premised on the expectation that Datatronix would absorb the costs of setting up new stores and that the Datatronix sales force would be involved in selling the solution as the hardware providers' salespeople were not familiar with the Datatronix software. Because of the high cost of opening and operating the Megastores, the costs of reselling licensing agreements were going to be high for Datatronix. To cover these costs, Datatronix offered its sales force higher commissions if sales were closed through the hardware providers rather than by Datatronix. Objectives were established for end-user sales to be applied against the hardware providers' outstanding commitments.

Datatronix recognized revenue when the hardware providers agreed to the purchase commitments even though Datatronix itself was paying the costs and expenses of setting up and operating the Megastores and its own sales force was going to do most of the reselling. This arrangement was in clear violation of the GAAP that if "other vendor obligations remaining after delivery are significant, revenue should not be recognized, because the earnings process is not substantially complete."

Datatronix committed these violations of GAAP and included this false information in its interim and annual financial statements. Information was also omitted or misrepresented in these statements and those filed with the SEC. As a result, the company's reports and filings were thus false and misleading.

At the end of March 1997, when the company announced a revenue shortfall, the stock price dropped 34.5 percent to \$9 29/32 from \$15 1/8 and reduced the Datatronix market capitalization to \$1.5 billion from \$2.3 billion. About two weeks after this collapse, auditors began to hear about accounting irregularities in 1995 and 1996. Management realized that if the truth came out there would have to be a restatement and they resisted further investigation by indulging in additional fraudulent behavior for the purpose of limiting the scope of the audit. Over the next few months, nevertheless, more of the story began to emerge and by early September 1997, more than \$100 million in various irregularities had been identified on the previously issued financial statements. On the basis of these revelations, amended 10-Ks and 10-Qs were filed with the SEC.

In the face of the SEC's intention to institute administrative proceedings against Datatronix, the company submitted an Offer of Settlement which the SEC accepted.

Conclusion and Analysis

The root of the problem seems to have been a lack of internal controls strong enough to permit the preparation of financial statements within GAAP. The effect of this lack of controls was magnified by an organizational structure that had important financial people responsible for revenue recognition reporting directly to sales personnel rather than to senior financial management. Salespeople under pressure to produce revenues to support analysts' forecasts were thus able to put pressure on their immediate financial inferiors to recognize revenues not generated in accordance with GAAP.

10.3.5 Improper Disclosures and Material Omissions

Accounting principles require that financial statements and notes include all information necessary to ensure that the financial statements are not misleading. Although management is responsible for disclosure of all material information, the auditor has a responsibility to ensure that management meets its disclosure obligations.

Statement of Auditing Standards (SAS) No. 32, *Adequacy of Disclosure in Financial Statements* (AICPA, *Professional Standards*, vol. 1, AU sec. 431), provides general information about informative disclosures. If an auditor believes management's disclosures are inadequate, appropriate disclosures must be made in the auditor's report, as provided by Statement of Auditing Standards (SAS) No. 58, *Reports on Audited Financial Statements*, (AICPA, *Professional Standards*, vol. 1, AU sec. 508), as amended.

Improper disclosures usually result from the failure to disclose or inadequate disclosure of the following:

1. Liability omissions
2. Significant events
3. Related-party transactions
4. Changes in accounting principle

Liability Omissions

GAAP requires the disclosure of all material liabilities. Typical omissions include the failure to disclose loan covenants or contingent liabilities, such as pending lawsuits. Under FASB Statement No. 5, contingent liabilities must be disclosed if they are reasonably probable and capable of estimation.

Significant Events

Examples of significant events include the introduction of new products and technology, as well as the obsolescence of existing products in inventory. Under GAAP, any significant event that could have a material effect on the financial statements must be disclosed.

Related-Party Transactions

Related-party transactions are transactions made with entities that are controlled by the company or have control over the company and may include other businesses, vendors, customers, creditors, or shareholders. Although management is responsible for the disclosure of related-party transactions, the auditor has a specific responsibility to understand the client's business including its relationships with related parties, to evaluate whether management's disclosures are appropriate. FASB Statement No. 57, *Related Party Transactions*, sets forth the disclosure requirements for related-party transactions and provides guidance for the identification and evaluation of such transactions.⁴¹ In the

⁴¹ Beyond the disclosure issues, related-party transactions may also trigger revenue recognition problems. For example, at Learnout & Hauspie, the Belgian maker of speech recognition software, an internal audit revealed that about a quarter of the company's revenues was comprised of revenue recorded from about 30 start-up customers funded with seed money from a venture capital firm linked to the company's founders.

aftermath of Enron, Tyco, and Adelphia, related-party disclosures will receive increased scrutiny.

Significant Accounting Changes

To ensure that financial statements are comparable from one period to the next, any changes to an issuer's accounting policies or procedures must be disclosed. APB Opinion No. 20 describes three significant accounting changes that must be disclosed:

1. Estimates, such as useful lives used to calculate depreciation, bad debt expense, amortization estimates, warranty liability, and earned revenue estimates
2. Accounting principles, such as depreciation, capitalization, or tax methods
3. The accounting entity resulting from mergers, acquisitions, and spinoffs

10.3.6 Special Purpose Entities: The Enron Case

The dramatic collapse of Enron Corp. in October 2001 has brought to light the potential for fraud in "off-balance-sheet" financing vehicles known as *special purpose entities* or SPEs. Enron investors were deceived because some SPEs were not consolidated even after they had ceased to qualify for off-balance-sheet treatment. Employees connected to the management of the SPEs improperly received nearly \$50 million in total from partnerships designed not to meet some legitimate economic objective or to transfer risk but to create financial statements for Enron that would be viewed favorably by Wall Street analysts and the rating agencies and thus support the stock price and lower financing costs. Some transactions were even designed in such a way that GAAP rules that would have permitted keeping assets and debt off the balance sheet but were broken in order to create other illusions of financial health. In the end, the autopsy on the bankrupt showed it had died of poorly thought-out solutions, self-interested employees, inadequate controls, and poor oversight of a business model that tried to push the envelope.

The SPE is a financing method that has been around since the 1980s and is widely used especially in the energy and financial services industries, yet has received no official definition beyond the recognition that it is a class of asset whose members have a number of things in common. In fact, it really does not meet the definition of a business at all in that it is not self-sustaining with a revenue source of its own. An SPE has no independent management or employees; a trustee usually performs the administrative functions required by its creators and primary beneficiaries. It usually takes the legal form of a business trust but can be a limited partnership or even a corporation.

The company that creates the SPE can treat it as an independent external entity for accounting purposes only if an outside investor owns a minimum 3 percent of the equity (the FASB has now changed this to 10 percent) and exercises control. Control here is, obviously, not defined by majority equity ownership but by rights stated in the covenant somewhat on the model of control rights in partnerships. The rest of the capital comes from debt. The company records gains and losses in transactions with the SPE on its income statement but the SPE's assets and liabilities are not entered on its balance sheet.

As its name indicates, an SPE is set up for some special purpose laid out in its trust agreement, charter or articles of formation. This purpose is usually to finance specific assets transferred to the SPE such as trade receivables, loans or securities against which the SPE

issues debt. The creator of the SPE thus gains access to low-cost funds because the lenders' risk is limited by the narrowly defined activities set forth in the trust agreement and the fact that the SPE cannot take on any additional debt. For example, an SPE could be the lessor of a pulp mill through a so-called "synthetic lease" that provides the lessee with tax advantages not available through a conventional mortgage loan.

The unconsolidated SPE is in a certain sense an accounting anomaly. It seems to stand against the long-standing and intuitive presumption that consolidated statements provide a more accurate picture of the company's overall financial condition.

Subsequent to the revelations in the Enron case (following) the FASB issued FASB Interpretation No. 46 in January 2003 (and FASB Interpretation No. 46R in December 2003) to address the accounting by variable interest entities (VIEs). Consolidation of such entities is required by the primary beneficiary of the entity if:

- Its at-risk equity position is insufficient to enable the VIE to finance its activities independently, or
- Its investors lack any one of the following control characteristics:
 - Sufficient equity
 - Residual equity
 - Authority to make decisions

The net effect has been to require a significant analysis of the relationship between entities and force the consolidation of many previously unconsolidated entities.

The Incredible Collapse of Enron Case Study

How Enron abused these features of the SPE is laid out in the *Report of Investigation by the Special Investigative Committee of the Board of Directors of Enron Corp.* commissioned by the Enron board and headed by William Powers, Jr., dean of the University of Texas Law School. The committee's mandate was not to investigate all the causes of Enron bankruptcy but simply to address "transactions between Enron and investment partnerships created and managed by Andrew S. Fastow, Enron's former Executive Vice President and Chief Financial Officer, and by other Enron employees who worked with Fastow." In practice, this meant investigating the causes of the \$544-million after-tax charge and a \$1.2-billion reduction in shareholders' equity in the third quarter of 2001 related to one of the partnerships. The inquiry then broadened to include the two dozen or so transactions between Enron and other partnerships. The result is an unprecedented look at SPEs, and their use and abuse.

Enron was a product not just of the merger of two gas pipeline companies in the late 1980s but also of the deregulation of gas and electricity prices carried out during the administrations of Ronald Reagan and George Bush, Sr. Enron grew by buying an energy asset such as a pipeline or power plant around which it built a wholesale or retail business. Deregulation allowed Enron to start packaging this energy into contracts and trading them like commodities contracts in the futures

market. The promises to deliver in the future at prices fixed in the past were then hedged with derivatives. As Enron grew throughout the 1990s, the range of its commoditized products expanded to include bandwidth on optical fiber networks, newsprint, and many others. By 1998, some 60 percent of its earnings were from businesses in which Enron had not been engaged 10 years earlier and some 30 to 40 percent from businesses entered into within the previous five years. The strategy seemed to be working since \$10,000 invested in Enron stock at the end of 1995 was worth more than \$47,000 by the end of 2000.

Since Enron saw itself as a long-term investor, it made large capital investments in the full realization that earnings and cash flow would not be significant in the short term. New borrowings to produce this growth would put pressure on Enron's already debt-heavy balance sheet that would affect credit ratings and on the cash flow needed for debt servicing. Reduction of its ratings below investment grade would punish its expanding energy trading business. Common-share equity financing at a time when newly acquired businesses were showing only slow earnings growth would result in significant dilution and downward pressure on the P/E multiple.

To escape these constraints yet keep growing, Enron management turned to joint ventures and SPEs in the early 1990s to keep the negative elements off its balance sheet while taking on risks expected to provide significant rewards. With the passage of time, Enron also created partnerships designed to hedge against its so-called "merchant investments," i.e., equity investments in public or private companies, debt, loans, or interests in limited partnerships.

Almost from the outset, Enron's SPEs failed to comply with the 3-percent and control criteria for nonconsolidation. In 1993, Enron formed a joint venture partnership with the California Public Employees' Retirement System (CalPERS) called Joint Energy Development Investment Limited Partnership (JEDI) in which Enron was the general partner contributing \$250 million in Enron stock, and CalPERS was the limited partner contributing \$250 million in cash. Because Enron owned a 50 percent interest, it did not have to consolidate JEDI. Gains and losses were recorded on the income statement and in the footnotes, but JEDI's debt did not appear on Enron's balance sheet.

When Enron wanted to form a \$1-billion partnership with CalPERS in 1997 to be called JEDI II, Enron offered to buy out CalPERS interest in JEDI in the belief that CalPERS would not want to be invested in both JEDIs simultaneously. Nevertheless, Enron wanted to keep JEDI as an unconsolidated entity despite the fact it no longer had a joint partner. To accomplish this, a new limited partner had to be found. A limited liability company called Chewco Investments (another Star Wars name derived, this time, from Chewbacca) was formed to take over the now \$383-million CalPERS interest. Michael Kopper, an Enron employee reporting to the CFO, controlled Chewco through intermediary companies. The \$383 million was redeemed with bank loans guaranteed by Enron. Since no outside party had taken an equity interest or control, Chewco should have been consolidated at this time.

Through a subsequent conversion to a limited partnership and labyrinthine financial arrangements, Enron tried to give Chewco the appearance of an unconsolidated SPE without actually finding any outside equity investors to put up the required 3 percent. Since Chewco failed both the third-party-equity and the control tests for nonconsolidation and JEDI's unconsolidated status depended on Chewco's independence, JEDI should also have been consolidated from the time of the breakup of the Enron-CalPERS joint venture.

Two other partnerships, LJM1 and LJM2, were set up for the purpose of transferring risk away from Enron through hedging transactions. The LJM partnerships were set up with Enron CFO Andrew Fastow as manager and investor along with other Enron employees. Enron entered into more than 20 different transactions with these two entities which resulted in the recognition of significant income for Enron and the displacement of significant losses onto the books of the partnership. Once again, questions arise concerning whether these entities met the criteria for nonconsolidation.

The purpose of LMJ1 (to restrict our discussion to just one of these entities) was to hedge Enron's investment in Rhythms NetConnections, Inc., a privately held Internet service provider. Enron purchased 5.4 million shares at \$1.85 per share for a total investment of \$10 million in 1998. Rhythms went public in April 1999 at \$21 and closed at \$69 at the end of the first trading day. By May, the stock had settled back to about \$55 per share and Enron's investment was worth approximately \$300 million but could not be sold until the end of 1999 because of a lock-up agreement. Since sale of the stock was forbidden and gains and losses in market value were reflected on Enron's income statement, Enron wanted to protect its enormous profits with a hedge. A conventional hedge through a dealer was out of the question, however, since Enron's holding was large and illiquid.

At the same time, the gain in market value of Enron stock had increased the value of forward contracts made through an investment bank to hedge future dilution from its own stock options obligations to its executives. LMJ1 was created to make use of the so-called "embedded" appreciated value of the Enron stock in the forward contracts transferred from Enron to "hedge" the Rhythms holding. The arrangement was flawed by the fact that Enron was attempting to hedge its Rhythm holdings with its own stock when both were at risk of decline. The essence of a hedge is that the price changes of the two assets must be inverse and that a counterparty assumes the opposite risk and will pay (or receive) the difference on closing out the position. Rhythms ultimately went bankrupt with enormous as-yet-uncalculated losses which Enron kept off its income statement at the time. There never was any true third party with a three percent equity position in control of LMJ1.

Conclusion and Analysis

The full story of Enron's involvement in these and other SPEs has yet to be told. Nevertheless, the Powers report, Congressional hearings, and media investigations show patterns of noncompliance not only with GAAP but also with Enron's own internal code of conduct. Once again, as we have seen in previous sections of this chapter, management took the definition of "performance" to mean meeting Wall Street expectations. Support the stock price at all costs! Impatience with slow cash-

flow and earnings growth in the face of the profitable strategies possible for those willing to take the risks in the new world of deregulated energy prices necessitated continuous new financing. The SPE was an obvious alternative as a source of cheap capital for an aggressive company. Unfortunately, when no third-party equity investors were willing to put up the required 3 percent and take control, Enron chose to force the issue and assert its will in a murky area of GAAP interpretation. Fuzzy notions of what constitutes a *third party*, *control*, and even *equity* permitted audacious self-serving managers to exploit the SPE for themselves as well as for Enron.

The role of the auditor in preventing and detecting SPE fraud is difficult to define since the very purpose of the SPE is to keep certain information from being recorded in published financial statements. Given the lack of definition of many issues, the auditor must be prepared to interpret the purpose of accounting practices associated with SPEs and defend that interpretation. The Enron case has revealed the need for greater definition not only of the accounting issues involved but of the related corporate governance issues as well. The auditor should, however, be able to recognize that equity participation by employees of the beneficiary company is suspect on the grounds of both third-party definition and compliance with internal codes of conduct. The presence of hybrid concepts such as *equity loans* must also be suspect as possible fudges to give the appearance of compliance with GAAP. So-called management fees for no obvious work or out of all proportion to normal billing levels plus returns on investment beyond anything possible given the economic behavior of the entity should all draw the auditor's attention to corporate accounting practices.

10.3.7 Methods to Conceal Financial Statement Fraud From Auditors

Financial statement fraud may be detected through the internal audit function or through substantive testing performed by independent auditors. But on occasion, the fraud may go undetected for years. This may result from audit failure or from intentional efforts by management to conceal the fraud from its independent accountants. (Audit failures are discussed in Section 10.6, entitled "Audit Deficiencies and Audit Failures," below.) The following examples illustrate instances in which financial improprieties were not detected because of corporate misconduct, as opposed to audit failure.

In the case of Kurzweil Applied Intelligence, discussed above, senior executives directed subordinates to falsify books and records; to hide, shred, or destroy key documents; forge customers' signatures on audit confirmation letters; and transfer goods improperly held at the off-site warehouse to even more remote locations to avoid detection.

In the matter of Structural Dynamics, the company stored more than \$30 million in product in a warehouse at the Cincinnati airport in order to avoid suspicion by its independent auditors. Much of this product represented bogus revenues recorded for sales to distributors in the company's Far East operations.

In the MiniScribe case, the company created fictitious inventory in transit, transferred nonexistent United States inventory from books in the United States to the books of its Far East subsidiaries, shipped boxes of bricks labeled as disk drives to distributors, repackaged accumulated scrap previously written off and counted it again as inventory. They also

received raw materials into inventory without recording the accounts payable liability. To conceal the inventory shortfall, employees broke into auditors' trunks to obtain copies of inventory items test-counted by the auditors in order to inflate other high-value inventory items not sampled by the auditors.

In the Sensormatic matter, the company turned back the computer clock that dated and recorded shipments in order to prematurely recognize revenue on shipments made past the end of the quarter. When shipping documents were inspected by the auditors, the ship date appeared to be before the quarter-end, when in fact, shipment occurred after the quarter had closed.

In the matter of Sahlen & Associates, the company supplied its auditors with customer addresses that were, in reality, post office boxes opened by the Company's employees. After the accounts receivable confirmations were sent out, the employees flew around the country to the customer destination, forged the customer signature on the audit confirmations, and locally mailed the forged confirmation back to the auditors without exception.

By being alert to the types of methods previously employed to conceal accounting irregularities, accountants and independent auditors may design appropriate procedures to avoid being duped by such chicanery.

10.4 PREDICTORS OF FINANCIAL STATEMENT FRAUD

Faced with the apparent pervasiveness of earnings and balance-sheet falsification, the problem for the auditor is to find any warning signs suggesting the risk of fraud may be present. A number of recent studies (to be discussed in more detail below) have suggested a group of indicators which, when taken together, give the generic profile of a company at risk of fraud.⁴²

The most typical fraud company is not listed on any of the major public stock exchanges. It has assets below \$100 million and is experiencing losses, barely breaking even or reporting a small profit. The *trend* of net income is *not* an indicator since fraud can be committed to hide losses or preserve profits. Internal audit controls are weak or nonexistent. This can be attributed in part to the total absence of an audit committee or the presence of a weak one made up of financially unsophisticated directors meeting as infrequently as only once a year. More than 50 percent of the board of directors are insiders or "gray" directors, i.e., members with a large equity ownership or family, business, or other connections to the company or its board members. Few directors are on the boards of other companies and therefore the level of general business experience on the fraud company's board is often quite low. Officers frequently hold incompatible positions such as CEO and CFO simultaneously. Finally, there usually is a change of auditor for the fraud period.

⁴² This portrait is drawn from Dechow and Skinner, and Levitt and COSO cited above, and important reports by the NYSE/NASD to be cited and discussed in Section 10.4.2, entitled "Qualitative Predictors, below.

10.4.1 Quantitative Predictors

Messod D. Beneish, an associate professor at the Kelley School of Business, Indiana University, has tried to develop quantitative fraud warning signs by analyzing a series of ratios which might be used as predictors when seen as a pattern of irregularity on the books of a given company.⁴³ This model would distinguish manipulated from unmanipulated earnings within the definition of earnings manipulation as a violation of GAAP. Beneish studied 74 companies identified as earnings manipulators by the SEC or the media for the period 1982 through 1992.

Characteristics of Sample and Control Companies

The typical manipulator of Beneish's study was a young, rapidly growing manufacturing company. As a group, they were smaller in terms of assets or sales, less profitable, more leveraged, and growing faster than Beneish's control (presumably nonmanipulating) companies but with similar market capitalizations. Companies with poor prospects were more likely to commit financial statement fraud. Earnings manipulation typically occurred by recording fictitious revenues or inventory, unearned or uncertain revenues or capitalizing costs improperly.

TABLE 10.1 CHARACTERISTICS OF SAMPLE AND CONTROL COMPANIES FISCAL YEAR PRIOR TO PUBLIC DISCLOSURE (1982–1992)

| Characteristics | Manipulators | | Nonmanipulators | |
|---------------------------------|---------------------|---------------|------------------------|---------------|
| | Mean | Median | Mean | Median |
| Size (Millions) | | | | |
| Total Assets | \$467.33 | \$43.20 | \$1,140.37 | \$ 95.84 |
| Sales | 469.87 | 53.56 | 1,295.22 | 122.54 |
| Market Value | 323.72 | 74.90 | 813.35 | 64.59 |
| Liquidity/Leverage | | | | |
| Working Capital to Total Assets | 0.26 | 0.28 | 0.30 | 0.31 |
| Current Ratio | 2.54 | 1.83 | 2.54 | 2.11 |
| Total Debt to Total Assets | 0.58 | 0.58 | 0.51 | 0.52 |
| Profitability/Growth | | | | |
| Return on Assets | -1% | 3% | 3% | 5% |
| Sales Growth | 58 | 34 | 13 | 9 |

⁴³ Messod D. Beneish, "The Detection of Earnings Manipulation," *Financial Analysts Journal* (24) September/October 1999, pages 24–36.

Ratio and Index Analysis

Beneish identified a group of financial statement variables that capture actual earnings manipulation or indicate the potential for manipulation. Of that group, the following sections describe the characteristic measures that generate statistically meaningful results.

Days' Sales in Receivables Index

The days' sales in receivables index (DSRI) shows the year-over-year comparison of the annual receivables/sales ratio taken as a ratio. This ratio, like all the other ratios in this study, should be 1:1. If receivables are beginning to become large in relation to sales, fraudulent sales practices may be in place. After allowing for external factors such as a more liberal credit policy that could have resulted in increased sales, an exceptionally large increase in receivables relative to sales might suggest revenue manipulation.

Gross Margin Index

The gross margin index (GMI) shows the year-over-year comparison of gross margins taken as a ratio. If the GMI is greater than 1, gross margins have weakened. Since the year-over-year deterioration of the gross margin is one of the most important signals of worsening prospects for the company, a GMI of greater than 1 is a red flag that financial statement manipulation may be about to occur.

Asset Quality Index

The asset quality index (AQI) shows the ratio of noncurrent assets exclusive of property, plant, and equipment to total assets in any given year. This ratio measures the proportion of assets whose power to produce future earnings is less certain. The higher the proportion of these intangibles to total assets, the greater the risk to future earnings growth. The AQI is the year-over-year comparison of these annual figures taken as a ratio. An AQI greater than 1 indicates that more costs are being capitalized and thus deferred, and the door has been left open to earnings manipulation.

Sales Growth Index

The sales growth index (SGI) shows the year-over-year comparison of sales taken as a ratio. Mere sales growth does not necessarily imply manipulation. But when a young growth company is under pressure from analysts, underwriters, and banks to show continuing sales increases to support the stock price, the possibility of manipulation is definitely present. Any dramatic increase in the SGI should alert the auditor to possible problems.

Total Accruals to Total Assets

The total accruals to total assets (TATA) shows the year-over-year comparison of total accruals and total assets taken as a ratio with total accruals defined as the change in working capital accounts other than cash less depreciation. The presence of higher accruals, that is, less cash, is likely to be associated with earnings manipulation.

Look for the Pattern

Because of the interconnectedness of income and balance-sheet accounts, no single ratio should be taken in isolation as an indicator of manipulation. It is the pattern that counts, both among the accounts of one reporting period and over several periods. The broader the pattern, the greater the likelihood of earnings manipulation. But care should be taken that unusual ratios cannot be accounted for by acquisitions, shifts in strategy, or changes such as improving economic conditions and other normal business events.

TABLE 10.2 MEANS ANALYSIS OF MANIPULATORS AND NONMANIPULATORS IN THE ESTIMATION SAMPLE

| Characteristic Measures | Manipulators Mean | Nonmanipulators Mean | Difference | Manipulators Percentage Increase over Nonmanipulators |
|-------------------------|-------------------|----------------------|------------|---|
| DSRI | 1.465 | 1.031 | 0.434 | 42.1% |
| GMI | 1.193 | 1.014 | 0.179 | 17.7% |
| AQJ | 1.254 | 1.039 | 0.215 | 20.7% |
| SGI | 1.607 | 1.134 | 0.473 | 41.7% |
| TATA | 0.031 | 0.018 | 0.013 | 72.2% |

The findings indicate that manipulators exhibit certain financial-statement characteristics that are detectable and different from nonmanipulators. The year-over-year change in days' sales in receivables, for example, was about 3 percent for nonmanipulators but over 46 percent for manipulators. Manipulators showed an increase of about 42 percent in days' sales in receivables in sales over the average change for the nonmanipulator peer group. The other indices demonstrate similar though smaller increases for manipulators over nonmanipulators. The total accruals-to-total-assets measure, however, was markedly different between the two groups. The TATA measure, which reflects noncash working capital to total assets, probably picked up the increases in receivables that typically accompany revenue manipulation.

These characteristic measures provide a quick and easy means of detecting the possibility of financial statement fraud. They are indicators and do not of themselves prove fraud. Auditors, however, desiring to implement SAS No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 316),⁴⁴ may want to include these characteristic measures in their financial statement analyses. Also, as an internal control, an internal auditor or controller could apply these measures when reviewing financial information from subsidiaries and divisions. An increase in any of the characteristic measures in the magnitude indicated in the above table should trigger additional inquiries. Such inquiries may very well head off an incipient fraudulent scheme.

10.4.2 Qualitative Predictors

Internal Work Environment and Corporate Governance

The board of directors is a group of persons elected by the shareholders to represent them at the highest level of corporate decision making and to monitor the work of management. A report published in 1999 for the NYSE and the National Association of Securities Dealers (NASD) by the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees (BRC) states explicitly that "the board must perform active

⁴⁴ Chapter 1, "Managing the Risk of Fraud," of this *Handbook* discusses the auditor's duty to detect fraud in detail.

and independent oversight to be, as the law requires, a fiduciary for those who invest in the company.”⁴⁵ The board must be committed to the principles of transparency and full disclosure and, one might add, to full compliance with GAAP and the regulations of the appropriate regulatory bodies. If the board understands its independent role, then it is likely the audit committee, a creature of the board, will also do its duty. Companies proven to be earnings manipulators tend to be those with no audit committee or a very weak and compromised one. About a quarter of all companies subject to SEC enforcement action did not have audit committees.

The report sees the role of the audit committee as follows:

The committee’s job is clearly one of oversight and monitoring, and in carrying out this job it acts in reliance on senior financial management and the outside auditors. A proper and well-functioning system exists, therefore, when the three main groups responsible for financial reporting—the full board including the audit committee, financial management including the internal auditors, and the outside auditors—form a “three-legged stool” that supports responsible financial disclosure and active and participatory oversight.

Characteristics of a Good Audit Committee

The BRC made numerous recommendations for the effective working of a good audit committee. Despite the fact that the BRC’s mandate was to make recommendations for the conduct of audit committees of companies big enough to be listed on the NYSE or NASDAQ, many of the principles would apply equally well to smaller, private companies.

The foundation of a good audit committee is the independence of its members. Recent studies have shown a direct correlation between audit committee independence and better oversight resulting in a lower incidence of financial statement fraud. The BRC defines independence as follows:

Members of the audit committee shall be considered independent if they have no relationship to the corporation that may interfere with the exercise of their independence from management and the corporation. Examples of such relationships include:

- A director being employed by the corporation or any of its affiliates for the current year or any of the past five years;
- A director accepting any compensation from the corporation or any of its affiliates other than compensation for board service or benefits under a tax-qualified retirement plan;
- A director being a member of the immediate family of an individual who is, or has been in any of the past five years, employed by the corporation or any of its affiliates as an executive officer;
- A director being a partner in, or a controlling shareholder or to which the corporation made, or from which the corporation received, payments that are or have been significant to the corporation or business organization in any of the past five years;
- A director being employed as an executive of another company where any of the corporation’s executives serves on that company’s compensation committee.

⁴⁵ Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees, 1999. Available at <http://www.nyse.com/> and <http://www.nasdaqnews.com/>.

Building on this foundation of independence, the BRC recommends that for listed companies with capitalization in excess of \$200 million, the audit committee should be composed of a minimum of three financially literate and entirely independent directors. The audit committee should have a charter approved by the full board describing its structure and responsibilities. The outside auditor should be accountable to the whole board of directors. The audit committee should be responsible for the selection of the outside auditors. The audit committee should have a formal written statement from the outside auditor describing all relationships between itself and the company. The audit committee should discuss with the outside auditor all aspects of the effectiveness or lack thereof of the company's accounting practices. Where the board of directors is weak and the audit committee is weak or nonexistent, internal controls are likely to be deficient or lacking altogether.

COSO

The COSO Report *Fraudulent Financial Reporting: 1987-1997—An Analysis of U.S. Public Companies* sought to identify and examine company and management characteristics in corporations involved in financial statement fraud.⁴⁶ The Committee examined about 200 cases (average assets of \$533 million but median assets of only \$16 million) from which it drew a number of generalized conclusions about the governance of fraud companies.

The presence and efficient functioning of internal controls are central to limiting the opportunities for fraud. Unfortunately, the small size of many companies makes them unable or unwilling to spend the money for proper controls or to pay for better trained and more experienced senior executives. These smaller companies are also unlikely to have strong audit committees capable of monitoring the nebulous but important matter of pressure on senior executives to report aggressively to meet investment community expectations or the numbers required to trigger bonuses. The CEO or CFO was involved in 83 percent of the reported fraud cases.

A strong audit committee is an essential element in fraud prevention. Among the fraud companies surveyed, 25 percent had no audit committee and among those that did, 65 percent of the directors were not certified in accounting or had held no accounting or financial positions. At the fraud companies, the committee usually met only once a year. (A pliable, inexperienced, and inattentive board is often the creation of a domineering CEO. Given the fact that in 83 percent of the reported fraud cases the CEO or CFO was involved, the combination of a weak board and aggressive leaders could be an indicator of financial statement fraud.)

The COSO Report confirmed the findings of the BRC mentioned above concerning the need for an independent board of directors. At the fraud companies, about 60 percent of the board members were insiders or "gray" directors, i.e., outsiders with some family, business, equity, or other tie to the company or its management. About 40 percent of the boards had no directors serving on the boards of other companies. Directors and officers owned about one-third of the companies' stock while the CEO/president owned about 17 percent. In about 40 percent of the companies, there were family relationships among the directors and/or officers. About 20 percent showed officers holding incompatible positions such as CEO and CFO.

⁴⁶ <http://www.coso.org/main.htm>

Since the average fraud period was 23.7 months and often started with the misstatement of interim statements, it is important to review the controls surrounding quarterly statement preparation. Because misstatements of accounts often occur near the period ends, internal controls governing the transaction cutoff and asset valuation should be tested.

The Boeing Company adopted recommendations from the 1992 COSO release entitled *Internal Control—Integrated Framework* and came up with a list of criteria for an *unsatisfactory* rating.⁴⁷ These criteria are the following:

1. Control environment criteria are:
 - *Hard controls* are missing or inadequate.
 - There are verified instances of breakdowns or *soft controls*.
2. Risk assessment criteria are the following:
 - Management has not predefined relevant objectives.
 - Such objectives are incompatible with broader objectives.
 - Management has not identified risks relevant to achieving its objectives.
 - Management does not have a basis for determining which risks are most critical.
 - Management has not ensured the mitigation of critical operating risks.
 - Audit tests detect key risks not previously contemplated by management.
3. Control activities criteria are the following:
 - Key control activities are not functioning as intended.
 - Management's risk mitigation strategy is not adequately reflected within control activities.
4. Information and communication criteria are the following:
 - Key metrics are not identified, collected, and communicated.
 - Employees' misunderstanding of their control responsibilities is pervasive.
 - Customer or supplier complaints and disputes are not resolved or remedial action is not undertaken in a timely manner.
5. Monitoring criteria address whether or not management has established a means of determining the quality of the internal control system over time either through independent evaluations or ongoing, structured, and independent process checks.
6. Overall, the ratings of all components should be considered to determine whether controls provide reasonable assurance that management objectives will be achieved. Strength in the internal controls of one component may compensate for a control weakness in another.

10.4.3 A New Fraud Profile (1997–2002)?

The aftermath of the longest bull market in history has revealed that financial statement management at companies many times larger than the median \$16-million company of the

⁴⁷ Dennis Applegate and Ted Wills, "Struggling to Incorporate the COSO Recommendations into Your Audit Process? Here's One Audit Shop's Winning Strategy," *Internal Auditor*, The Institute of Internal Auditors: December 1999, http://www.coso.org/Articles/audit_shop.htm

COSO Report. Whether these multibillion-dollar frauds point the way to a new era of larger and bolder financial statement scandals remains to be seen. The Great Crash of 1929, the end of the Go-Go market of the late 1960s, and the collapse of stock prices in October 1987 also brought enormous scandals to light. These scandals proved to be the exception rather than the rule, however, and were not indicators of things to come.

Table 10.3 lists 13 of the major investigations and financial restatements of this period, together with the nature, period, and amount of the estimated or actual restatement.

TABLE 10.3 MAJOR INVESTIGATIONS AND FINANCIAL RESTATEMENTS

| Company | Nature of Investigation or Restatement | Restatement Period | Restatement/ Error Amount |
|-------------------------|--|---------------------------|---|
| Adelphia Communications | Questionable accounting practices and related-party transactions | 1993–2001 | \$2.3 billion |
| America Online | Improperly capitalized advertising costs instead of expensing in the period incurred; also may have recorded \$45 million in improper payments from third parties in 2000–2002 | 1995–1996 | \$385 million |
| Cendant | Inflated annual income through the misuse of reserves | 1995–1997 | \$300 million |
| Dynegy | “Project Alpha” was a complex transaction that artificially inflated cash flow from operations | 2001 | \$79 million |
| Enron | Corporate executives under investigation for creating and approving transactions designed to improperly keep billions of dollar in losses off the books | 1997–2000 | \$500 million |
| Microsoft | Used reserves, accruals, allowances, and liability accounts to manage earnings | 1995–1998 | \$200 million to \$900 million per year |
| MicroStrategy | Restatement resulting from improper recognition of software revenue in contravention of SOP 97-2 | 1998–2000 | \$66 million |
| Qwest Communications | Under investigation for improper recognition of revenue on sales of fiber-optic capacity | 2000–2001 | \$2.2 billion |
| Rite Aid | Overstated income through unsupported journal entries and fraudulent credits for damaged goods | 1997–1999 | \$1.6 billion |
| Sunbeam | Used cookie-jar reserves, big-bath restructuring charges, and channel stuffing to artificially inflate revenue | 1996–1998 | \$97 billion |
| Xerox | Improperly accelerated revenue from long-term leases of copiers and other office equipment. | 1997–2001 | \$6.4 billion |
| Waste Management | Improperly eliminated and deferred current period expenses to inflate earnings | 1992–1997 | \$1.7 billion |
| WorldCom | Restatement of \$7.1 billion in improperly capitalized operating expenses in 2001–2002; possible overstatement of profits by \$1 billion in 1999 and 2000 through the improper use of reserves | 2001–2002 1999–2000 | \$7.1 billion \$1 billion estimated |

Although not all of these revelations have resulted in fraud charges, some important differences from the COSO profile are evident. Deceptive financial statements occur today in a much wider range of industries than technology, health care, and financial services. Most interesting of all has been the discovery that many companies restating were actually profitable. The deception was not perpetrated to cover up losses or a deteriorating break-even position; instead, management managed the financial statements to maintain the appearance of continued growth in order to support the stock price.

The vastness of the pool of disaster these frauds and misdeeds created appeared to be limited to the U.S. market, an assumption that was a source of smug commentary in overseas management circles. But, in late 2003, the smiles vanished when Parmalat, the Italian dairy and food conglomerate collapsed in the wake of the revelation of a deficiency of assets of between 8 and 12 billion Euros. Over a 15-year period the company had inflated sales (for example, by double billing for merchandise), and borrowed monies on falsely reported rapidly growing assets, becoming more audacious in its actions as time went on. Sending liabilities "off the balance sheet" to related entities in offshore tax havens like the Cayman Islands, the thread that started to unravel the fraud was a missed \$185 million payment. A big clue lay in what would later prove to be a bogus confirmation of a 4 billion Euro cash account (the account did not exist). The company's founder, Colisti Tanzi, a college drop-out with other failed family business ventures to his credit (to which he admitted some of the missing Parmalat assets were diverted) can lay claim to creating one of the most brazen and largest frauds ever, under the watchful eyes of two international accounting firms. Before the fraud was discovered, Parmalat operated in 30 countries and employed 36,000 workers. With elements of Enron (SPEs), Phar-Mor (asset manufacture and diversion of company assets), and Adelphia Communications (family businesses and related party transactions). Parmalat became the new world poster-child for fraud and greed.

10.5 REGULATORY RESPONSES TO FINANCIAL STATEMENT FRAUD

10.5.1 Public Company Accounting Oversight Board

One of the most sweeping responses to financial statement fraud and misstatements of financial statements in the early years of the new millennium was the Sarbanes-Oxley Act of 2002, described in Chapter 1. Under this act the SEC was given increased authority and ability to prosecute corporate misdeeds. One of the most significant provisions of the Sarbanes-Oxley Act of 2002 was the establishment of a Public Company Accounting Oversight Board (PCAOB) to oversee the establishment of accounting standards and oversee audits of public companies. The PCAOB was charged to adopt quality control, ethics, independence and other audit standards, including rules governing the retention of working papers, concurring partner review of audit reports, and testing and reporting on reporting companies internal control systems. The SEC was charged with oversight of this new Board, which was to be funded by public companies and auditors registered with the Board to perform public company audits. In 2004 the PCAOB enacted Auditing Standard (AS No. 2) requiring auditors to opine on the effectiveness of public company internal controls and adopted an auditing standard on documentation, including guidance on what should be retained in audit documentation. Below are a number of other initiatives that have in recent years been directed to discourage financial statement fraud.

10.5.2 SEC Initiatives and Staff Accounting Bulletins

Commission-Wide Initiatives

In the past four years, the SEC has adopted a number of initiatives to address the problem of financial fraud and earnings management. Commission-wide initiatives to address financial fraud include the formation of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees (referred to above) set up in 1999 to develop standards to improve audit committee effectiveness, the promulgation of new rules on audit committee disclosure, the issuance of new rules governing auditor independence, CEO and CFO certification of financial statements, and the issuance of accounting guidance in the form of SABs.

The Rules on Audit Committee Disclosure

Following the BRC's highly publicized report, the Accounting Standards Board (ASB) implemented a number of its recommendations including new rules for audit committees. The rules on audit committee disclosure, effective January 1, 2000, require that:

- Independent auditors review interim financial statements before they are filed on Form 10-Q with the SEC.
- Issuers must include in their proxy statements certain disclosures under Item 302(a) of Regulation S-K, which requires reconciliation and description of adjustments to quarterly financial information.
- Issuers must disclose in their proxy statements whether the audit committee reviewed and discussed with its auditors matters specified in the accounting literature, that is, SAS No. 61, *Communication With Audit Committees* (AICPA, *Professional Standards*, vol. 1, AU sec. 380), as amended, and Independence Standards Board Standard (ISBS) No. 1, *Independence Discussions with Audit Committees*. These matters include proposed adjustments, independence issues, the *quality* of financial statements such as any unusual entries or adjustments, and the question of whether the numbers in the financial statements reflect economic reality.

Interim auditor reviews began the first fiscal quarter ended after March 15, 2000. The other new requirements went into effect on December 15, 2000. These rules are incorporated into Section 10.5.2, "New Statements on Auditing Standards," below.

Independence Rules

During 2001, the SEC adopted a series of rule amendments regarding auditor independence. The amendments, effective February 5, 2001, provide guidelines for:

1. Determining whether an auditor is independent in light of investments made by auditors or their family members in audit clients
2. Employment relationships among auditors, their family members, and audit clients
3. The scope of services provided by audit firms to their audit clients. (Notably, the scope of services provisions identify certain nonaudit services provided by an auditor to a public audit client that would impair the auditor's independence.)

CEO Certification of Financial Statements

On June 28, 2002, the Commission issued an order requiring the principal executive and financial officers of 947 public companies to certify personally, under oath and for publication, the completeness and accuracy of their most recent financial statements filed with the SEC. Specifically, corporate officers must certify that covered reports do not contain any untrue statements of material fact or omit to state material facts necessary to make the statements in the covered report, under the circumstances under which they were made, not misleading.

In a speech delivered to the National Press Club on July 22, 2002, Harvey Pitt, then the chairman of the SEC, noted that the Division of Enforcement has already filed a record 122 actions for financial reporting and issuer disclosure violations in the first 10 months of fiscal 2002, and further stated:

In just ten months, we've sought to throw unfit officers and directors out of corporate boardrooms for good in 71 cases, with more on the way—already almost twice the number we sought in 2000. As the President acknowledged in his Ten Point Plan, corporate officers and directors, and especially the CEOs and CFOs, must personally assume responsibility for compliance with our full disclosure laws. The ouster of unfit officers and directors is a critical tool to ensure that officers and directors “get it” that their mission is to safeguard the interests of shareholders. It is also important to prevent any corporate wrongdoers from getting a second chance to injure investors.

The chairman went on to say that “the heaviest hammer . . . is criminal prosecution and serious jail time.”

On July 30, 2002, the President signed into law the Sarbanes-Oxley Act of 2002, which imposes additional requirements on corporate officers. Section 906 of the Act, which is effective immediately, requires periodic reports filed with the Commission to be accompanied by a written certification by the CEO and CFO that the report fully complies with Sections 13(a) or 15(d) of the Securities Exchange Act of 1934; and that “the information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer.” The Act imposes *criminal penalties of up to \$1,000,000 or 10 years in jail* for corporate officers who “willfully certify” while knowing that the periodic reports do not comply with these requirements.

Staff Accounting Bulletins

Other significant Commission-wide initiatives include the issuance by the Office of the Chief Accountant of Staff Accounting Bulletins (known as SABs) to provide guidance on materiality, restructuring and impairment charges, revenue recognition, and loan loss allowances. That guidance was issued in the form of SABs No. 99 Materiality, No. 100 Restructuring and Impairment Charges, No. 101 Revenue Recognition, and No. 102 Loan Loss Allowance Methodology and Documentation Issues.

Staff Accounting Bulletins

SAB No. 99, Materiality

SAB No. 99, published August 12, 1999, outlines the staff's concerns about the misuse of materiality. SAB No. 99 does not change existing legal or accounting requirements, but emphasizes that auditors should consider qualitative as well as quantitative benchmarks in

determining whether an item is material to the financial statements. By way of example, it notes that the following considerations “may well render material a quantitatively small misstatement of a financial statement item.” A material misstatement occurs if it:

- Arises not from an item capable of precise measurement, but rather from an estimate, taking into account the degree of imprecision of the estimate.
- Masks a change in earnings or earnings trends.
- Hides a failure to meet analysts’ consensus expectations for the enterprise.
- Changes a loss into income or vice versa.
- Concerns a segment or other portion of the registrant’s business that has been identified as playing a significant role in the registrant’s operations or profitability.
- Affects the registrant’s compliance with regulatory requirements.
- Affects the registrant’s compliance with loan covenants or other contractual arrangements.
- Has the effect of increasing management’s compensation, e.g., by meeting income targets necessary to trigger the award of bonuses or other incentive compensation.
- Involves the concealment of an unlawful transaction.

In these instances, a relatively small item (in quantitative terms) may be considered material to the financial statements as a whole.⁴⁸

SAB No. 99 also reminds auditors of their obligations under Section 10A of the Securities Exchange Act of 1934 and existing auditing standards to inform management, in certain circumstances, the audit committee, and in exceptional circumstances, the SEC, of illegal acts detected in the course of an audit. Auditor obligations under Section 10A is discussed in greater detail in Section 10.5.3, “Enforcement of Section 10A of the Securities Exchange Act of 1934,” below.

SAB No. 100, Restructuring and Impairment Charges

SAB No. 100, published November 24, 1999, provides guidance on the accounting for and disclosure of expenses and liabilities currently reported in connection with restructuring activities and business combinations including detailed guidance on the reporting of exit costs. It also provides guidelines for the recognition and disclosure of asset impairment charges.

SAB No. 101, Revenue Recognition

SAB No. 101, published December 3, 1999, provides guidance on the recognition, presentation, and disclosure of revenue in financial statements including criteria for revenue recognition. It also includes guidance on recommended disclosures about revenue recognition policies and the impact of events and trends on revenue. It covers a number of specific situations where there is some room for judgment in interpreting GAAP. Although the SAB does not create new GAAP, it is intended to narrow practice to a single preferred approach.

⁴⁸ SAB No. 99 was quoted with approval by the Second Circuit in *Gambino v. Citizens Utilities Company* (228 F.3d 154).

Because SAB No. 101 addressed specific situations not directly addressed in the accounting literature, the SEC gave issuers a grace period to comply with the SAB and permitted issuers to adopt a change in accounting principle to reflect the changes.

Initially, the grace period was scheduled to end the first fiscal period after December 15, 1999 (first-quarter 2000 for most issuers), but many issuers requested additional time to comply. In response, the SEC issued two amendments (SAB No. 101A and No. 101B) that delayed implementation until the fourth quarter of the fiscal year beginning after December 15, 1999 (fourth quarter 2000 for most companies).

Despite these delays, SAB No. 101 had an impact. A Bear Stearns study released the first quarter after the reporting requirement went into effect, found that at least 32 issuers changed the way they booked revenue as a result of the SAB and the SEC's heightened scrutiny of revenue recognition.

SAB No. 102, Loan Loss Allowance Methodology and Documentation Issues

SAB No. 102, published on July 6, 2001, provides guidance on the development, documentation, and application of a systematic loan loss methodology. The Commission previously issued guidance on this topic in December 1986 through Financial Reporting Release No. 28, *Accounting for Loan Losses by Registrants Engaged in Lending Activities*. SAB No. 102 applies to registrants who are creditors in loan transactions that, individually or in the aggregate, have a material effect on the registrant's financial statements.

SAB No. 102 covers the following topics:

- A summary of current loan loss allowance guidance under GAAP and Commission rules and interpretations
- General factors or elements to consider in developing and documenting loan loss allowance methodologies including in written policies and procedures
- Staff expectations for documenting loan impairment under FASB Statements No. 5 and No. 114, *Accounting by Creditors for the Impairment of a Loan*
- Staff expectations related to summary documentation of the results of a systematic loan loss allowance methodology
- General guidance on validating and documenting the validation of a systematic loan loss allowance methodology.

Enforcement Initiatives

There have also been a number of important initiatives within the Division of Enforcement to address the problem of financial statement fraud:

1. The staff has heightened its scrutiny of investigations involving allegations of financial statement fraud. The staff has expanded its inquiries beyond the more typical revenue recognition and inventory management cases, to more difficult and controversial issues involving managed earnings, as in the W.R. Grace case; the application of technical accounting bulletins such as SOP 97-2, as in the MicroStrategy case; and the accounting for complex off-balance sheet financing transactions, as in the Enron investigation.
2. The Division changed the way it staffs accounting fraud investigations to investigate more quickly and charge those responsible for such transgressions. Traditionally, the Division staffed its accounting fraud cases with one staff attorney and one staff

accountant. The turnaround time from the commencement of the case to the recommendation of charges ranged from an average of two to four years, depending on the complexity of the case. In 1999, the Division realigned its resources and formed SWAT teams consisting of two or three staff attorneys and one or two accountants to enable the staff to ascertain liability and recommend enforcement action in three to six months. The Livent case is an excellent example of the Commission's success with this approach.

3. The Division of Enforcement formed a special branch to focus exclusively on accounting fraud cases. This new group focuses on novel and complex financial fraud cases.
4. The Division of Enforcement has leveraged its resources through sweeps. Exactly one year after former chairman Arthur Levitt's September 1998 "Numbers Game" speech, the division announced its first financial fraud sweep by charging 68 individuals and entities with fraud and/or abuses of the financial reporting process. Just about one year later, in September 2000, the SEC district office in San Francisco announced another financial fraud sweep against six companies.
5. The Division has made increasing numbers of criminal referrals in cases involving egregious misconduct. In August 2000, for example, the SEC and U.S. Attorney's office brought civil and criminal charges against former officers of Cendant Corporation and CUC International. In a press release, Dick Walker, then Director of the Division of Enforcement, was quoted as stating that the action makes it "crystal clear that the SEC and U.S. Attorney have ZERO TOLERANCE for fraudulent financial reporting." That sentiment was clear in the Commission's subsequent actions against officers of Sirena Apparel, McKesson, and Informix. In Sirena Apparel, the SEC charged and the U.S. Attorney indicted the CEO and CFO for directing employees to reset computer clocks to backdate invoices. In McKesson, the SEC and U.S. Attorney charged the former president and CFO for their involvement in a scheme to overstate earnings. In Informix, the SEC and U.S. Attorney charged a former European sales executive who issued side letters allowing customers to delay payment for software. Most recently, swift SEC enforcement action and/or criminal indictments were brought against senior executive officers of WorldCom, Tyco, and Adelphia. These criminal referrals convey the message that financial fraud is a crime that carries both civil and criminal penalties.
6. The Division has also made a concerted effort to identify the individuals responsible for false financial statements. This effort signifies a rejection of the "innocent soldier" defense. To avoid delays, the Division may opt to settle with an issuer but continue its investigation of individuals. The effort to identify individuals responsible for an issuer's false financials included increased scrutiny of gatekeepers, in particular, mid-level accounting personnel and independent auditors who reviewed the false financials.
7. The Division has used its powers under the Remedies Act more flexibly to encourage cooperation and appropriately credit issuers and individuals who cooperated in the staff's investigations. That effort was formalized in October 2001 by Chairman Pitt in the highly publicized Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions. In the Cendant case, despite civil charges against seven former officers and criminal charges against three, the SEC only charged the company with violations of the periodic reporting, corporate recordkeeping, and

internal control provisions of the federal securities laws. There were no fraud charge against Cendant, and in fashioning its order, the Commission specifically recognized remedial acts promptly undertaken by Cendant as well as its cooperation with the Commission and other authorities.

Likewise, the SEC filed a settled administrative action, with no fraud charge and no civil penalties, against Waste Management, because of the company's remedial action and change in management. The outcome of Aurora Foods and Microsoft represent other examples of the staff's commitment to reward early cooperation. By contrast, the staff's imposition of a \$10 million penalty against Xerox represents the consequences of a lack of cooperation.

10.5.3 New Statements on Auditing Standards

As previously mentioned, the PCAOB issued an auditing standard (AS 2) requiring auditors to provide an opinion on the effectiveness of internal controls. Management is also required to attest to its internal controls in its annual report. Since adoption part way into the 2004 audit year, the Standard has fallen under criticism for its many required audit procedures and the burdens of implementation. Initially the Standard only was implemented for the largest public companies ("accelerated filers"), and, as of August 2006, the requirement for smaller companies to report on controls had been deferred again. Smaller companies with fiscal years ending on or after December 15, 2006, will be required to self-report on their internal controls, with auditor involvement and opinions scheduled to be implemented the next year.

In response to the widening scandal on the dating of stock options, the PCAOB issued its first Staff Alert in July 2006 reminding auditors to include stock option policies and processes in their internal controls procedures and to direct audit procedures to this identified risk area.

In response to heightened concerns about earnings management, the Auditing Standards Board (ASB) issued new Statements on Auditing Standards that affect the relationship among the auditor, corporate management, and the audit committee. They are SAS No. 89, *Audit Adjustments* (AICPA, *Professional Standards*, vol. 1, AU secs. 310, 333, and 380), which covers audit adjustments, and SAS No. 90, *Audit Committee Communications* (AICPA, *Professional Standards*, vol. 1, AU secs. 380 and 722), which relates to audit committee communications.

SAS No. 89, Audit Adjustments

SAS No. 89, *Audit Adjustments*, governs engagement letters, management representation letters, and audit committee communications. SAS No. 89 amends existing guidance under SAS No. 85, *Management Representations* (AICPA, *Professional Standards*, vol. 1, AU sec. 333) and AU Section 310, *Appointment of the Independent Auditor* (AICPA, *Professional Standards*, vol. 1, AU sec. 310), to add to the list of items typically included in the engagement letter a new item relating to management responsibility for adjusting the financial statements to correct material misstatements. In addition, management is required to affirm to the auditor in the management representation letter that the effects of any uncorrected misstatements aggregated by the auditor during the current engagement are immaterial, both individually and in the aggregate, to the financial statements taken as a whole. In making the assessment

of materiality, the auditor is directed to consider not only quantitative, but also qualitative materiality, consistent with the requirements of SAB No. 99. SAS No. 89 also amends SAS No. 61, *Communication With Audit Committees* (AICPA, *Professional Standards*, vol. 1, AU sec. 380), to require the auditor to inform the audit committee about uncorrected misstatements aggregated by the auditor during the current audit that management determines to be immaterial, both individually and in the aggregate.

SAS No. 90, Audit Committee Communications

Given the auditor's increased responsibility to report unadjusted differences to the audit committee under SAS No. 89, the ASB issued SAS No. 90, *Audit Committee Communications*, to provide additional guidance on audit committee communications. SAS No. 90 further amends SAS No. 61 to require that the auditor discuss with the audit committee and corporate management the auditor's judgments about the quality as well as the acceptability of the reporting entity's accounting principles as applied in its financial reporting. The discussion should include items that have a significant impact on the representational faithfulness, verifiability, and neutrality of the information included in the financial statements. These should include but not limited to changes in accounting policies, estimates, judgment and uncertainties, unusual transactions, and accounting policies relating to significant financial statement items including the timing of transactions and the period in which they were recorded.

SAS No. 90 also amends SAS No. 71, *Interim Financial Information* (AICPA, *Professional Standards*, vol. 1, AU sec. 722), to implement the recommendations of the Blue Ribbon Committee. It requires auditors to discuss with audit committees:

1. The matters outlined in SAS No. 61 prior to filing quarterly financial information on Form 10-Q.
2. In performing SAS No. 71 limited review procedures, the issue of whether any of the matters discussed in SAS No. 61 may bear on the financial statements.

Any matters identified should be communicated to the audit committee.

SAS No. 99, *Consideration of Fraud in a Financial Statement Audit*, was effective for audits for periods beginning on or after December 15, 2002. It enhanced the guidance and requirements in SAS No. 82 on that same subject and added more teeth to the previous requirements in the wake of the widespread scandals and frauds being discovered in 1999 to 2002. A long standard with 82 paragraphs and an appendix and an exhibit, it had more "should" requirements than many previous standards in an effort to make fraud-directed procedures a standard part of the audit process. Among other requirements, it called for:

- a risk assessment process directed at the consideration of fraud risk
- a planning discussion among key audit engagement team members about the risks of fraud
- inquiries of personnel outside the financial accounting circle
- directing audit procedures against presumed fraud risk areas such as revenue recognition.

An appendix to the document enumerated fraud risk factors, classified by types and an exhibit was directed at companies to help them establish anti-fraud policies and procedures.

In 2006, a new suite of risk assessment and response standards was introduced by the ASB for private company audits (SAS No. 104 to SAS No 111). The specific provisions of some of these standards are discussed in earlier sections of this *Handbook*. Preceding their issuance was the implementation of a new documentation standard, SAS No. 103, *Audit Documentation*, to clarify auditor responsibilities to create and retain adequate audit documentation to support the opinion. It also clarified which documents need to be retained and those that can be discarded as the audit progresses and after the audit report is issued. The documentation standard is effective for most 2006 audits.

Although the risk assessment suite of standards is not required to be implemented until 2007 for private company audits, many larger accounting firms have already integrated their provisions into their audit approaches because of the international nature of their audit approaches and the similarity of the U.S. SASs with IAASB Standards (principally ISAs 315 and 330) that were implemented internationally in 2005. The ASB and IAASB worked together on the development of these standards beginning in the late 1990s, but factors in the U.S. environment including the disruptions caused by the aforementioned frauds and changes in the standard-setting process for companies delayed their finalization and implementation. Many of the provisions in these standards have implications for deterring or identifying fraud as well as misstatement, and include many specific performance requirements.

Although the compilation entitled *Statements on Auditing Standards 104–111*, published by the AICPA in 2006, is 206 pages long, some of the more important provisions are enumerated below and are detailed in a 2006 AICPA publication entitled *Understanding the New Auditing Standards Related to Risk Assessment*:

- Clarification that “reasonable assurance” is a high level of assurance
- Requires a risk assessment, including the assessment of internal control
- Expands in more detail the business, environmental and company specific factors that should be considered when making the risk assessment
- Does not allow the auditor to “default” to high control risk and perform a substantive procedures audit without a basis for that assessment. Thus, auditors will need to assess the design of controls and that the controls have been implemented (placed in operation) on GAAS audits.
- Directs that audit risks, controls and further audit procedures should be linked throughout the workpapers through using audit assertions.
- Identifies a new type of risk—a “significant risk” that carries restrictions on how that risk can be addressed by audit procedures. One or more significant risks are presumed to be present in most audits
- Clarifies when evidence from prior audits can be used in current audits
- Directs that tolerable misstatement should be set to less than materiality amounts in order to allow for the risk of undetected misstatements in reaching a high assurance that the financials are free of material misstatement.
- Requires the communication of auditor identified known and likely misstatements

The AICPA is preparing an extensive audit guide, including a case study, to illustrate the key provisions of the standards and related standard SAS No. 112.

On the heels of the new Risk Standards, SAS No. 112 *Communicating Internal Control Related Matters Identified in an Audit* (AICPA, 2006) was issued. However, this standard is effective for most 2006 audits and requires the annual written communication of identified significant deficiencies and material control weaknesses to management and “those charged with governance.” Additional guidance and examples are provided to help auditors identify these deficiencies and assess their severity. In combination with the required assessment of controls design (SAS No. 109), this standard is likely to push many companies to correct deficient controls and reduce the “opportunities” for fraud and misstatement in the private company sector, including non-profit and government entities.

An attestation standard on reporting on internal controls is also under revision for possible adoption in late 2006 (AT 501). Non-profit and government entities have expressed high interest in beginning to require auditor involvement in attestations concerning internal control effectiveness. To do that, the requirements of AS 2 seem too onerous and rigid, so AT 501 is designed to be more flexible, permitting the expression of assurance on just the “design of controls” rather than requiring the tests necessary to opine on operating effectiveness of the controls. This “toe in the water” strategy is expected to lead to future requirements to test and report on the effectiveness of controls, also an option under AT501.

10.5.4 The Paradigm: COSO’s “Internal Control—Integrated Framework”

The initially vague notion of “framework” above is clarified in the Sarbanes-Oxley Act and in the SEC’s writings as meaning, for all practical purposes in the U.S., the COSO framework, Internal Control—Integrated Framework. This 1992 report grew out of the Treadway Commission, established as a result of a spate of frauds and misstatements observed in the 1970s and 1980s. The SEC notes that the COSO framework “satisfies our criteria and may be used as an evaluation framework for purposes of management’s annual internal control evaluation and disclosure requirements”. The SEC stops short of mandating the COSO framework, however, since other frameworks exist outside the U.S. (COCO in Canada and the Turnbull Report in the UK) and new ones might be developed in the future. For the purposes of compliance, it is expected registrants will use the COSO framework.

The COSO authors defined an internal control system as having three objectives:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

By restricting the final rules to internal control over financial reporting, the SEC therefore does not deal with operating controls or the self-monitoring process that ensures compliance with all laws and regulatory bodies. However, certain regulatory (e.g., compliance with environmental laws) and operating matters (e.g., operating reports are integral to management’s monitoring of reported financial results) may be included within the definition of internal control over financial reporting.

Controls

There are two types of control over financial reporting:

1. Preventive
2. Detective

Preventive controls (e.g., sensors to detect merchandise theft) are designed to thwart the commission of errors or fraud that could cause a misstatement of financial results. Of course, determined fraudsters can override or avoid them by some stratagem. (It is the function of the code of ethics to deflate their desire to do so.) If the fraudsters manage to bypass the preventive controls, the detective controls (e.g., physical counts at year-end) should be able to catch the fraudsters or correct the statements before their crimes result in material financial misstatements.

The COSO model, *Internal Control—Integrated Framework*, breaks internal control into five broad areas:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communications
5. Monitoring

Control Environment

The control environment is the most pervasive of all the controls because it sets the ethical tone in which all operations of the business take place. It influences the behavior of employees and their susceptibility to temptations to commit fraud or cut corners in dealing with suppliers, customers, and regulatory authorities. A written code of ethics should be drawn up, provided to all employees, reinforced through education and adhered to by example. Like any good army, a good company should be led from the front. The chairman, board and senior officers should all be of the highest integrity and be known throughout the company as ethical persons since the tone at the top will be felt all the way down to the lowest levels and out to suppliers and customers. Management's operating style and general philosophy of business will be reflected in its view of risk, attitude toward compliance with the new SEC rules, and its way of developing operating goals and budgets. This philosophy will have a significant effect on the whole control process. The test of management's ethical standards will come when forced to follow up on problems revealed by the internal or external auditors, whistleblowers, environmental accidents, and creditors and regulators.

Cases such as Phar-Mor and Adelphia Communications illustrate the pervasive effect of the chief executive's ethics and the "tone at the top" on the entity. Without integrity at the top, the underlying detailed controls are a less relevant detail. PCAOB Auditing Standard No. 2 explicitly identifies senior management fraud of "any magnitude" to be a strong indicator of a controls weakness.

Management must also make sure the segregation of duties as well as performance goals and rewards are reasonable. Segregation of duties must recognize the possibility of conflicts that could lead to fraud. The perpetrator cannot simultaneously be in a position to both

commit the fraud and cover it up in the course of his or her assigned duties. The person responsible for booking receivables, for example, should not also be responsible for disbursements. The history of fraud is littered with cases of trusted employees giving way to temptation when performing conflicting duties. Short-term high-performance goals that are unrealistic simply open the door to fraud by high achievers. Unsegregated duties and unachievable performance goals could easily lead to improper financial reporting practices.

One of the most important parts of the control environment is the organizational structure including the allocation and delegation of authority and responsibility. The degree to which employees recognize their personal accountability is an important part of the overall effectiveness of all internal controls. The organizational structure must define jobs, assign but not duplicate or overlap decision-making powers, yet leave enough room for initiative and the unimpeded flow of information.

The competence of those with authority will be dependent on the hiring and training policies of the human resources department. HR is the gatekeeper checking the educational credentials and work histories of everyone who seeks employment at the enterprise. Unfortunately, the person who ultimately commits fraud usually has the profile of the ideal hire; everything checks out. Employee fraud is most frequently committed by someone responding to a personal financial crisis or seeing an opportunity to improve their lifestyle. To remove these incentives to fraud, HR must provide competitive compensation, opportunities for advancement through education and seniority, regular and fair performance reviews, plus bonuses to spur above-average efforts.

Risk Assessment

The COSO framework recognizes that specific risks derive from the objectives set by the company and, as mentioned above, identifies three broad classes of objectives achievable through internal control:

- Operations
- Financial reporting
- Compliance with laws and regulations

The one that concerns us here is the objective of internal control over financial reporting. The COSO framework considers the achievement of the financial reporting objectives as “[t]he preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly”. The term “reliable” is taken as synonymous with “presents fairly” defined in *Statement on Auditing Standards No. 69 The Meaning of “Presents Fairly in conformity with Generally Accepted Accounting Principles” in the Independent Auditor’s Report*. A fair presentation recognizes the following factors:

- The financial statements present the financial position, results of operations, and cash flows within limits reasonably attainable in financial statements
- The accounting principles used have general acceptance and are appropriate in the circumstances
- The amount of information is neither too sparse nor too detailed
- The financial statements are accompanied by explanatory notes

The COSO study sets out that materiality is inherent in the concept of fair presentation. Staff Accounting Bulletin (SAB) No. 99 defines a matter as material "if there is a substantial likelihood that a reasonable person would consider it important." In other words, would a financial statement user change his or her opinion if the matter were changed, included, or excluded?

Underlying the preparation of reliable published financial statements is another group of concepts:

- *Existence or occurrence* recognizes that assets, liabilities and ownership interests exist at a specific date; recorded transactions represent events actually occurring during the period
- *Completeness* means everything that occurred and should have been recognized during the period has, indeed, been recorded
- *Rights and obligations* refer to the rights inherent in assets and the obligations inherent in liabilities at a certain date
- *Valuation or allocation* refers to the accurate recording and summarization of assets, liabilities, revenues, and expenses according to relevant and appropriate accounting principles
- *Presentation and disclosure* means that items recorded in the statements are properly described, sorted and classified

The identification of a specific risk affecting financial reporting will be very difficult since the effects of all risks taken by the company will eventually feed into the financial statements. The creation of any account entry at any level of the company will be felt in the financial statements by virtue of being transmitted through the various levels of the reporting process. On this interpretation, the control governing the creation of any reportable number has to be considered part of the control system that must be assessed and audited to assure reliable financial statements and compliance with the SEC final rules.

Controls can lose their effectiveness and thus increase the risk of noncompliance as the company's operating environment changes: personnel change; accounting rules change; competition increases; new regulations come into force; new technology is acquired; new product lines are introduced; mergers, acquisitions and restructurings occur. All these factors and many more require a review of the internal controls systems including that affecting control over financial reporting.

Control Activities

The function of controls, generally speaking, is to reduce the risks that would prevent the company from achieving its business objectives. Control activities can be divided into policy making and procedures. Policies will be determined by the overall risk assessment for the enterprise which will reflect its evaluation of operating, credit, and market risks. Because no two companies are the same, even in the same industry, control policies and procedures must be specific to the entity. Any control must counter the identified risk effectively and carry out the directives of management. Policies should be written but, in fact, are often communicated orally, especially in smaller companies. Problems identified during the enforcement of the procedures should be followed up and corrected.

Control activities to ensure internal control over financial reporting will be most important in the areas of:

- Information processing
- Physical control of assets
- Segregation of duties.

Information and Communication

Information is the lifeblood of any organization. It must be accessible, accurate and flow freely to wherever it is required. It must flow upwards from the operating level to management and downward from the policymakers to those responsible for putting the policies into practice. The effectiveness of any control system depends on the quality and availability of information and the efficiency of the means of communicating it to those who need it to carry out their responsibilities. One of the key pieces of information that must be captured and communicated by the internal control system is any deficiency in the system itself. IT controls as a part of the information system will be treated separately below under *IT Controls*.

Information affects the functioning of control systems by making known to operators of the systems what is expected by way of ethical behavior, the level of competence required, how their work affects other departments, what to do in case of problems and so on. As changes occur in the enterprise risk assessment, changes may be needed in the control systems that must be communicated to the affected personnel.

Monitoring

Monitoring assesses the effectiveness of the design and performance of the control system over time. Monitoring should be an ongoing process built into the control system that detects problems as they occur and assures that the information on which the CEO and CFO are making their assessment complies with the requirements of Sarbanes-Oxley. Reports by the internal and external auditors are an important part of the review process and can point out where the self-reporting controls are failing. Complaints by customers or suppliers should also be considered a form of monitoring report that requires investigation.

COSO Revisits the Framework in 2006 Report

At the prompting of the SEC, COSO began to study the application of the 1992 *Integrated Framework* document to smaller public companies in anticipation of their required public reporting on internal controls. Leading up to the report, a Roundtable discussion was held in 2005 with companies, auditors and the COSO project team to share ideas and experiences. A report was exposed for public comment in late 2005 and released as a final report *Internal Control over Financial Reporting—Guidance for Smaller Public Companies* in July 2006. It can be ordered through any of the sponsoring organization Web sites including the AICPA Web site.

This study re-affirmed that controls effectiveness does not differ between small and large entities, but acknowledges the differences in the small versus large company environments and provides examples from business experience that illustrate how effective controls can be implemented at smaller companies. Many larger companies may also find the guidance helpful in aligning their controls to meet the control objectives in COSO.

The “tools” section of the 2006 report includes a simplified set of matrices for documenting and assessing controls effectiveness. In a new direction, the report uses 20 major principles

and numerous underlying attributes in lieu of the enumeration of the extensive number of control objectives that were in the 1992 report. The simplification of the control objectives this way may also help the comprehension of the requirements for smaller companies, but at the proverbial “end of the day,” the standard for evaluating the effectiveness of the controls is the same.

10.5.5 Preventive and Detective Controls Under Sarbanes-Oxley

The SEC final rules governing internal control over financial reporting can be construed as rules to prevent financial statement fraud by controlling the accounting and IT subsystems that supply the information with which the financial statements are constructed. In practice, this means internal fraud, procurement fraud and computer fraud. The PCAOB recognizes the following list of five problem areas is not exhaustive:

1. Controls on the misappropriation of assets
2. Controls inherent in the company's entire risk assessment processes
3. Code of ethics concerning conflicts of interest, related-party transactions, illegal acts and the monitoring of the code by management and the audit committee or board
4. Adequacy of the internal audit mandate and reporting process as well as the audit committee's degree of involvement in the internal audit
5. Procedures for handling complaints and whistleblower reports

In the end, both the IT system and the accounting cycle feed into the financial statements every public company must prepare to comply with SEC disclosure requirements. It is the figures on these statements whose integrity must be guaranteed by the internal controls protecting the IT system and the accounting cycle. Given that the intent of Sarbanes-Oxley is to achieve reliability in financial reporting, any tampering with the means of producing financial statements will result in an unreliable and therefore noncompliant financial statement.

Unfortunately, even if the internal accounting and IT systems are reliable, senior management can still intervene to manipulate the results for fraudulent purposes. Management controls these systems and also has the power to override.

Financial statement fraud is often hard to distinguish from the exercise of discretion in the recognizing of income or expenses under GAAP. When there is a pattern of pushing the reading of GAAP rules, however, there is probably a fraud somewhere in the numbers. If exceptions to GAAP principles are not discussed in the footnotes to the financial statements they become misleading abuses; the unwary reader will erroneously assume the accounts have been accrued in the same way as other accounts. It is this kind of deception that Sarbanes-Oxley was designed to avoid.

Controls on the Misappropriation of Assets

The best way to achieve control over the misappropriation of assets is to relate the definition of internal control over financial reporting contained in the SEC final rules to areas of the accounting cycle where fraud is a risk. The risk of fraud in the accounting cycle is dealt with in detail in Chapter 5 of this *Handbook*, “Internal Fraud”.

The sales and collection part of the accounting cycle creates the revenue accounts on the income statement and the cash and receivables accounts on the balance sheet. It is in this part of the accounting cycle that most cash thefts occur, kickback schemes are developed, and the falsification of sales records takes place. The foundation of reliability in this cycle is a well-designed IT system for recording and processing transactions. The system itself needs to be reviewed in light of the COBIT compliance standards.

The acquisition and payment portion of the accounting cycle is traditionally a very vulnerable area because funds are constantly flowing out of the company to pay for goods and services. This part of the cycle is touched on in Chapter 5 but receives a separate and more detailed discussion of its own in Chapter 13, “Detecting and Investigating Procurement Fraud”.

Most fraud at capital acquisition and repayment stages of the cycle are committed by senior management because they are most closely involved with the banks and underwriters and have the most override power. Because of the size of the funds involved, the impact on the balance sheet and income statement can be quite significant. The balance sheet accounts usually affected are cash, mortgages, accrued interest, capital stock and capital in excess of par value. On the income statement, interest expense, dividends and retained earnings usually feel the impact of this kind of fraud.

As for computer crime, most computer crime is not committed by hackers raiding the system from outside but from employees manipulating the system from inside.

A thorough review of Chapter 8, “Computer Crime, Computer Criminals, and Computer Evidence” as well as Chapter 4, “Computer Security and System Recovery” should be made in conjunction with the COBIT audit standards.

Controls Inherent in the Company’s Entire Risk Assessment Process

This topic is beyond the scope of this *Handbook* and belongs in the broad area of enterprise risk management. The most up-to-date discussion of this matter is contained in the new COSO book, *Enterprise Risk Management—Integrated Framework*. COSO’s *Internal Control—Integrated Framework*, the internal control over financial reporting accepted by the SEC final rules, as noted frequently above, is, of course, essential reading. James Lam’s *Enterprise Risk Management: From Incentives to Controls* is also an excellent recent book.⁴⁹

Code of Ethics

Because the topic of ethics is too broad to be dealt with fully here, the reader is referred elsewhere. Chapter 2 of this *Handbook*, “Promoting an Ethical Environment” is a good place to start. COSO’s *Report of the National Commission on Fraudulent Financial Reporting*, especially Chapter 2, “Recommendations for the Public Company” continues to be relevant to any discussion of ethical issues and governance. COSO’s *Enterprise Risk Management Framework* mentioned above also has an excellent discussion of the need for strong ethics, in particular Chapter 3, “Internal Environment”. As noted above, Brunswick Corporation has developed a good example of a written code of ethics.⁵⁰

⁴⁹ Lam, James, *Enterprise Risk Management: From Incentives to Controls*, (John Wiley & Sons, Inc.: Hoboken), 2003.

⁵⁰ <http://www.brunswick.com/ethics/english/index.html>

Internal Audit, Reporting Process, Audit Committee

The Sarbanes-Oxley Act places great reliance on the audit committee as the body ultimately responsible for the production of transparent and reliable financial statements. The audit committee is responsible for hiring and firing the auditors, reviewing “all critical accounting policies and practices” to be used in the audit as well as “all alternative treatments of financial information” within GAAP after the auditor has discussed them with management. The auditor must also make the audit committee aware of any outstanding differences between itself and management. The audit committee is thus the final arbiter for conflicts between management and the auditor over accounting policies and practices.

Because it bears such great responsibility for resolving problems affecting compliance with Sarbanes-Oxley, the audit committee must display the greatest independence and professionalism. The audit committee and its oversight responsibilities including those for the internal audit function are discussed in detail in *Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees*, a joint study by the New York Stock Exchange and the National Association of Securities Dealers published in 1999.⁵¹

In addition to ten recommendations, many of which have had their substance included in Sarbanes-Oxley, this Report provides what it calls in a chapter heading “Guiding Principles for Audit Committee Best Practices.” This chapter is a useful “how to” of the best way for the audit committee to conduct itself, what the Report calls “a catalog of common sense fundamentals that apply regardless of an individual company’s situation.” Recognition of the importance of these “fundamentals” will go a long way in assisting an audit committee to bring its company into compliance with Sarbanes-Oxley.

The Report emphasizes the oversight role of the audit committee over management, the internal auditor, and the external auditor and the need for open, objective relations with each. The committee should always be aware of the interrelationship among the three elements: management must implement the required controls, the internal auditor must “objectively assess” these controls, and the external auditor must review the effectiveness of both management and the internal auditor. By understanding each of these three roles, the audit committee should be able to ask incisive questions and thus improve the effectiveness of the whole control and reporting process.

Tension is inevitable between management and the internal auditor who is an employee of the company but has the role of objectively reviewing management’s effectiveness. There should therefore be a formal mechanism in place to allow the internal auditor to have regular meetings with the audit committee to discuss all aspects of the internal audit without any representative of management being present. Such dialogue should be open and uninhibited yet objective. Openness becomes especially important when management is unwilling to support requests by the internal auditor.

A similar relationship should be established with the external auditor in which meetings are held for a frank exchange of views without the presence of representatives from either management or the internal auditor. These meetings will be used to discuss the state of internal controls and the effectiveness of management and the internal auditor in

⁵¹ <http://www.nyse.com/content/publications/1043269645811.html>

overseeing them. The focus of these discussions will be the effectiveness of all parties in producing reliable financial statements.

The committee must rely on management for its view of the enterprise risks and the establishment of controls to combat them. Management will be expected to supply reviews of the financial statements and documents prior to submission to the SEC. Management should also be prepared to present a report on any changes to accounting policies, treatment of significant transactions and any discrepancies between budgets and performance. The audit committee should expect that management will discuss any second opinions obtained from outside auditors that pertain to matters discussed by the internal auditor or the already retained external auditor. The committee should also invite management to speak openly about the assessments prepared by the internal and external auditors.

On the basis of these discussions with management, the audit committee should return to the internal and external auditors to see whether management is actually complying with all its own policies and procedures. None of this, however, should be a substitute for the audit committee's own investigations to assure that there are no shenanigans among the other parties that might present a better picture of the company's condition than is warranted.

Procedures for Handling Complaints and Whistleblower Reports

Under Section 301 of Sarbanes-Oxley, audit committees are required to establish procedures for "the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters." The urgency of this can be measured by statistics in the *2004 Report to the Nation* of the Association of Certified Fraud Examiners (ACFE) which shows that 39.6% of cases were detected by tips from all sources and of these 59.6% were from employees. Although the Act only requires channels be opened for employees, the ACFE study shows that customers and vendors are also important sources of leads that ultimately uncover fraud.⁵² This report and its predecessors are extremely important because they give a picture of the extent of occupational fraud.

10.5.6 Enforcement of Section 10A of the Securities Exchange Act of 1934

Section 10A of the Securities Exchange Act of 1934 requires auditors to take certain actions upon the discovery of a possible "illegal act." This requirement is an affirmative obligation that arises when, in the course of an audit, an auditor detects an illegal act—whether or not the effect of that act is material to the financial statements as a whole. In other words, materiality may not be avoided by offsetting improper revenue with other financial statement items.

These requirements are spelled out in the accounting literature, specifically, in the SASs. SAS No. 54, *Illegal Acts by Clients* (AICPA, *Professional Standards*, vol. 1, AU sec. 317), and SAS No. 82, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU secs. 110, 230, 312, and 316), require auditors to report evidence of fraud to management, and if senior management is involved in the fraud, the auditor must report to the audit committee.

⁵² <http://www.cfenet.com/resources/RttN.asp>

Section 10A goes one step further. It provides that, after the auditor notifies the audit committee, the auditor must make three determinations. First, the auditor must determine whether the illegal act has a material effect on the issuer's financial statements (quantitative or qualitative). Second, the auditor must determine whether management has failed to take appropriate remedial action. Third, the auditor must determine whether the failure to take remedial action will require a departure from the auditor's standard audit report.

Once all three determinations have been made, the auditor must notify the board of directors "as soon as practicable." That time period is not clearly defined, but it is clear that once the auditor notified the board of directors, the board has one business day to notify the SEC Office of the Chief Accountant.

The board may provide a copy of the auditor's report or a summary. If the auditor does not receive a copy of that notice by the end of the next business day, the auditor must resign from the engagement or provide the SEC a copy of its report. Resignation does not relieve the auditor of its obligation to report to the SEC; it just buys one additional day since, upon resignation, the auditor must submit its report to the Office of the Chief Accountant the following business day.

This obligation of auditors to report to the SEC was included in Title III of the Private Securities Litigation Reform Act of 1995 (PSLRA), which is best known for heightening the pleading standards for plaintiffs in securities class action litigation and added Section 10A to the Securities Exchange Act of 1934. The original intent of Section 10A was to provide an incentive for management to take remedial action. But the number of financial fraud cases in recent years, and the number of enforcement actions against auditors suggests that the hammer of Section 10A was not enough.

Solucorp and Rosetti & Yonkers Section 10A Case Studies

On October 31, 1999, the SEC brought its first two cases against auditors for failing to file Section 10A reports. Those cases were *In the Matter of Solucorp* and *In the Matter of Pat A. Rosetti and Jeffrey M. Yonkers*. In the Solucorp matter, the SEC charged a chartered accountant with the Canadian accounting firm McKay & Partners for failing to take appropriate action upon the discovery of possible illegal conduct during an audit of Solucorp's financial statements, in violation of Section 10A. Specifically, the auditor failed to follow the procedures outlined in Section 10A, and required by GAAS, upon his review of a backdated license agreement used to cover up improper revenue recognition. *In the Matter of Rosetti and Yonkers*, the SEC determined that two CPA's employed by the firm Marcum & Kliegman, LLC, failed to take appropriate action as required by Section 10A upon learning that the firm's client was preparing its financial statements using fractions of numbers from existing financial statements, rather than actual results of operations, and failed to properly record or require management to record an expense related to options issued to consultants. In both cases, the auditors were sanctioned under rule 102(e) of the Commission's Rules of Practice.

10.6 AUDIT DEFICIENCIES AND AUDIT FAILURES

10.6.1 The Top 10 Audit Deficiencies (1987–1997)

A complementary report by the authors of the COSO Report, entitled *Fraud Related SEC Enforcement Actions Against Auditors: 1987–1997* (the Audit Failure Report), documented the ten most common audit failures in 45 SEC enforcement actions where sanctions were imposed against auditors for their association with fraudulent financial statements during the period 1987 to 1997.⁵³

The most common problem, in 80 percent of the cases reviewed, was the auditor’s failure to gather sufficient audit evidence, most commonly in the areas of asset valuation, asset ownership, and corroboration of management representations. In about half of the enforcement actions reviewed, the auditors incorrectly applied or failed to apply GAAP pronouncements. In 44 percent of the cases, audit program design was cited as a problem. Specifically, the auditor failed to address inherent risk properly and adjust the audit program accordingly, recognize the additional risk associated with nonroutine transactions or prepare a new audit program for each engagement. Other common audit problems included the failure to exercise due professional care and appropriate professional skepticism, overreliance on inquiry as a form of audit evidence, deficiencies in the confirmation of accounts receivable, failure to recognize related-party transactions, and the failure to expand testing to compensate for identified weaknesses in internal controls.

Table 10.4 classifies the audit deficiency cited, together with the number and percentage of cases in which the deficiency occurred.

TABLE 10.4 AUDIT DEFICIENCIES

| Audit Deficiency | Number of Cases (45 Total) | Percentage |
|--|---------------------------------------|-------------------|
| Gathering sufficient audit evidence | 36 | 80% |
| Exercising due professional care | 32 | 71% |
| Demonstrating appropriate professional skepticism | 27 | 60% |
| Interpreting or applying GAAP | 22 | 49% |
| Audit program design and planning | 20 | 44% |
| Using inquiry as a form of evidence | 18 | 40% |
| Obtaining adequate evidence to evaluate significant management estimates | 16 | 36% |
| Confirming accounts receivable | 13 | 29% |
| Recognizing related parties | 12 | 27% |
| Reliance on internal controls | 11 | 24% |

⁵³ Also see the article “Top 10 Audit Deficiencies” by Beasley, Carcello, and Hermanson in the *Journal of Accountancy*, April 2001.

10.6.2 Audit Failures (1997–2002)

Several of the audit deficiencies noted above were also present in SEC enforcement cases against auditors during the period 1997 to present. Some of the most notable cases during this period are discussed in the following sections.

Sunbeam Corporation

On May 15, 2001, the SEC brought fraud charges against five former officers of Sunbeam Corporation, as well as the former engagement partner from Arthur Andersen who authorized unqualified audit opinions on Sunbeam's 1996 and 1997 financial statements, which were determined by the SEC to have been materially misstated. Among the accounting gimmicks used to artificially inflate reported revenues and earnings were the use of big-bath restructuring charges to create cookie-jar reserves, the recognition of revenue on contingent sales, the acceleration of potential sales into the current quarter, and the improper use of bill-and-hold transactions. Despite these deviations from GAAP, Andersen issued unqualified audit opinions in contravention of GAAS.

Waste Management, Inc.

On June 19, 2001, the SEC filed settled administrative proceedings against Arthur Andersen for the firm's issuance of materially false and misleading audit reports on Waste Management's financial statements for the period 1993 through 1996. Specifically, the SEC alleged that at the time Andersen issued unqualified audit reports certain of its partners knew or were reckless in not knowing that the company's financial statements were not presented fairly, in all material respects, in conformity with GAAP. The SEC claimed the Andersen audit engagement team had identified and documented numerous accounting issues that ultimately led to the company's restatement of financial results for the period 1992 to 1996 and the first three quarters of 1997. As a result of Andersen's failure to ensure that all known misstatements were quantified and all likely misstatements estimated, the SEC further alleged that Andersen's audits were not conducted in accordance with GAAS.

Notably, from the time of Waste Management's IPO in 1971 until 1997, every chief financial officer and chief accounting officer in Andersen's history had previously worked as an auditor at the company. During the 1990s, when the fraud occurred, 14 former Andersen employees worked for Waste Management, mostly in key financial and accounting positions.

According to the SEC, Andersen recognized as early as 1988 that Waste Management employed aggressive accounting tactics including improper adjustments to decrease depreciation expense, the capitalization of interest on current-period development costs, the failure to accrue properly for tax and insurance expenses, improper charges of operating expenses to reserve accounts, and the refusal to write off costs associated with impaired assets. During each audit performed in the restatement period, the engagement team proposed adjusting journal entries to account for material current- and prior-period misstatements. However, management refused to make the entries and Andersen's audit partners declined to take appropriate action or modify the firm's unqualified audit opinions. The adjustments were not made until a new management team took over in late 1997 and determined to restate the company's prior-period financial statements.

Enron Corporation

On June 15, 2002, Arthur Andersen was convicted of obstructing justice by impeding an investigation by securities regulators into the events leading to Enron's financial demise. The conviction represents the first against a major accounting firm, and ultimately led to the firm ceasing operations in 2002.

In addition to the fraud charges, federal investigators are continuing to examine Andersen's audit failures during the firm's long relationship with Enron management. Although charges have not yet been brought, the numerous audit deficiencies noted to date include the failure to identify and require disclosure of significant related-party transactions, the failure to review off-balance-sheet financing transactions, the failure to exercise appropriate professional skepticism, the failure to challenge management's estimates, and the approval of complex, nonroutine accounting transactions that were not permissible under GAAP, without the approval of the firm's technical experts.

California Micro Devices

Following the indictment of Cal Micro's senior executive officers on fraud charges for artificially inflating reported revenues and earnings, the SEC in August 1998 brought Rule 102(e) proceedings against the engagement partner and senior manager on Cal Micro's 1994 audit. These individuals were both members of a then Big Five accounting firm. The SEC alleged that the auditors were reckless in failing to comply with GAAS during the Cal Micro audit, and more specifically, that the auditors conducted themselves unprofessionally in the three critical audit areas of accounts receivable, inventory and property. In each of these areas, the SEC alleged that the auditors failed to exercise appropriate professional skepticism, obtain competent evidential matter or properly supervise audit personnel. Moreover, although Cal Micro had been singled out for "special attention," the SEC alleged that the auditors ignored red flags that indicated potential accounting irregularities.

For example, the SEC alleged that in the revenue recognition category, the auditors did not examine the writeoff of one-third of the Company's accounts receivable balance—a red flag that, in the eyes of the SEC, should have alerted the auditors to the possibility of a material misstatement. The three areas where the auditors were alleged to be lax—accounts receivable, inventory, and property—directly correspond to the areas where most of the accounting adjustments occurred when Cal Micro restated its financial results for fiscal 1994.

However, in a surprising turn of events, an SEC administrative law judge (ALJ) on September 21, 2001, dismissed all 102(e) charges against Cal Micro's auditors, including charges that the CPAs had acted recklessly. Key to the ALJ's opinion was the finding that despite the alleged violations of technical standards there was no evidence to prove a direct link between the audit deficiencies and the misstated financial results. Specifically, the ALJ found that:

1. The auditors were negligent but not reckless in auditing accounts receivable, sales, and returns.
2. No GASS violations were proven in auditing the values of Cal Micro's property, equipment, and obsolete inventory.

3. The evidence did not support the conclusion that Cal Micro materially misstated its property, equipment, obsolete inventory, revenues, or accounts receivable in violation of GAAP.

10.6.3 Lessons Learned

The audit failures noted above provide important lessons in audit planning, execution, and management. For example, as noted in the Audit Failure Report, the three most common audit deficiencies, failure to gather sufficient competent evidence, lack of due care, and lack of professional skepticism, all reflect engagement management problems. The recommended solution to this problem is the development of a properly designed and executed quality control system. The emphasis would be on sound audit planning, supervision, and review as well as adherence to guidelines for the collection of sufficient audit evidence to perform substantive testing and corroborate management representations.

In the planning phase, the Audit Failure Report recommended more extensive participation by engagement partners and concurring partners as well as managers. This would increase the likelihood that the auditor would correctly assess audit risk; make appropriate modifications to the nature, extent, and timing of planned tests; and identify nonroutine transactions that might require additional investigation.

To reduce the incidence of GAAP violations, the Audit Failure Report recommended consultation with technical partners or industry specialists when certain accounting issues arise, expanded coverage of technical accounting topics and industry specific requirements in firm-sponsored training courses, and training on the provisions of SAS No. 69, *The Meaning of Present Fairly in Conformity with Generally Accepted Accounting Principles in the Independent Auditor's Report* (AICPA, *Professional Standards*, vol. 1, AU sec. 411).

To confirm accounts receivable effectively, CPA firms must ensure that their audit teams confirm accounts receivable balances, confirm an adequate selection of the receivables, maintain control of the confirmation process, and employ alternative procedures when confirmations are not returned or exceptions are received.

To increase the likelihood of detecting related-party transactions, the auditor should, for each engagement, prepare a list of related parties, continually update the list throughout the engagement, and provide the list to all audit team members. The audit team should also make inquiries of management regarding the existence of related-party transactions. In addition, it is advisable to confirm with the counterparty the existence and nature of unusual client transactions.

10.7 GUIDANCE FOR AUDITORS

In this regulatory environment, auditors should be mindful of the lessons learned from past audit failures. It is also prudent to review existing guidance in each of the key phases of the audit process, namely, initial risk assessment, analytical procedures, substantive testing, and the issuance of audit opinions.

10.7.1 Risk Assessment

During the risk assessment phase, auditors should obtain an understanding of the prospective client's industry and identify contractual, market, regulatory, and company-specific incentives to manage earnings. Risk assessment is particularly important in determining whether to accept a new audit client, when interviewing former auditors, and when drafting the initial audit plan. To minimize risk, auditors should consider each of the risk factors identified in SAS No. 53, *The Auditor's Responsibility to Detect and Report Errors and Irregularities*, superseded by SAS No. 81, and SAS No. 82, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 316), with an eye to any red flags that might signal a need for further review. Some of the most important risk factors to consider include the existence of a weak internal control environment, evidence that management provided untruthful or evasive answers to prior audit inquiries, indications that management is unduly aggressive or places undue emphasis on meeting earnings projections, and the existence of nonroutine transactions that may be difficult to audit.

10.7.2 Analytical Procedures

Analytical procedures are important tools used by auditors to identify problem areas and to inform substantive testing. Analytical procedures include vertical, horizontal, and ratio analysis. Vertical analysis is a technique for analyzing the relationships between items on an income statement, balance sheet, or statement of cash flows by expressing components as percentages of net sales, total assets, or liabilities and owners' equity. These relationships may be used with historical averages to identify anomalies. Horizontal analysis is a technique for analyzing the percentage change in financial statement items each year. The first period in the analysis is the base year and changes in subsequent periods are computed as a percentage of the base. This method may be effective in identifying material inconsistencies. Ratio analysis is a technique used to identify relationships between two different financial statement amounts and to compare those relationships to industry averages. Of the three techniques, ratio analysis is the most useful for detecting red flags.

The most common ratios used to analyze financial statement amounts are the current ratio, the quick ratio, receivables turnover, inventory turnover, profit margin and asset turnover ratio.

The *current ratio*, which compares current assets to current liabilities, measures a company's ability to meet its present obligations from its liquid assets. A significant increase in the current ratio may indicate an understatement of liabilities.

The *quick ratio* is similar to the current ratio but focuses on assets that may be liquidated immediately: cash, securities and accounts receivable. These assets are then compared to current liabilities to measure a company's ability to meet its immediate cash requirements. A significant decrease in the quick ratio may indicate an increase in accounts receivable, which may suggest the improper recognition of revenue to artificially inflate sales.

The *receivables turnover ratio* compares net sales to average net receivables. As with the quick ratio, a decrease in receivables turnover resulting from an increase in receivables may signal the existence of improper revenue recognition.

The *inventory turnover ratio* compares cost of goods sold to average inventory and measures the number of times inventory is sold during a period. Although a high inventory turnover is generally favorable, an abnormally high inventory rate may indicate inventory theft; an abnormally low inventory rate may reflect false debits to cost of goods sold to conceal fictitious sales.

The *profit margin ratio* compares net income to net sales and measures the amount of profit in each dollar of sales. An abnormally high profit margin may indicate the overstatement of net income resulting from inflated revenues or understated expenses.

The *asset turnover ratio* compares net sales to average operating assets. A decrease in the ratio may indicate overstatement of assets while an increase in the ratio may indicate overstatement of revenues or understatement of expenses.

10.7.3 Targeted Substantive Testing

The auditor should carefully design substantive tests based upon the initial audit plan as modified by the results of analytical procedures. Emphasis should be placed on specific potential problem areas.

For example, if the initial assessment indicates that management is overly aggressive about meeting earnings projections, it may be appropriate to increase and vary sample size in the accounts receivable confirmation process. It may also be advisable to evaluate the nature and adequacy of reserves through the application of analytical procedures to total accruals and individual accrual accounts. This analysis should include comparisons of year-to-year totals in the company and within the industry. This is especially important in companies with historically consistent earnings trends.

In addition, rather than simply accepting management's best estimates, auditors should prepare a schedule of management estimates and estimates suggested by the audit evidence. If individual estimates suggest a directional effect on earnings and the aggregate difference is material, the auditor should evaluate the reasonableness of management estimates. Heightened scrutiny should be applied to unusually large accounting estimates or accruals that decrease earnings, since the overstatement of expense in one year will create upward pressure on earnings in subsequent years.

10.7.4 Scope Limitations and Qualified Audit Opinions

Finally, scope limitations and qualified audit opinions should be used where information cannot be tested or verified. The tendency to waive immaterial discrepancies should be avoided. As regulators scrutinize the conduct of auditors in financial restatement cases, conservatism should be applied in all areas where the auditor's discretion may be questioned.

10.7.5 Typical Frauds Related to Misappropriation of Assets, Example Audit Procedures, and Internal Control Questions⁵⁴

The purpose of this section is to help auditors design extended audit procedures whenever it is believed planned audit procedures are insufficient to respond to the assessed risk of material misstatement due to fraud. This section is organized according to audit area and within each area, the following considerations are included:

- A description of the typical fraud schemes that might be discovered in that area. As described in Chapter 3, of “Fraud Detection In A GAAS Audit” it is relatively unusual for auditors to encounter a fraud and thus, they can become lulled into believing that the risks of material misstatement due to fraud may be negligible at their client. One of the keys for overcoming this assumption and developing a more skeptical attitude is for auditors to become familiar with the types of fraud that might occur. The descriptions included here are designed to do just that. The auditor should consider discussing these common frauds as part of their brainstorming session.
- A listing of what may be discovered during the information-gathering and risk assessment phase of the audit that may indicate the existence of the specified frauds.
- A description of audit procedures that may help detect material misstatements resulting from those frauds. As indicated in Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 316), response to address specifically identified risks of material misstatement due to fraud may include changing the nature, timing, and extent of auditing procedures. The example procedures in this section go beyond the example procedures included in SAS No. 99 (AU sec. 316.53).

For fraud schemes relating to the misappropriation of assets, a listing of supplemental internal control questions are included to help identify control deficiencies that leave them susceptible to fraud. (Note: Fraudulent financial reporting usually is perpetrated by management, who has the ability to override most internal controls. For this reason, the sections dealing with fraudulent financial reporting do not include a discussion of controls.)

This section, is written for auditors performing an audit in accordance with generally accepted auditing standards (GAAS). When audit procedures are extended, audit procedures should continuously be evaluated whether the procedures performed are part of a GAAS audit or part of a fraud examination consulting engagement. Again, it is important to note that the example audit procedures are not required by SAS No. 99 but rather consist of the author of “Fraud Detection In A GAAS Audit.”

⁵⁴ Adapted from *Fraud Detection In A GAAS Audit*, by Michael J. Ramos, CPA, Copyright © 2004 published by AICPA and available at www.cpa2biz.com.

**Extended Audit Procedures
Misappropriation of Assets**

Accounts Receivable

Typical Frauds

Most frauds relating to the misappropriation of collections on accounts receivable involve the diversion of payments received from customers. The scheme is fairly simple to perform, for example, an employee opens a bank account with a name similar to that of the company (Acme Inc. rather than Acme Company). Customer payments can then be taken by the employee and deposited into this bogus bank account.

What varies in accounts receivable frauds is how the frauds are concealed. Common techniques include the following:

- *Lapping.* The payment from customer A is diverted by the employee. To keep customer A from complaining, the payment from customer B is applied to customer A's account. Customer C's payment is applied to customer B's account, and so on.
- *Posting bogus credits to the account.* To conceal the fraud, the employee posts credit memos or other noncash reductions (for example, representing a sales return or the write-off) to the customer account from whom the funds were diverted.
- *Altering internal copies of invoices.* The company's copy of the sales invoice is altered to report an amount lower than that actually billed to the customer. When payment is received, the "excess" amount is diverted by the employee.

Another accounts receivable fraud involves the diversion of payments from written-off accounts. Most companies do not monitor the activity on accounts that have been written off, which provides the employee with the opportunity to divert payments from these customers and not be detected. For example, an employee will work with a customer to collect an overdue receivable. As the customer is about to pay, the employee writes off the account, removing it from the books.

Finally, the author is aware of one fraud committed by an employee who made an arrangement with customers to "manage" their past-due accounts. The employee took steps to make sure these customers' accounts were always shown as current in the company's books and records. This effectively gave the customers an unlimited amount of time to pay their bills and avoid late fees and interest charges. In exchange for this service, the employee received a kickback from the customers.

What to Look For

Be alert for the following, which may be present when the frauds described here are occurring or have occurred.

- Unexplained differences noted by customers on their accounts receivable confirmations.
- Significant delays between the time when the customer states a payment was made and the payment was recorded as received by the company.

- A significant number of credit entries and other adjustments made to the accounts receivable records.
- Unexplained or inadequately explained differences between the accounts receivable subsidiary ledger and the general ledger.

Example Audit Procedures

The following audit procedures will help detect the frauds described above. Depending on your assessment of the risk of material misstatement due to fraud, these procedures may be performed as part of an audit conducted in accordance with GAAS. Alternatively, they may be performed outside the scope of a GAAS audit. If these procedures are already being performed, consider expanding their extent, for example, by selecting more items.

- Confirm account activity (not just the balance) with the customers directly. Be sure to confirm credit memo and sales return activity, as well as the date payments on account were made.
- Perform analytical reviews of credit memo and write-off activity, for example, by comparing to prior periods. Look for unusual trends or patterns, such as large numbers of credit memos pertaining to one customer or sales person, or those processed shortly after the close of an accounting period.
- Vouch credit memos and other write-offs to receiving records for returned goods, correspondence with customers, and other documentation supporting the transaction.
- Investigate all differences between the payment date reported by the customer and the payment date recorded by the company. Do not rely on company-generated activity summaries—review both sides of the original checks or check copies.
- Analyze recoveries of written-off accounts.
- Obtain an understanding of how the accounts receivable aging is prepared and who has access to the data used to prepare the aging.

Expanding Your Internal Control Questionnaire

Your internal control questionnaire may have questions aimed at identifying the client's vulnerability to the misappropriation of accounts receivable. Make sure the person completing the questionnaire understands the implication of these questions. "No" responses may not change your control risk assessment or your assessment of the risk of material misstatement due to fraud. As a client service matter, however, you should consider discussing these items with your client and explaining how the lack of certain controls leaves the company exposed to fraud.

In addition, you may wish to review the control objectives enumerated for this area in the 1992 *Internal Control—Integrated Framework* or the principles and attributes enumerated in the 2006 *Internal Control over Financial Reporting—Guidance for Smaller Public Companies*. Deficiencies in control design or operating effectiveness are an invitation for fraud to occur.

TABLE 10.5 INTERNAL CONTROL QUESTIONS RELATED TO FRAUD

| Accounts Receivable | Yes | No |
|---|------------|-----------|
| 1. Are different employees responsible for preparing invoices, receiving payment, and maintaining accounts receivable records? | _____ | _____ |
| 2. Has the company limited the logical access to computerized accounts receivable records and processes? | _____ | _____ |
| 3. Are employees with accounts receivable responsibilities required to take vacations, and are other employees cross-trained to perform those functions when an employee is absent? | _____ | _____ |
| 4. Are credit memos approved and reviewed by management? | _____ | _____ |
| 5. Does the entity have a method for tracking and monitoring customer complaints related to billing? Are these complaints periodically reviewed by management? | _____ | _____ |
| 6. Is the accounts receivable subsidiary ledger reconciled to the general ledger account balance on a regular basis? | _____ | _____ |

**Extended Audit Procedures
Misappropriation of Assets
Inventory**

Typical Frauds

One of the more common inventory frauds is the theft of inventory for personal use. This is more likely to happen when inventory items are small and easy to steal, and the items have value to an employee as a consumer. For example, computer chips are small and easy to steal, but they have no value to the employee as a consumer. A laptop computer has the physical characteristics that make it susceptible to theft, *plus* the employee can use it immediately. The computer is more likely than the computer chip to be stolen for personal use.

A more lucrative inventory fraud is the theft of inventory for sale. For these frauds, it's not necessary for the inventory to have value to the employee as a consumer, since the goods won't be used for personal use. A common scheme is for the receiving personnel to steal the goods right from the receiving dock, before physical custody is established by the warehouse. For example, the employee signs a receiving report stating that 100 units were received, but only 90 are stocked in the warehouse and 10 are placed in the trunk of the employee's car. The missing units will not be discovered until the year-end physical inventory count.

For larger inventory items that are more difficult to transport, the receiving personnel may collude with the vendor's delivery personnel. The delivery personnel diverts 10 units of inventory to another location and delivers the remaining 90 units. The receiving personnel prepares a receiving report indicating that all 100 units were received. The stolen merchandise is then sold and the proceeds split between the two.

Theft of scrap is another common fraud. For example, a hospital employee was convicted of stealing used x-rays, then recovering and selling the silver. In most companies, inventory scrap is not recorded or well-controlled, which makes it easy to steal. These thefts can be significant, especially in situations where the embezzler has the ability to inappropriately designate good inventory as scrap.

What to Look For

Be alert for the following, which may be present when the frauds described here are occurring or have occurred.

- Large differences between the physical inventory counts and perpetual inventory records.
- Unexpected or unexplained increases in inventory turnover accompanied by decreases in gross profit percentages.
- Unexplained entries in the perpetual inventory records.
- Key inventory ratios (for example, shrinkage, turnover, or gross profit) that vary significantly from industry norms or between company locations or inventory types.
- Shipping documents (that is, showing goods were shipped from the company) without corresponding sales documentation.

Example Audit Procedures

The following audit procedures will help detect the frauds described here. Depending on your assessment of the risk of material misstatement due to fraud, these procedures may be performed as part of an audit conducted in accordance with GAAS. Alternatively, they may be performed outside the scope of a GAAS audit. If these procedures are already being performed, consider expanding their extent, for example, by selecting more items.

- Analyze inventory shortages by location or product type. Compare key inventory ratios to industry norms. Look for unusual concentrations, patterns, or trends as a way to direct further inquiries and investigations.
- Review receiving reports and look for indication of alternative shipping sites.
- Review supporting documentation for reductions to the perpetual inventory records.
- Compare shipping documents to corresponding documentation.

Because of the nature of inventory theft, it may be difficult to detect using traditional audit techniques. If your client has reason to believe inventory is being stolen, a fraud examination may be required. For example, a fraud examiner might perform surveillance of receiving personnel or make surprise counts of items received into inventory.

Expanding Your Internal Control Questionnaire

Your internal control questionnaire may have questions aimed at identifying your client's vulnerability to the misappropriation of inventory. Make sure that the person completing the questionnaire understands the implication of these questions.

“No” responses may not change your control risk assessment or your assessment of the risk of material misstatement due to fraud. As a client service matter, however, you should consider discussing these items with your client and explaining how the lack of certain controls leaves the company exposed to fraud.

In addition, you may wish to review the control objectives enumerated for this area in the 1992 *Internal Control—Integrated Framework* or the principles and attributes enumerated in the 2006 *Internal Control over Financial Reporting—Guidance for Smaller Public Companies*. Deficiencies in control design or operating effectiveness are an invitation for fraud to occur.

TABLE 10.6 INTERNAL CONTROL QUESTIONS RELATED TO FRAUD

| Inventory | Yes | No |
|--|------------|-----------|
| 1. Does the client maintain adequate safeguard controls (for example, locked warehouses) over inventory susceptible to misappropriation? | _____ | _____ |
| 2. Is there proper segregation of duties between persons responsible for inventory recordkeeping and those responsible for its physical custody? | _____ | _____ |
| 3. Are employees with inventory, shipping, and receiving responsibilities required to take vacations, and are other employees cross-trained to perform those functions when an employee is absent? | _____ | _____ |
| 4. Has the company limited the logical access to computerized inventory records? | _____ | _____ |
| 5. Are physical inventory counts performed regularly? Are the count procedures adequate to ensure an accurate count? | _____ | _____ |
| 6. Is scrap inventoried and controlled? | _____ | _____ |
| 7. Is there a proper segregation of duties between those with the authority to sell scrap and those with the responsibility for doing so? | _____ | _____ |

**Extended Audit Procedures
Misappropriation of Assets
Purchasing and Payroll**

Typical Frauds

The purchasing function is particularly vulnerable to fraud. For many small businesses it represents the largest area of the risk of embezzlement.

The most common fraud scheme is the payment of invoices to a fictitious company. To perpetrate this scheme, the embezzler establishes a fake entity (often with a P.O. box for an address, and a name similar to that of a legitimate company) and gets the fake entered into company records as a legitimate vendor. The embezzler then produces invoices for the fake vendor, which get processed by the accounts payable system. Sometimes the embezzler is responsible for authorizing payment; other

times not. The scheme may also require collusion between various people, such as receiving (doctoring a receiving report to indicate something was received) and accounts payable (approving the invoice for payment).

Another common fraud is a kickback paid by vendors to the company's purchasing agent. In collusion with suppliers, a purchasing agent may get paid a kickback for any number of activities, including:

- Allowing the vendor to submit fraudulent billing and approving the payment. Examples of fraudulent billing practices include billing for goods or services never performed or received, billing more than once for the same item, substituting lower quality items than the ones billed, or overbilling for the items delivered.
- Excess purchasing of property or services.
- Bid-rigging.

Kickbacks are "off-the-book" frauds, that is, their concealment is not recorded on the books of the company. For that reason, it is often difficult for auditors to detect the presence of kickbacks.

The most common payroll fraud is the use of *ghost employees*, where the embezzler enters fictitious employees into the payroll system and receives the resulting payroll checks. A variation on this scheme is to keep terminated employees on the payroll several pay periods after they leave their job. The embezzler then receives the paycheck for the terminated employee.

What to Look For

Be alert for the following, which may be present when the frauds described here are occurring or have occurred.

- Fictitious vendors
 - Photocopied invoices or invoices have obviously been tampered with (for example, sections have been "whited out" and typed over).
 - Invoice numbers from the same vendor occur in an unbroken consecutive sequence.
 - Invoices from companies have a P.O. box address or no phone number.
 - Invoices from companies have the same address or phone number as an employee.
 - The amount of each invoice from a particular vendor falls just below a threshold for review.
 - Multiple companies have the same address and phone number.
 - Vendor names appear to be a "knock-off" of well-established businesses.
- Kickbacks
 - Purchasing agent handles all matters related to a vendor even though it might be outside or below his or her normal duties.
 - Vendors who receive an inordinate amount of business from the company for no apparent business reason.
 - Vendor salesmen make frequent, unexplained visits to purchasing personnel.

- Prices from a particular vendor are unreasonably high when compared to others.
- Quality of goods or services received is low.
- Tips or complaints are received from other employees or honest vendors.
- Key contracts are awarded with no formal bid process.
- Ghost employees
 - Employees with duplicate addresses, checking accounts, or Social Security numbers.
 - Employees with no withholding taxes, insurance, or other normal deductions.

Example Audit Procedures

The following audit procedures will help detect the frauds described in the previous list. Depending on your assessment of the risk of material misstatement due to fraud, these procedures may be performed as part of an audit conducted in accordance with GAAS. Alternatively, they may be performed outside the scope of a GAAS audit. If these procedures are already being performed, consider expanding their extent, for example by selecting more items.

- Review selected invoices and look for evidence that the invoice has been doctored.
- Perform a computerized search of the vendor list and look for P.O. box addresses, duplicate addresses, and vendors with no phone number.
- Perform a computerized match of the vendor list with a list of employees and look for matches of addresses or phone numbers.
- Perform a computerized sort of invoices by vendor and look for unusual sequencing or amount (indication of possible fictitious company). Look for unusual pricing and volume trends (indication of possible kickback).
- Review selected invoices and examine supporting documentation indicating goods or services were received.
- Perform a computerized search of payroll records to identify duplicate addresses, Social Security numbers, or bank accounts.
- Review personnel files and look for those that contain little or no evidence of activity, for example, a lack of performance evaluations, requests for changes to withholdings, or retirement plan options.

Because kickbacks are conducted off the books, they may be difficult to detect using traditional audit techniques. If your client has reason to believe a purchasing agent is accepting kickbacks, a fraud examination may be required.

Expanding Your Internal Control Questionnaire

Your internal control questionnaire may have questions aimed at identifying your client's vulnerability to the misappropriation of assets in the purchasing and payroll functions. Make sure that the person completing the questionnaire understands the implication of these questions. "No" responses may not change your control risk assessment or your assessment of the risk of material misstatement due to fraud. As a client service matter, however, you should consider discussing these items with

your client and explaining how the lack of certain controls leaves the company exposed to fraud.

In addition, you may wish to review the control objectives enumerated for this area in the 1992 *Internal Control—Integrated Framework* or the principles and attributes enumerated in the 2006 *Internal Control over Financial Reporting—Guidance for Smaller Public Companies*. Deficiencies in control design or operating effectiveness are an invitation for fraud to occur.

TABLE 10.7 INTERNAL CONTROL QUESTIONS RELATED TO FRAUD

| Purchasing and Payroll | Yes | No |
|--|------------|-----------|
| 1. Is there adequate segregation of duties between purchasing, receiving, and the accounts payable function? | _____ | _____ |
| 2. Are employees with purchasing and accounts payable responsibilities required to take vacations, and are other employees cross-trained to perform those functions when an employee is absent? | _____ | _____ |
| 3. Has the company limited the logical access to computerized vendor, accounts payable, and payroll records? | _____ | _____ |
| 4. If the company chooses suppliers based on competitive bids, are all bids date stamped when received, and opened at the same time under dual control? | _____ | _____ |
| 5. Does the accounts payable system include controls to avoid duplicate payments? | _____ | _____ |
| 6. Are new vendors reviewed by management before being added to the list of qualified vendors? | _____ | _____ |
| 7. Does the company have a written policy on the amount and type of gifts an employee can accept from suppliers and customers? Is that policy communicated to employees, customers, and suppliers? | _____ | _____ |
| 8. Does the company include a “right to audit” clause in its contracts with major suppliers? ⁵⁵ | _____ | _____ |
| 9. Are new employees approved by management before being added to the payroll records? | _____ | _____ |
| 10. Are there controls in place to ensure that terminated employees are removed from payroll records in a timely fashion? | _____ | _____ |
| 11. If the size of the entity permits it, does the owner-manager periodically review the payroll records to determine if every employee listed is personally known to him or her? | _____ | _____ |

⁵⁵ “Right to audit” clauses can be included in contracts or printed on the back of all purchase orders. Under a right-to-audit clause, the company reserves the right to audit the vendor’s books at any time. Vendors who know their records are subject to examination generally are reluctant to make bribery payments.

**Extended Audit Procedures
Misappropriation of Assets**

Cash

Typical Frauds

The most common way in which a company (particularly a small business) is defrauded of cash is through fraudulent disbursements. Under these schemes, the employee uses company checks to either (1) withdraw cash directly for their own benefit or (2) pay personal expenses. For example:

- An employee wrote checks payable to cash and posted the debit to various expense accounts. When the bank statement came back with the canceled checks, she simply discarded the ones she had cashed then proceeded to perform the bank reconciliation.
- An employee used company checks to pay personal credit card bills. Each month, he had a credit card bill approximately equal to the company's required payroll tax withholding. Instead of making the payroll tax deposit, he wrote a check to the credit card company. He discarded these checks when they were returned with the bank statements. He also discarded the notices received from the IRS stating that the company's payroll withholding deposits had not been made.

There are infinite variations on these types of frauds.

People who commit these kinds of frauds are faced with two tasks. First, they must post a debit somewhere in the general ledger to disguise the disbursement. The clever embezzler will post this debit to an expense account (which is closed out at the end of the year, thus eliminating the audit trail), or to inventory (where differences between the books and the physical count flow through cost of sales, thus eliminating the audit trail). Second, the embezzler must have a way for avoiding detection during the bank reconciliation process. In a small business, this usually is possible because of a lack of segregation of duties. It might also involve collusion.

Companies that handle large amounts of cash are also susceptible to theft of cash on hand. Industries such as retail sales or restaurants are particularly susceptible to these kinds of frauds. It would be rare that the theft of cash on hand would be material to an entity's financial statements, but as a client service matter, you should be alert to the possibility. Common schemes include:

- *Skimming.* Cash is "skimmed" before it enters the accounting system. For example, the employee accepts cash but never prepares a receipt, or prepares a receipt for less than the amount taken.
- *Substituting personal checks for cash.* The employee takes money from the cash register and substitutes a personal check. In that way, the cash drawer is always "in balance," but the employee never submits the personal check for deposit to the company's bank account. In that way, the employee receives free use of the cash.

- *Fictitious refunds and discount.* The employee records a refund and removes cash as if a refund had occurred, but no merchandise was returned or discount given.
- *Altered credit card receipts.* This is a problem in the restaurant business where the waitperson will increase the tip on a credit card receipt.

What to Look For

Be alert for the following, which may be present when the frauds described above are occurring or have occurred:

- Large, unexplained reconciling items in the bank reconciliations.
- Bank statements that do not include canceled checks.
- Some canceled checks are missing.
- Disbursements are unsupported by invoices or other documentation.
- Customer complaints.
- Altered or missing cash register tapes.

Example Audit Procedures

The following audit procedures will help detect the frauds described above. Depending on your assessment of the risk of material misstatement due to fraud, these procedures may be performed as part of an audit conducted in accordance with GAAS. Alternatively, they may be performed outside the scope of a GAAS audit. If these procedures are already being performed, consider expanding their extent, for example by selecting more items.

- Examination of bank reconciliations. A thorough review of bank reconciliations is one of the best ways to detect fraud relating to cash.
- Review bank statements and canceled checks. Look for checks made out to cash or to employees. Compare endorsement to payee. Make sure all canceled checks are accounted for.
- Obtain a bank cut-off statement. Cut-off statements are ordered from the bank and delivered directly to the auditor who reconciles them.
- Search for and examine unusual expense account activity close to the end of an accounting period. The theft of cash usually is concealed with a debit to an expense account because expenses are closed to retained earnings at the end of the accounting cycle. The clever embezzler will concentrate his or her theft at the end of the cycle to limit the amount of time the theft remains on the books.
- Surprise cash counts. These will sometimes turn up embezzlement of petty cash.
- Analyze sales discounts and returns. Compare current period to prior periods or breakdown activity by employee. Look for unusual patterns or trends.

Expanding Your Internal Control Questionnaire

Your internal control questionnaire may have questions aimed at identifying your client's vulnerability to the misappropriation of cash. Make sure that the person completing the questionnaire understands the implication of these questions. "No" responses may not change your control risk assessment or your assessment of the risk of material misstatement due to fraud. As a client service matter, however, you

should consider discussing these items with your client and explaining how the lack of certain controls leaves the company exposed to fraud.

In addition, you may wish to review the control objectives enumerated for this area in the 1992 *Internal Control—Integrated Framework* or the principles and attributes enumerated in the 2006 *Internal Control over Financial Reporting—Guidance for Smaller Public Companies*. Deficiencies in control design or operating effectiveness are an invitation for fraud to occur.

TABLE 10.8 INTERNAL CONTROL QUESTIONS RELATED TO FRAUD

| Cash | Yes | No |
|---|------------|-----------|
| 1. Are all bank accounts reconciled on a timely basis? | _____ | _____ |
| 2. Is the person who reconciles the bank accounts different from the person responsible for cash disbursements? | _____ | _____ |
| 3. Does the company receive canceled checks along with its bank statements? | _____ | _____ |
| 4. Do the bank reconciliation procedures include accounting for all canceled checks? | _____ | _____ |
| 5. Are employees with cash disbursement and bank reconciliation duties required to take vacations, and are other employees cross-trained to perform those functions when an employee is absent? | _____ | _____ |
| 6. Has the company limited the logical access to computerized cash disbursement records? | _____ | _____ |
| 7. Does the company limit the physical access to negotiable assets, such as blank checks? | _____ | _____ |
| 8. Does the owner review and sign all checks? If not, do disbursements over a certain dollar amount require dual signature or other control procedure? | _____ | _____ |
| 9. If company employees process a significant amount of cash transactions, does the company adequately control and monitor these transactions? | _____ | _____ |

**Extended Audit Procedures
Misappropriation of Assets**

Computer Schemes

Typical Frauds

The most common types of computer schemes involve input tampering. This can be accomplished by altering, forging, or fabricating computer input documents. In an entity without adequate logical access control (which is not uncommon for small businesses), input tampering is quite easy to accomplish. The more common computer input schemes include:

- *Entering false transactions.* For example, entering invoices for fake vendors into the accounts payable system or recording false credit memos to accounts receivable.
- *Entering bogus file maintenance transactions.* File maintenance activities include such transactions as changing a customer's address or adding a new employee to the payroll. Bogus file maintenance transactions can lay the groundwork for any number of frauds, for example, the use of ghost employees to embezzle funds.
- *Failure to enter legitimate transactions or file maintenance instructions.* For example, when an employee is terminated, that information should be entered into the computer system to remove that employee from the payroll records. A failure to do this creates a ghost employee.
- *Altering input data.* For example, changing the amounts, dates, or other information contained on the input data.

Other computer frauds involve *program modification* schemes, sometimes referred to as "throughput frauds." To accomplish these schemes requires an understanding of and the ability to modify computer application programs. Typical schemes include:

- *Bogus instructions.* A computer programmer may place bogus instructions into a computer program so the computer will perform unauthorized functions, for example, making payments to a vendor not listed on an approved list.
- *Siphoning funds.* Funds can be siphoned in small amounts from a large number of accounts, for example, pennies and portions of pennies (due to rounding) can be shaved from thousands of savings accounts. The money is then accumulated in a single account that is accessed by the embezzler.
- *Direct manipulation of accounts.* Computer programs may be altered to obtain direct access to manipulate files without authorization. For example, file maintenance changes may be accomplished without the input of the normal documentation.

What to Look For

Computers often are used to accomplish the frauds listed elsewhere in this section of the publication. Observing signs of other frauds may lead you to one of the computer fraud schemes listed here. In addition to the items listed elsewhere, be alert for the following, which may be present when the frauds described here are occurring or have occurred.

- Inability to process computer applications in a timely manner.
- Unexplained differences in batch or hash totals, or other means to control computer input.
- Undocumented or unauthorized account postings, file changes, or modifications to application programs.
- Unexplained differences between the general ledger and computerized accounting records (for example, a computer spreadsheet) maintained on a separate computer.

Most small businesses use microcomputers, either to process accounting information or to prepare or summarize information for input (for example, through

use of a spreadsheet). The use of microcomputers and a highly decentralized computer processing environment can leave a company vulnerable to various fraud schemes because of:

- *A lack of segregation of duties.* The same person can prepare a source document (for example, an invoice), process the information (prepare a spreadsheet summary for the day or month), and review the output (review the output and input the totals to the general ledger).
- *Lack of logical access.* Many off-the-shelf computer programs contain logical access controls, such as password protection. Unfortunately, entities often fail to install these controls or do so ineffectively.
- *Lack of adequate computer processing controls.* Most microcomputer accounting packages contain controls to ensure the accuracy of processing or to identify conditions that require user follow-up (for example, exception reports). Again, many entities fail to properly implement these controls.

When gaining an understanding of the entity's internal controls, be alert for weaknesses relating to the entity's use of microcomputers. An excellent source of additional information is *Auditing in Common Computer Environments*, an Auditing Procedures Study published by the AICPA.

Example Audit Procedures

The following audit procedures will help detect the frauds described above. Depending on your assessment of the risk of material misstatement due to fraud, these procedures may be performed as part of an audit conducted in accordance with GAAS. Alternatively, they may be performed outside the scope of a GAAS audit. If these procedures are already being performed, consider expanding their extent, for example by selecting more items.

- Review documentation supporting a selection of financial transactions or file maintenance procedures.
- Review error reports, batch processing totals, and other user controls over the input and processing of financial transactions or file maintenance procedures.
- Reconstruct accounts or files from original source documents.

Expanding Your Internal Control Questionnaire

Your internal control questionnaire may have questions aimed at identifying your client's vulnerability to computer fraud. Make sure that the person completing the questionnaire understands the implication of these questions. "No" responses may not change your control risk assessment or your assessment of the risk of material misstatement due to fraud. As a client service matter, however, you should consider discussing these items with your client and explaining how the lack of certain controls leaves the company exposed to fraud.

In addition, you may wish to review the control objectives enumerated for this area in the 1992 *Internal Control—Integrated Framework* or the principles and attributes enumerated in the 2006 *Internal Control over Financial Reporting—Guidance for Smaller*

Public Companies. Deficiencies in control design or operating effectiveness are an invitation for fraud to occur.

TABLE 10.9 INTERNAL CONTROL QUESTIONS RELATED TO FRAUD

| Computer Schemes | Yes | No |
|--|------------|-----------|
| 1. Is there a proper segregation of duties between the authorization of input, the preparation of input, and the reconciliation of output? | _____ | _____ |
| 2. Are employees with computer input duties required to take vacations, and are other employees cross-trained to perform those functions when an employee is absent? | _____ | _____ |
| 3. Is there a proper segregation of duties between computer programmers and computer operators? | _____ | _____ |
| 4. Has the company implemented effective logical access controls, including access to application programs, master files, and databases? | _____ | _____ |
| 5. Does the company have adequate controls to ensure the adequacy and legitimacy of input data? | _____ | _____ |
| 6. Does the company have adequate controls to ensure that changes to computer applications are authorized and they function as planned? | _____ | _____ |
| 7. Are exception reports, error listings, and other computer-generated items that require user follow-up investigated and resolved in a timely manner? | _____ | _____ |
| 8. Are spreadsheets and other microcomputer applications used to process significant accounting information checked for accuracy by someone other than the person who prepared it? | _____ | _____ |

**Extended Audit Procedures
Fraudulent Financial Reporting**

Inventory

Typical Frauds

Inventory frauds are perpetrated to manipulate earnings—inflated ending inventory balances reduce the amount of reported cost of goods sold, which results in improper increases to gross profit and net income. The usual method for inflating ending inventory is to report fictitious inventory amounts. This can be done in numerous ways, including:

- Altering quantities reported on inventory count tags that were not checked by the auditors.
- Entering inventory count tags for nonexistent inventory.
- Shifting the same inventory between several different locations.

- Altering or disguising the physical characteristics of inventory items to make it appear as if larger quantities are on hand. For example, hollow stacks of inventory that are made to appear solid, or inventory boxes filled with weights.

In other instances, management may be predisposed to understate beginning inventory balances, which has the same desired effect of increasing current period earnings. For example, this scheme may be perpetrated when there has been a change in management, and current management wishes to report improved profitability. The most common method for understating beginning inventory is to overstate the allowance for inventory obsolescence.

What to Look For

Be alert for the following, which may be present when the frauds described above are occurring or have occurred.

- Inability to produce all inventory count tags.
- Lack of control over the population of used count tags.
- Slow inventory turnover; increases in certain types of inventory or in branches or other locations not examined by auditors.
- Inability to produce vendor invoices supporting purchases (for example, invoices unavailable while performing price test work).
- Significant changes in gross profit percentages.
- Large unexplained reconciling differences between the inventory amounts recorded on the books and the physical inventory count.
- Large increases in inventory balances without corresponding increases in purchases.
- Journal entries made directly to the inventory account and not through the purchases journal.

Example Audit Procedures

Your primary audit procedure relating to the existence of inventory is the physical inventory count. The following audit procedures, performed during the physical inventory count, will help detect the frauds described here. Depending on your assessment of the risk of material misstatement due to fraud, these procedures may be performed as part of an audit conducted in accordance with GAAS. Alternatively, they may be performed outside the scope of a GAAS audit.

- Account for all inventory tags used during the physical count.
- Expand the number of test counts.
- Rigorously examine all items counted, for example by opening sealed boxes to observe the contents.
- Perform physical inventory counts at all locations simultaneously.
- Use the work of a specialist to help determine the quality (for example, the purity, grade, or concentration) of the inventory items.
- Perform analytical review procedures of gross profit; analyze according to location or inventory type.

- Perform analytical review procedures of inventory balances and purchases; analyze according to location or inventory type.
-

**Extended Audit Procedures
Fraudulent Financial Reporting**

Overvalued Assets

Typical Frauds

Overvaluing assets is a relatively simple way to directly manipulate reported earnings because overstated assets usually result in understated expenses. Common schemes for reporting overvalued assets include:

- Improper capitalization of costs that should have been expensed.
- Failure to recognize impairment losses on long-lived assets.
- Recognition of fictitious assets, for example, through the use of related-party transactions, the manipulation of intercompany accounts, or the failure to write off expired assets.
- Recognition of assets that the company does not have title to.
- Unreasonable or unsupported asset valuation allowances.
- Unreasonable or unsupported estimates of fair value, for assets required to be reported at fair value.
- Improper classification of marketable securities such as trading, available-for-sale, or held-to-maturity.
- Manipulation of depreciation expense, for example through unreasonable assumptions about the useful lives of assets or their residual values.

What to Look For

Be alert for the following, which may be present when the frauds described above are occurring or have occurred.

- Unusually high fixed-asset balances, when compared to total assets or to comparable entities.
- Unrealistically large changes in asset balances.
- Unusual or unexplained relationship between depreciation expense and fixed asset balances.
- Events or changes in circumstances that indicate assets may have been impaired.
- Missing documents related to asset transactions.
- Journal entries affecting the reported amount of assets, particularly entries made near the end of the reporting period or those that are unsupported or unauthorized.
- Unusual discrepancies between the entity's asset-related records and the general ledger.

Example Audit Procedures

Auditors have an advantage when auditing for overvalued assets because they direct their audit procedures toward *an amount the entity has already recorded*. This is much easier than trying to detect transactions or amounts that the entity has *not* recorded, such as unrecorded liabilities. In addition to your normal procedures to address the assertions related to assets, you also might consider performing the following:

- Extending the scope of detailed audit procedures related to the acquisition of fixed assets, such as the examination of supporting documents.
- Physical observation of fixed assets.
- Confirm the terms of significant fixed asset additions with the counterparty to the transaction.
- Confirm that the entity has title to reported assets through a review of relevant legal documents or public records.

Extended Audit Procedures Fraudulent Financial Reporting

Underreported Liabilities

Typical Frauds

The fraudulent underreporting liabilities can have a direct positive effect on an entity's financial position and its reported earnings. Common schemes to underreport liabilities include the following:

- Understating accounts payable, for example, by recording purchases in subsequent accounting periods, overstating purchase returns, or falsifying documents that make it appear liabilities have been paid off.
- Recognizing unearned revenue as earned revenue.
- Failure to record all debt or other liabilities.
- Failure to recognize contingent liabilities.
- Underreporting future obligations, such as warranty costs.

What to Look For

Be alert for the following, which may indicate that one of the frauds mentioned above is occurring or has occurred.

- Unusual or unexplained trends in accounts payable balances or differences between the entity's payables balances and those of comparable entities.
- Evidence of contingent liabilities in attorney's letter responses, correspondence from regulatory agencies or others, or other information gathered during the engagement.
- Significant purchases of assets with no recorded debt.
- Unusual or unexplained relationships between interest expense and recorded liabilities.

- Unexplained significant decreases in liabilities.
- Unusual relationship between the trend in the accrual for estimated warranty expense and sales.
- Receiving reports received near the end of the reporting period without a corresponding invoice.
- Amounts listed on vendor's statements that were not reported as purchases.
- Discrepancies in debt confirmations.
- Obligations reported as being discussed by management in the entity's minutes, but not reported in the accounting records.

Example Audit Procedures

In addition to the audit procedures typically performed related to liabilities, you might also consider the following:

- Perform lien searches on entity properties to search for unrecorded debt.
- Confirm the existence and terms of liabilities, including payables, with third parties.
- Read internal correspondence and correspondence between the entity and third parties to identify the existence or possible underreporting of liabilities.

10.8 CHECKLIST: DETECTION OF FINANCIAL STATEMENT FRAUD

This checklist addresses internal controls issues, taken from the discussion in this chapter, specific to suspected financial statement fraud. The checklist is an addition to Section 1.5, "Risk Management Checklist," and Section 2.2, "Ethical Environment Checklist," of this *Handbook*.

This checklist is intended for general guidance and information only. Use of the checklist does not guarantee the prevention or detection of fraud and is not intended as a substitute for audit or similar procedures. Those with vital concerns about fraud prevention or who suspect fraud should seek the advice of a competent fraud practitioner.

TABLE 10.10 FINANCIAL STATEMENT FRAUD CHECKLIST

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|---|--------------------------|--------------------------|--------------------------|-------|
| 1. Motives | | | | |
| <i>A Yes answer to any of the questions in this section indicates a greater likelihood of potential financial statement fraud.</i> | | | | |
| a. Is there a perception among management of the company or of individual operating units that there is extraordinary pressure (over and above the pressures typically associated with this industry) to achieve a higher level of reported earnings? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

(continued)

TABLE 10.10 (continued)

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| b. Do management compensation agreements tie compensation or bonuses to higher levels of reported earnings? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Is there extraordinary pressure from outside shareholders or other outsiders to improve the value of company stock? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. With regard to shares held by management or major shareholders, could the existence of any of the following provide an incentive to maintain or increase reported earnings, especially in the near term? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Vesting provisions in employee stock ownership plans that postpone ownership. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Stock option exercise restrictions that prevent managers from acquiring shares until specified dates or the occurrence of specific events. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Rule 144A restrictions that limit the number of shares that can be sold on United States securities exchanges on a given trading day. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Income tax provisions that afford more favorable treatment to capital gains in shares held for a sufficient period of time to qualify as long-term capital gains (the restriction being that the government would receive more of the sale proceeds if the share sales were classified as short-term capital gains). | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Corporate control requirements that necessitate holding significant blocks of stock past some event such as an annual shareholders meeting before they can be sold. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Is the company in danger of losing its listing on a major stock exchange, or is it attempting to obtain a new listing? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. If the company is publicly traded, is there extraordinary pressure to meet analysts' or market expectations, whether explicitly stated in published reports, public filings or public statements by company officials or implicitly perceived by management? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. Is there extraordinary pressure, whether explicit or implicit, to continue to report a rising trend in earnings and/or revenues? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| h. Is the company operating close to or in violation of the limits of financial covenants, such as minimum shareholders' equity, maximum debt-to-equity ratios or minimum current ratios, contained in bank credit facility agreements or other debt instruments? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| i. For firms doing business in regulated industries, is the company operating close to or in violation of the financial restrictions set by regulators or by statute? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

TABLE 10.10 (continued)

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| 2. Quantitative Characteristics | | | | |
| <i>A Yes answer to any of the questions in this section indicate a greater likelihood of potential financial statement fraud.</i> | | | | |
| a. When calculating the following indexes for the previous and the current year, do any of the indexes show a year-over-year increase greater than 10 percent (i.e., an index greater than 1.1)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Days' Sales in Receivables Index | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Gross Margin Index | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Asset Quality Index | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Sales Growth Index | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. When calculating the following indexes for the previous and the current year, do any of the indexes show a year-over-year increase greater than 10 percent more than increases for similar indexes of peer (same industry) companies? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Days' Sales in Receivables Index | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Gross Margin Index | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Asset Quality Index | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Sales Growth Index | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Is the change in working capital over the past year (excluding cash changes) relative to total assets at the end of the period more than 20 percent greater than similar calculations for peer companies? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Qualitative Predictors: The Audit Committee | | | | |
| <i>A Yes answer to any of the questions in this section indicate a need to take action to improve the integrity and effectiveness of the Audit Committee.</i> | | | | |
| a. Has the board of directors failed to designate an audit committee or failed to approve a charter for an audit committee? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. If there is an audit committee, do any of the following conditions exist with regard to members of that committee? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● A director being employed by the corporation or any of its affiliates for the current year or any of the past five years. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● A director accepting any compensation from the corporation or any of its affiliates other than compensation for board service or benefits under a tax-qualified retirement plan. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 10.10 (continued)

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|---|--------------------------|--------------------------|--------------------------|-----|
| <ul style="list-style-type: none"> ● A director being a member of the immediate family of an individual who is, or has been in any of the past five years, employed by the corporation or any of its affiliates as an executive officer. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● A director being a partner in, or a controlling shareholder or to which the corporation made, or from which the corporation received, payments that are or have been significant to the corporation or business organization in any of the past five years. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● A director being employed as an executive of another company where any of the corporation's executives serves on that company's compensation committee. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Are there less than three audit committee members with at least some financial accounting experience? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Is it not clear or not the case that: | | | | |
| <ul style="list-style-type: none"> ● The audit committee should be responsible for selecting the outside auditors. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● The audit committee has a formal written statement from the outside auditors describing all relationships between the auditors and the company. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● The audit committee regularly discusses with the outside auditors all aspects of the propriety or lack thereof of the company's accounting practices. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| <ul style="list-style-type: none"> ● The audit committee receives all reports of internal control deficiencies in a timely manner from both internal and outside auditors? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 4. Other Qualitative Predictors | | | | |
| <i>A Yes answer to any of the questions in this section indicate a greater likelihood of potential financial statement fraud.</i> | | | | |
| a. Has the company had a history of internal control problems, whether those problems resulted in detection of financial statement or any other type of fraud? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. Does the company CEO engage in micro-management or other practices that could unduly influence accounting decision-makers with regard to financial statement reporting? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Are financial statements presented to the board of directors or to outsiders (banks, minority investors, etc.) prepared on a basis other than GAAP? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Are outside auditors unaware of any interim or quarterly financial statements, or financial statements prepared for selected outside parties such as banks or investors? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

TABLE 10.10 (continued)

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| e. In establishing and reviewing internal controls, has management failed to establish adequately the key metrics or guidelines to determine the extent and frequency of internal auditor review? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Is there a lack of evidence that management has properly communicated the internal control guidelines and procedures to appropriate personnel? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. If there is no audit committee, does the firm lack procedure for reporting accounting irregularities to the entire board, either directly or through senior management? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| h. Does it appear that management does not assess the quality of its internal controls over time? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| i. If the firm is not audited annually, has more than one year elapsed since either outside accountants or internal auditors have reviewed all internal controls? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| j. Have any audit tests detected significant risks not previously known to management? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| k. Is there a history of using a quantitative standard for materiality, such as a percentage of earnings or assets, to fail to correct known accounting errors or irregularities? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 5. Special Areas | | | | |
| <i>A Yes answer to any of the questions in this section should generate further inquiry to determine if specific internal controls need to be improved.</i> | | | | |
| 1. Failure to Record Loss Contingencies | | | | |
| a. Given the nature of the company's business, is it likely that any of the following issues could be relevant? | | | | |
| ● Collectibility of receivables | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Obligations related to product warranties and product defects | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Risk of loss or damage of enterprise property | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Threat of expropriation of assets | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Pending or threatened litigation | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Actual or possible claims and assessments | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Guarantees of indebtedness of others | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Agreements to repurchase receivables (or repurchase related property) that have been sold | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

(continued)

TABLE 10.10 (continued)

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| b. With regard to possible contingencies, does there exist: | | | | |
| ● The incidence of claims prior to the date of financial statements | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Correspondence with (and bills from) outside legal counsel | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Internal correspondence within production and research staffs as to the need to address a critical problem with a product already on the market | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Internal correspondence among department heads of production, R&D, general counsel, and senior management about postproduction problems and product claims | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● External correspondence between the manufacturer and its customers about a given product concerning special price concessions or special return privileges | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● The incidence of special or over-budget freight charges to accommodate returns and/or the shipment of replacement product | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Shifting of production schedules to manufacture replacement product | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Halting manufacture of the product in question | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Shifting of R&D staff away from planned research projects to applications engineering relating to redesign of existing products | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Payments in sometimes seemingly immaterial amounts to customers on a regular basis over a period of weeks or months that indicate some arrangement to compensate for product defects | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. If there is a suspected contingency, does correspondence between departments or within departments indicate a problem? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. If a contingency is likely to exist, has management used an inadequate or inappropriate standard for quantifying the potential claim? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 2. Failure to Record Asset Writeoffs | | | | |
| a. Has the company's industry experienced rapid changes in engineering or materials applications that may lead to asset write-offs? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. Is the industry in which the company operates very cost-competitive? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

TABLE 10.10 (continued)

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| c. Has the company experienced: | | | | |
| ● Significant changes in customer demand | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Significant loss of business to a competitor | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● A need to obtain or retain a customer relationship by bidding below cost | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. When reviewing fixed asset schedules with production or divisional personnel, have any of the following occurred? | | | | |
| ● A significant decrease in the market value of an asset | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● A significant change in the extent or manner in which an asset is used or a significant physical change in an asset | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● A significant adverse change in legal factors or in the business climate that could affect the value of an asset or an adverse action or assessment by a regulator | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● An accumulation of costs significantly in excess of the amount originally expected to acquire or construct an asset | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● A current-period operating or cash-flow loss combined with a history of operating or cash-flow losses or a projection or forecast that demonstrates continuing losses associated with an asset used for the purpose of producing revenue | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Is there evidence of significant changes in production or product demand? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. From the review of moving expenses and discussion with production personnel, does it appear that any equipment has been moved off the shop floor into storage? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| g. Does the company not maintain profitability analyses by product line or by customer? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| h. Upon reviewing profitability analyses, does it appear that certain products have not been historically profitable? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| i. For historically unprofitable product lines, to justify not writing down assets for impairment, has management used: | | | | |
| ● Overly optimistic forecasts of future profitability | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Out-of-date forecasts | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Forecasts not prepared or reviewed by personnel with line responsibility for production | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| j. If written narratives accompany the forecasts, do they discuss downside possibilities that management has not adequately taken into account? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 10.10 (continued)

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| k. Are there any facts now known that would invalidate assumptions contained in the forecast? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| l. For investments in nonpublicly traded securities: | | | | |
| • Does the company have financial data adequate to determine historical profitability of the investee? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| • If the investee has not been historically profitable, has management failed to write down the investment based upon an overly optimistic forecast? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| • If the investee has not been historically profitable, has management failed to write down the investment based upon a forecast prepared by management with business or family ties to the investor company? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 3. Acquisition and Cookie-Jar Reserves | | | | |
| a. Were reserves established without a clear purpose or justification? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. If reserves were established by a current period charge to income, were earnings prior to the charge in excess of management or outside expectations? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Were reserves established at or near the close of a reporting period? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Were reserves established without adequate review by senior management? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Upon review of charges to a given reserve, are there charges for expenses that are not appropriate to the stated purpose of the reserve? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Was the timing of the take-down of reserves coincident with achieving certain financial targets set by management or outsiders? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. Was the amount of the take-down of reserves for a given period necessary to achieve certain financial targets set by management or outsiders? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| h. For acquisition reserves: | | | | |
| • Were reserves established after twelve months from the date of the acquisition? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| • Were reserves set up for items not related to the acquisition? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| • Does the quantity of costs allocated to the reserve in a given period cause earnings to reach certain financial targets set by management or outsiders? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

TABLE 10.10 (continued)

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| 4. Cost Shifting | | | | |
| a. Has management made a recent change in policy with regard to capitalizing previously expensed costs? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. Has a change in policy with regard to capitalizing previously expensed costs not been disclosed in company financial statements? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Has management proposed to capitalize a new category of expenditure that customarily is expensed on peer-group firm financial statements? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Does the timing of changes in policy with regard to capitalizing expenses coincide with: | | | | |
| ● Implementation of a management bonus plan or calculation of bonuses under that plan | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Commencement of the sale of stock or the search for an equity partner | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Implementation of a new credit facility or recent problems in maintaining financial covenants under an existing facility | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. But for the capitalization of certain expenses: | | | | |
| ● Would management not receive certain bonuses or other benefits under a management compensation plan? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● In the opinion of securities analysts, appraisers, or underwriters, would the company's share price be significantly lower? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Would the company be in violation of loan or debt covenants? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Does the capitalization of expenses cause the firm's Asset Quality Index to increase significantly in excess of increases (if any) for its industry peers? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. If company management provides segment or subsidiary financial data, especially if management or outsiders tend to point to performance of that segment or subsidiary in their discussions of company performance: | | | | |
| ● Have expenses been incurred by the parent that relates to the segment or subsidiary? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Have other segments or subsidiaries incurred expenses that should be allocated to the segment or subsidiary in question? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

(continued)

TABLE 10.10 (continued)

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| h. Has senior management failed to establish proper procedures for allocating or apportioning costs among affiliates or, if there is a policy, is there evidence that adherence is lax or that there have been documented lapses? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| i. Is there correspondence among heads of affiliates concerning disputes over expense allocations or apportionment that has not come to the attention of the audit committee? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| j. Were reserves established at the parent company for expenses anticipated for subsidiaries? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| k. Are there debit entries in subsidiary expense or liability accounts that could reflect cost transfers to the parent or another subsidiary? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| l. Are there debit entries in subsidiary expense or liability accounts that could reflect cost transfers to reserves established at the parent level or in another subsidiary? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| m. Is there any correspondence between accounting personnel at the parent and subsidiary levels that describe special procedures for certain costs that are incurred by the subsidiary but not charged to earnings of that subsidiary? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 5. Recording Fictitious Revenues | | | | |
| a. If the company requires signed agreements from customers before revenue is recognized: | | | | |
| • Have sales personnel indicated that their managers have approved as income sales contracts that were not signed as of the period end? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| • Have sales personnel stated that unsigned contracts were recorded as revenue under the premise that key buyer personnel had given verbal approvals? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| • Have sales personnel stated that unsigned contracts were recorded as revenue under the premise that key buyer personnel had signed the contract but the contract was held up for other reasons? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. Have there been prior internal control failures with sales cutoff? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. If fabricated contracts are suspected, have the sales cutoff tests performed by internal or outside auditors failed to look for the fabrication and substitution of contracts? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Have sales cutoff tests failed to examine the history of sales returns and reversals over time? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. With regard to the requirement for timely delivery: | | | | |
| • Are there lapses in documentation of delivery? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

TABLE 10.10 *(continued)*

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| ● Have customers complained about receiving deliveries too early? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Have returns from a certain customer or reseller been abnormally high? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Is there evidence that certain customers or resellers are receiving unusually generous sales terms for returns or refunds? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. Is there evidence that certain customers or resellers are receiving unusually low prices or above-average discounts? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| h. Is the price for component products sold by the company dependent, at least in part, upon the price of the final product sold by another company? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| i. Have royalties been accrued to income prior to receipt of confirmation from the payer that royalties are owed? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| j. Do department heads have the authority to both approve sales and the recognition of related revenue in the financial statements? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| k. Is there a lack of review of sales revenue recognition at the senior management level? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| l. Is there a history of revenue being recognized improperly? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| m. Have department heads approved significant refunds or returns that are out of the ordinary or appear to violate company policies? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| n. Have refunds or returns been historically high for a certain department? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| o. Have the reasons for refunds and returns not been documented or, if documented, have the reasons given been insufficient? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| p. Has senior management failed to review or been lax in reviewing significant sales refunds and returns? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| q. If side letters are suspected: | | | | |
| ● Have engineers, technicians, or others involved with the installation of the products indicated that certain customers made additional demands before agreeing to buy? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| ● Are there notes or letters in sales files indicating customer demands had been made to allow for returns or refunds? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| r. Are sales approved before obtaining credit checks for new customers or for existing customers that are experiencing financial difficulties? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

(continued)

TABLE 10.10 *(continued)*

| Financial Statement Fraud Checklist | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| s. Is there an unusual concentration of orders from small or distressed customers occurring near the end of a reporting period or sales contest? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

10.9 CHECKLIST: SARBANES-OXLEY

This checklist addresses control issues affecting the internal control over financial reporting required by the SEC final rule for compliance with the Sarbanes-Oxley Act of 2002.

This checklist is intended for general guidance and information only. Use of the checklist does not guarantee compliance or the prevention or detection of fraud and is not intended as a substitute for audit or similar procedures. Those with vital concerns about compliance and fraud prevention or who suspect fraud should seek the advice of a competent fraud practitioner.

A No answer to any of the questions in this checklist indicates a greater likelihood of potential noncompliance and fraud.

TABLE 10.11 INTERNAL CONTROL OVER FINANCIAL REPORTING CHECKLIST

| Sarbanes-Oxley Checklist | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| 1. Ethics | | | | |
| a. Does the company have a written code of ethics? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Is the code of ethics distributed to all employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Is there ongoing ethical education for all employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. Audit Committee | | | | |
| a. Has an audit committee been established? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Does the committee understand its duties? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Does at least one member meet the definition of “financial expert” as defined by the Sarbanes-Oxley Act? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Are all members independent as defined by the Act? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Has the committee set up a process by which it may receive and review complaints including those from whistleblowers? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. Has each member of the committee received and read the new Auditing Standards Numbers 1 and 2 and the proposed Number 3 from the PCAOB? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| g. Has each member of the committee received and read the SEC final rules? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| h. Has each member of the committee received a copy of and read <i>Internal Control—Integrated Framework</i> , published by COSO? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Control Over Financial Reporting | | | | |
| a. Has a committee been established or a senior person designated to implement the SEC final rules to make the enterprise compliant with the Sarbanes-Oxley Act? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Has each member of senior management received and read <i>Internal Control—Integrated Framework</i> published by COSO? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 10.11 (continued)

| Sarbanes-Oxley Checklist | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| c. Is the COSO or equivalent framework being used to evaluate the effectiveness of the internal control over financial reporting? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Do the CEO and CFO understand the elements of the company's internal control system, including the control environment, that must be reviewed in order to attest to the effectiveness of internal control over financial reporting? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Do the other members of the management team understand the elements of the company's internal control system that must be reviewed in order to attest to the effectiveness of internal control over financial reporting? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Is the internal control system evolving as the company grows and changes? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. Does the internal control over financial reporting record a description of authorized transactions? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| h. Does the internal control over financial reporting classify transactions according to their description? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| i. Does the internal control over financial reporting place the transaction in its proper accounting period? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| j. Does the internal control over financial reporting enable transactions to be included in periodic financial reports? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| k. Are there any design or operating deficiencies in the internal control system as defined by the PCAOB? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| l. Are there any significant design or operating deficiencies in the internal control system as defined by the PCAOB? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| m. Are there any design or operating material weaknesses in the internal control system as defined by the PCAOB? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| n. Would any resultant material misstatement meet the test of materiality as defined by SAB No. 99? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| o. Do those persons responsible for the financial reporting process understand the distinction between "internal control over financial reporting" and "disclosure controls and procedures"? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| p. Has a committee been established to oversee the implementation of disclosure controls and procedures? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| q. Is there a system of disclosure controls and procedures in place that will ensure compliance with SEC reporting requirements? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| r. Can the control system distinguish between error and fraud? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| s. Does the documentation describe the results of any management tests of the effectiveness of the internal control over financial reporting? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

TABLE 10.11 (continued)

| Sarbanes-Oxley Checklist | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| t. Have the internal controls reporting project team management members received and read PCAOB Auditing Standard No. 2, (as suggested by the SEC) to identify the details of company compliance (e.g., communications with auditors, scope of controls examinations, etc.) not enumerated in SEC documents? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| u. Does the documentation describe accounting policies used and how they conform to GAAP? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| v. Has all system testing been done in a timely manner to meet the “as of” requirement for Sarbanes-Oxley compliance? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| w. Have all material weaknesses been disclosed to the CEO and CFO? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| x. Are the CEO and CFO aware they must sign an attestation to the establishment and effectiveness of internal control over financial reporting? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| y. Are the CEO and CFO aware the external auditor must review the basis of their attestation and sign off on it? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| z. Has management reviewed the PCAOB documents describing the suggested phraseology of its report? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| aa. Is the external auditor being given all the help needed to review the internal control over financial reporting and provide “reasonable assurance” as to its effectiveness? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

7

7

7

CHAPTER 11:

Corporate Security: Threat and Crisis Management

| | | |
|--------|--|----|
| 11.1 | Overview | 3 |
| 11.2 | The Threat | 4 |
| 11.2.1 | Identifiable Threats..... | 4 |
| 11.2.2 | Vulnerabilities..... | 5 |
| 11.2.3 | Some Risks of Greater Concern..... | 6 |
| 11.2.4 | Relative Vulnerability | 7 |
| 11.3 | Planning and Prevention..... | 8 |
| 11.3.1 | Post-September 11 Crisis Management..... | 8 |
| 11.3.2 | Elements of a Corporate Security Review | 8 |
| 11.3.3 | The Threat Assessment Process | 9 |
| 11.3.4 | The Comprehensive Risk Assessment Process..... | 10 |
| 11.3.5 | Preventing and Detecting Security Breaches | 12 |
| 11.4 | Crisis Management | 16 |
| 11.4.1 | Essentials of a Threat and Crisis Management Plan | 16 |
| 11.4.2 | Denial of Insurance Coverage for Terrorist Acts | 21 |
| 11.5 | Corporate Security Checklists | 24 |
| 11.5.1 | Comprehensive Risk Assessment..... | 24 |
| 11.5.2 | Threat and Crisis Management Planning..... | 28 |
| 11.5.3 | Financial Issues to Address When Disaster Strikes | 33 |
| 11.6 | The Kroll October 2001 Survey on Security Risk Management..... | 36 |

CHAPTER 11:

Corporate Security: Threat and Crisis Management

11.1 OVERVIEW

In a world as unpredictable as ours, events are often beyond our control. There are natural disasters; there are accidents; and there are intentional catastrophes. The September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon are a chilling reminder of the last category. Although certain threats may be totally unforeseen, appropriate security measures can sometimes prevent losses, and appropriate crisis management planning can help to minimize the impact when disaster strikes. Whether the threat relates to fraud committed by an insider or an extremist who has threatened the lives of some of your employees, there are a variety of security measures that can be undertaken to minimize your company's vulnerability.

When the events of September 11 unfolded, certain companies were prepared to handle the ensuing crisis after the 1993 bombing of the World Trade Center had caused them to consider and address their weaknesses. Many companies, however, were not prepared.

A survey conducted by Kroll Associates in October 2001 (included at the end of this chapter) of business executives in New York, Boston, and Toronto revealed that the awareness and concern of the business community for security risk management had increased dramatically since September 11, and many executives now believed their security risk management systems needed upgrading. Previously, the main security-driven priorities had been employee integrity and information security, but this list has expanded to include the physical security of both a company's assets and its people. Awareness of the importance of appropriate security measures has also increased. But *what* is appropriate? Each company's circumstances, needs, and risk profiles are different, so the security measures that are appropriate for one company may not be sufficient for another.

This chapter has been written to assist in defining this *what*. It identifies the types of threats that a business faces, and then goes through the primary considerations for an effective security plan to prevent or detect such threats so that you, as a CPA, can be better informed of the need for security, and the types of security measures that should be undertaken. There are certain threats, however, that no plan can prevent but their effects may be mitigated by a good recovery plan.

11.2 THE THREAT

11.2.1 Identifiable Threats

There are a wide variety of threats to a business, ranging from natural threats to those that are either intentionally or unintentionally caused by people. There are conventional threats that have existed for hundreds of years, and there are more contemporary threats that arise from technological advances. Threats associated with civil unrest, war, and terrorism have become a way of life in some parts of the world, whereas North America and other parts of the world have enjoyed relative stability in recent years, and these threats are only now being considered seriously.

In order to set up appropriate security measures, it is necessary to identify all imaginable threats. The next step in the security process is to assess the likelihood of such threats becoming reality. What follows is an extensive but not all-inclusive list of the potential threats:

- Theft and other intrusions include the following:
 - Theft
 - Armed attacks, for example, bank robbery, and so on
 - Vandalism and other malicious acts
 - Systems intrusion
- Water damage may result from the following:
 - Flood
 - Tidal waves or storm surge
 - Drought
 - Water pollution
- Fire includes the damage from either of the following:
 - Fire
 - Smoke
- Accidents and mechanical breakdowns can arise from the following:
 - Vehicular accidents
 - Equipment malfunctioning
- Utility interruption may involve the following:
 - Water, power, utility, and communication outages
 - Fuel shortages
- Earth movements include the following:
 - Earthquakes
 - Avalanches and landslides
 - Volcanic eruptions
- Weather conditions can be any of the following:
 - Extreme cold and extreme heat
 - Snow, ice, and hail

- Typhoons, tornadoes, and hurricanes
- Dust and sandstorms
- Lightning storms
- Infestations
- Threats to the safety of a company's personnel can include the following:
 - Kidnap and ransom
 - Hostage-taking
 - Workplace violence, such as physical assault or assault with lethal weapons
- Bomb threats and explosions can be caused by the following:
 - Suicide bombings
 - Conventional bombs
- Civil disorder can arise from the following:
 - Riots, strikes, and demonstrations
 - Warfare, including attacks that could be conventional, biological, chemical, or nuclear
- Hazardous materials present the following dangers:
 - Intentional contamination that could be chemical, biological, or radioactive
 - Accidental contamination that could be chemical, biological, or radioactive
- Cyber attacks can include any of the following:
 - Theft of information
 - Misinformation about your company on the Internet
 - Denial of service
- Corruption of the system can involve disruption of any of the following:
 - 911 emergency response system
 - Electric power grids
 - Water supply
 - Telecommunications
 - Air traffic control
- Terrorist acts, conducted by individuals or groups with an ideological agenda, and can include any of the above threats, but often include the following:
 - Kidnap and ransom or hostage-taking, or both
 - Workplace violence
 - Bomb threats and explosions
 - Hazardous materials contamination

11.2.2 Vulnerabilities

There are four primary aspects of a company that are vulnerable to security threats: physical assets, including premises and equipment; people; information; and reputation.

A company's *physical assets* include all of its premises, for example, manufacturing locations, showrooms, head office and warehouse facilities, as well as equipment such as computers and all the equipment used in the operational processes of the company. Such assets are vulnerable to access violations, malfunctions, theft or conversion, and destruction.

People are the lifeblood of an organization. Without adequate security measures and training, the people employed by a company can become victims of a kidnapping, be injured, or, in certain cases, become a fatality. If an employee is abducted, injured, or dies because of inadequate security measures, the employer also suffers not only because of the downtime caused by the loss of that employee, but also because of the impact on the other employees, and the effect on the company's reputation. The people in a company who are the most vulnerable include expatriates in foreign jurisdictions, traveling executives, employees who deal directly with the public, employees who are operators of sophisticated equipment or who have critical skill sets and knowledge of company processes and procedures, and security personnel.

Information that needs to be protected includes information that is stored electronically on computers, networks, tapes, drives, and disks as well as in paper files and books. Several companies destroyed in the World Trade Center attacks cited the loss of the company's history, often in the form of a commissioned book, as irreplaceable. Electronic information, however, is only one source of information that is vital to an organization. Other information that needs to be protected includes intellectual property such as trade secrets, product development ideas, competitive intelligence, customer lists, processes and procedures, training manuals, legal contracts, and accounting and tax records.

The *reputation* of a company represents its credibility and image as seen by its employees, customers and suppliers, shareholders, the general public, the media and regulatory authorities. A company's reputation is created by its actions and communications as well as the communications of other parties, all of which must be consistent, credible, and positive in order for that reputation to remain intact. If the security of a company has been breached, a company's reputation is vulnerable, particularly if the communications are not all positive. Effective communication, therefore, is vital to maintaining a company's reputation.

11.2.3 Some Risks of Greater Concern

The above-mentioned Kroll survey taken in October 2001 shows that there is a heightened awareness of the need for appropriate measures to protect against a wide range of threats to a company's security of which manmade threats now represent more of a concern than natural disasters.

The Kroll survey revealed that before September 11, the most important security issues related to threats from the following:

- Systems intrusion
- Computer and telecommunications failures, or both
- Fire and explosion

After September 11, these three issues continued to represent the greatest area of concern to executives. However, since the attacks, the degree to which these risks were considered important increased by at least 25 percentage points. For instance, 86 percent now viewed

systems intrusion as an important security issue compared to 61 percent who viewed systems intrusion to be important before. This represents an increase of 25 percentage points. Computer and telecommunications failures were considered to be important issues to address by 83 percent of respondents subsequent to the attacks, compared to 57 percent before; and the threat of fire and explosion was considered to be an important issue to be addressed by 77 percent of the respondents now, compared to 48 percent who considered it to be important before.

The Kroll survey also revealed that certain other security issues, previously considered to be less of a threat, have become much more of a concern than they were. Bomb and hazardous materials threats showed the biggest gain in importance (up 42 and 47 percentage points respectively to 71 percent each). More than half of the respondents considered the following threats to be important issues to address now, whereas less than a third of the respondents considered these to be important issues to address before September 11:

| Threat | Important Before September 11 (Percentage of Respondents) | Important After September 11 (Percentage of Respondents) |
|-------------------------|--|---|
| Bomb Threats | 29 | 71 |
| Hazardous Materials | 24 | 71 |
| Civil Disorder | 16 | 53 |
| Armed Attack | 22 | 52 |
| Hostage-Taking | 21 | 51 |
| Water and Power Outages | 44 | 66 |

The Kroll survey also shows that bomb threats and hazardous materials were considered to be more of a concern after the attacks than threats related to water and power outages, whereas before, water and power outages had been considered to be more of a concern.

11.2.4 Relative Vulnerability

All companies face security risks, some more so than others. The vulnerability of one company compared to another is a function of several factors, including the extent to which appropriate security measures have been implemented, the degree of security preparedness, and the geographic location and the nature of the company's operations.

Certain regulated industries, such as oil and gas, have mandated security procedures to mitigate known risks. They can, however, be vulnerable because they have limited security procedures related to other aspects of their operations. Companies in other industries can be vulnerable because they have few or no security measures in place.

The companies that face the biggest threat from a terrorist perspective are those whose activities could impact large numbers of people such as those that:

- Have large groups of employees at one location.
- Handle precious commodities.
- Handle toxic substances.
- Handle food and other items consumed by the general public.

11.3 PLANNING AND PREVENTION

11.3.1 Post-September 11 Crisis Management

The Kroll Survey revealed that in the aftermath of September 11, companies are more aware of the need to identify and assess risks and reduce vulnerability through planning.

For example, 89 percent now view physical security as important, compared to 40 percent before. Approximately 86 percent identified emergency planning as important, compared to 34 percent before. About 80 percent cited business resumption planning as important, compared to 38 percent before.

As a result, more companies are paying attention to their security needs than ever before, and many are hiring risk consultants to conduct corporate security reviews and make recommendations to improve their security and emergency preparedness.

This response is not only wise from the perspective of protecting a company's assets and its people, but it is also becoming more of a necessity for insurance reasons as more companies face rising insurance costs. Some companies are finding they cannot get insurance coverage unless they have adequate security and crisis management plans in place. Many insurers are looking for evidence that companies are taking all reasonable steps to mitigate their risks by conducting corporate security reviews and by the preparation of threat and crisis management plans. Companies that have conducted security reviews and that have threat and crisis management plans are better able to reduce their losses through improved security and are, therefore, more likely to get or retain their insurance coverage.

Certain risks, however, such as terrorist acts and acts of war, are no longer covered by most insurance companies. In the absence of insurance coverage, the ability of a company to cope with such acts quickly and effectively is the only way to minimize the losses that would otherwise be suffered.

11.3.2 Elements of a Corporate Security Review

A comprehensive corporate security review involves the following five steps:

1. Identify all the threats that a business faces (for instance, all the threats identified in the previous section of this chapter).
2. Conduct a threat assessment to consider the probability of each threat.
3. Conduct a comprehensive risk assessment of each sector of the business and each location.
4. Identify appropriate security measures to eliminate, avert, or minimize the risk of the most significant threats; or, if that is not possible, to provide an early detection system that warns of the existence of such threats.

5. Develop an effective threat and crisis management plan that covers all aspects of the business to help facilitate management's response to the threat or crisis, and, more than likely, to minimize the effects of business interruption.

11.3.3 The Threat Assessment Process

The threat assessment process involves assessing for each location and threat:

- The likelihood of each threat becoming a reality
- The severity of the impact of such a threat

More specifically, the issues to assess relative to each threat must include:

- Identifying whether the threat could affect the particular location under review.
- Identifying the frequency with which this threat is likely to recur (several times per annum, once every three years, once every ten years, once in a lifetime, once every hundred years, or highly improbable).
- Identifying whether the threat represents a significant threat to a company's operations, facilities, people, information, or reputation. Part of this assessment involves considering the number of people likely to be affected by the threat, recovery time, insurance coverage both to repair and replace damaged equipment or premises and to cover business interruption losses, and the financial impact.
- Identifying whether appropriate security measures are in place to prevent such a threat from materializing or to mitigate its impact.
- Determining the ease with which security measures could be introduced.

Such an assessment is subjective by nature. It is useful to make the assessment, however, as the process provides valuable information that can be used to prioritize the areas for review. This information can then be used to establish the priorities for implementing appropriate security measures to minimize the risks associated with these threats. This is particularly important when resources allocated to the implementation of appropriate security measures are limited.

Threats that would have a negligible impact but which are frequent threats should have a lower priority than threats that could cause catastrophic damage, even if they are only remote possibilities. The following table can be used to assist in assigning the relative priorities for addressing the threats faced by a business. Frequent threats with catastrophic consequences would be assigned an *A* priority, whereas improbable threats with negligible consequences would be assigned a *D* priority.

TABLE 11.1 ASSESSING THE RELATIVE PRIORITY FOR DEALING WITH EACH THREAT

| Frequency of Occurrence | Severity of the Risk | | | |
|-------------------------|----------------------|-------|-------|------------|
| | Catastrophic | Major | Minor | Negligible |
| Frequent | A | A | A | C |
| Occasional | A | B | B | D |
| Remote | A | B | C | D |
| Improbable | B | C | C | D |

11.3.4 The Comprehensive Risk Assessment Process

A comprehensive risk assessment is often done with the assistance of external experts and involves assessing the security-related controls and procedures that need to be in place to protect four basic areas of the business for each operating site:

- *Premises and equipment.* Assess the company's physical controls that prevent and detect unauthorized access.
- *People.* Assess the degree to which a company's personnel are aware of ways to avoid crises and what to do if they should occur. Risky travel destinations, for example, should be identified and travel advisories prepared for relevant personnel.
- *Information.* Assess the company's hardware and software controls to prevent and detect unauthorized access to information. The speed of recovery through the use of backup data should also be part of this assessment.
- *Reputation.* Assess the communication system that advises employees, customers, suppliers, shareholders, and the media.

The results of this overall assessment should be documented so that future assessments can consider whether there have been any changes to the company's vulnerability.

Premises and Equipment

The assessment of a company's premises and equipment must concern itself primarily with access and exit controls. The following is a list of the type of information that should be assessed for each facility:

1. Type of facility (corporate offices, retail outlets, and factories)
2. Location
3. Number of floors including a basement
4. Number of persons in each building and on each floor
5. Type of department on each floor
6. Type of equipment on each floor
7. Tenant and visitor access control
8. Alarms and monitoring in general
9. Access to loading docks
10. Access and surveillance of elevators and stairwells
11. Type of access technology (cards)
12. Closed circuit TV surveillance
13. Nature of businesses of other building tenants
14. History of security breaches and their correction

People

Putting in place an adequate plan to secure a company's premises and equipment is an important step in safeguarding a company's people but it is just a first step. Other aspects to assess affecting personnel include the following:

1. Educational material should be provided to executives, security personnel, and employees regarding the following security-related policies and procedures:
 - Mail and package handling processes
 - Evacuation procedures
 - Crisis management procedures
2. Company hiring practices should include screening and background checks. What is the awareness level of personnel with respect to political risks in the countries to which they are traveling?
3. Personnel awareness of corporate practices to address a crisis such as a bomb or biohazard threat and contingency plans in case of an emergency

Information

This section of the plan should concern itself primarily with unauthorized access to confidential information and the ability to restore or recover such information in the event that it is destroyed or otherwise corrupted. The following is a list of issues to be addressed in securing confidential corporate information:

1. Access the controls that exist to protect the company's computer(s) and the information stored in them.
2. Protect the company Web site from hackers.
3. Establish the frequency of data and software backups.
4. Provide for the offsite storage and security of backups.
5. Access controls to protect company accounting information, customer lists, manuals and procedures, patents, and processes.

Other computer security issues such as physical security, logical security and system recovery are addressed in Chapter 4, "Computer Security and System Recovery," of this manual. Also refer to Chapter 8, "Computer Crime and Computer Criminals."

Reputation

The security of a company's reputation depends on the effectiveness of control over all forms of communications affecting the company. The following is a list of how the types of information should be assessed to protect a company's reputation:

1. Clearly designate the persons authorized to speak for the company to the media, analysts, and shareholders.
2. Issue authorized press releases.
3. Train those persons who deal with the media.
4. Monitor the media for reports on the company.
5. Monitor chat rooms.
6. Develop a strategy for countering false information about company products or services in media or chat rooms.
7. Develop policies that clearly state the consequences of committing an act that is adverse to the interests of the company, such as fraud or the destruction of property.
8. Require that all personnel sign a statement acknowledging they have read and agreed to the policies.

11.3.5 Preventing and Detecting Security Breaches

The overall security plan of a company should be the responsibility of one independent security department and not fragmented among the functional areas of the business on the model of the internal audit and designed to protect premises and equipment, people, information, and reputation.

The following case illustrates what can happen when corporate security is not performed in this way.

Mining Security in a Global Setting Study

When the events of September 11, 2001, were over, members of the board of directors of a large multinational mining company started to ask themselves some hard questions about the security of their own operations. Would their company be able to handle a crisis that threatened to disrupt production at one of their mine sites? What security measures were in place to prevent access to the company's processing plants? The directors were surprised to find that the answers to these and other questions were unclear. It had quickly become apparent that the company needed to strengthen its security overall and to establish a crisis management plan to address a wide variety of threats to the company's operations, including threats associated with terrorist acts.

Management retained the services of an international risk consulting firm to help them address these questions, to conduct a comprehensive corporate security review of its worldwide operations, and to develop recommendations to improve security at each location.

The mining company had rapidly grown from a single-site mining operation in the United States to a multinational leader in the mining and processing of precious metals. This growth had been achieved through the acquisition of various complementary businesses and mine sites.

Security was quite comprehensive at some sites but lax or virtually nonexistent at others. At certain locations, there were sophisticated plans to protect the health and safety of the employees while, elsewhere, conditions invited breaches of security that could result in loss of property and/or harm to employees. This unevenness occurred because security was considered to be the responsibility of the plant manager at each location rather than that of a single company-wide security department. For instance, plant managers sometimes opted to use security personnel to do maintenance or clerical duties. While such duties were being performed, the security personnel were unable to perform their security duties. At these times, employees and others had free access to the site to steal inventory and supplies without being challenged.

Although individual plant managers did have an awareness of the need for security at their respective facilities, security was not their main priority. Costs related to the security function at their location were considered to be an overhead expense, and the plant managers' priority was to reduce overhead and improve earnings. As a result, recommendations for improved security measures in the past had been dismissed or shelved.

One of the primary recommendations from the risk consultant was, therefore, to integrate the security function at a corporate level by hiring an experienced security manager and having the security personnel at each site report to him. The risk consultant also recommended that the costs related to security personnel at each site should be accounted for as a head office cost and should be budgeted in a separate corporate security budget. This would prevent the plant managers from making decisions regarding security issues based on the impact on the profitability of each site.

Other recommendations by the risk consultant included the establishment of common access controls, the training of security personnel, and the instruction of all management personnel in the importance of security. Failure to comply with these policies and procedures would be punished.

The Mining Security case above illustrates several important points:

1. Security should be an integrated function with on-site personnel reporting all security matters to head office representatives at each location who report to head office. Administrative matters would be handled locally.
2. Security costs would be a head-office cost rather than local overhead.

Set out below are a number of security measures that are typically recommended for the protection of a company's premises and equipment, people, information and reputation.

Premises and Equipment

The effective use of guards is essential.

- Use the services of competent uniformed guards who are actively involved in protecting the facility rather than doing other jobs such as driving buses and groundskeeping.
- Change the corporate mentality to make each employee consider himself or herself a guard. Everyone has a responsibility to be on the lookout for possible breaches of security.

Controls to authenticate and authorize access should include the following:

- Establish access controls through the use of cards and card readers to prevent unauthorized entry to the facilities. Establish additional access controls to network hubs and other critical areas within the facilities.

- Insist that employees wear photo identification badges with security features to be produced together with their access cards. This not only inexpensively improves security but by its very nature increases the level of security awareness across all departments.
- Install an alarm button for the reception area to be monitored continuously whenever reception is open.
- Use biometric technology such as facial and iris recognition.
- Install entry cameras at all access points.

Exit controls to prevent unauthorized departures should restrict use of:

- Stairwells for emergency exit only. This can be accomplished by installing audible alarms on each access door and tying these into the building alarm system.
- Freight elevators.

Procedures relating to bomb threats, weapons, and hazardous materials:

- Install magnetometers and implementing bag checks for all personnel entering the site.
- Prevent unattended curbside parking around the building without a permit.
- Conduct vehicle inspections of all vehicles entering the loading bay where applicable.
- Inspect all storage areas and vehicles carrying hazardous materials for leaks.

People

Screening in the form of employee background checks (also important for preventing internal fraud as is discussed more fully in Chapter 5) is essential in any security plan. Such screening should include the following:

- Pre-employment screening of educational, employment, and other information in résumés
- Reference checking
- Employee integrity and honesty testing

Provide staff training, awareness programs, and general information to ensure the safety of all personnel regarding the following:

- How to avoid a crisis that could threaten their personal safety
- How to handle suspicious letters and packages
- The dissemination of travel advisory information to executives that provides up-to-date information on political risks and other local threats to security

Establish policies explaining the consequences of involvement in any activities detrimental to the interests of the company. For instance, the company should make clear that any employee involved in fraud will be terminated and subject to criminal prosecution.

Information

Access controls through the use of passwords by all personnel and the requirement that such passwords be changed regularly.

Use computer logs to monitor unauthorized attempts to obtain access to data or software.

Electronic countermeasures include the following:

- Sophisticated firewalls and virus alerts to prevent unauthorized access by hackers
- Regular sweeps for any tools installed to obtain unauthorized access to information or passwords

Reputation

Monitoring the information reported in the press should include the following:

- Monitoring information appearing in chat rooms about the company.
 - Take legal action against any parties committing slander or libel against the company and the company's reputation.
-

Security in an Emerging Nation Case Study

A global corporation needed to evaluate conditions for a potential manufacturing site in an emerging nation. If the project was to proceed, it needed to identify and deal with the day-to-day risks.

The region was rich in raw materials, and transportation to world markets was efficient and cost effective. In addition, labor costs were low and the local government provided strong incentives for the location of manufacturing businesses in its jurisdiction. In purely economic terms, the decision to build the plant was straightforward.

Management was concerned, however, about the day-to-day risks created by civil disorder arising from the country's economic difficulties. There was also growing anti-American sentiment because of the alignment of the local government with international issues and factions critical of United States policies. In addition, there had been incidents over the years in which company personnel had been exposed to violence and threats of kidnapping

A risk consulting firm was brought in to assess the situation and devise strategies to protect the company's people and facilities in the event that the project was to proceed. Based on the strength of these strategies, a decision was made to proceed with developing the site as a new manufacturing facility.

The risk consulting firm devised security strategies for the company's executives and management personnel traveling to and from the manufacturing site that took into consideration safety and security issues as well as political conditions.

These strategies included the provision of a local guard force for both the housing and office quarters for designated corporate employees. Site access was controlled and electronic monitoring for key areas was installed. Company officials were briefed on personal security issues and trained in the security measures taken at the site. A threat and crisis management plan was devised that specifically addressed the threat of a kidnapping or hostage-taking incident. The company's top executives were then trained on what to do in the event of such an incident.

Simulation exercises were conducted so that management would be very familiar with every aspect of the plan and could refine it over time.

For personnel traveling to the site from head office, comprehensive travel advisory information and personalized instructions and training were provided to make them aware of the dangers involved and to train them to avoid kidnapping or hostage taking.

To date, there have been no incidents that have threatened the safety of either the expatriate personnel or traveling executives.

The Emerging Nation case above illustrates several important points regarding the risk assessment process:

1. The risks of operating in an emerging nation can be mitigated by the implementation of appropriate security procedures.
2. The biggest concern in an emerging nation should be for the security of a company's personnel.
3. Adequate security for personnel involves more than just guards and locks.

11.4 CRISIS MANAGEMENT

11.4.1 Essentials of a Threat and Crisis Management Plan

In overview, an effective threat and crisis management plan should cover at least the following two topics:

1. Initial response to the emergency should include evacuation procedures, assembly points before and after the incident, and processes for communicating with employees and their families, clients, and the media.
2. Business resumption planning after an emergency is also needed.

Ideally, the plan should be written in a way that considers every type of threat that an organization can face as discussed earlier in this chapter, namely, theft and other intrusions, water damage, fire, accidents and mechanical breakdowns, utility interruption, earth movements, weather conditions, threats to the safety of a company's personnel, bomb threats and explosions, civil disorder, hazardous materials, and cyber and terrorist attacks.

The plan should be documented in a manual or other form readily accessible to all employees involved in implementing the plan.

The plan should address each of the four primary areas of the business that need protection, namely, the company's premises and equipment, people, information, and reputation.

It should specifically cover how and where to relocate or maintain the security of each of these aspects of a company's business in times of crisis so that critical operations can be restored as quickly as possible and additional losses prevented or minimized.

In order for a plan to remain effective, however, it must be reviewed on an annual basis, and tested and enhanced. This way, the plan will be known by more personnel than just its authors and can remain current as the company's circumstances evolve and new personnel come on board.

Included in the last section of this chapter is a "Threat and Crisis Management Plan" checklist that identifies many of the issues that need to be addressed in such a plan. This checklist is not a substitute for obtaining professional advice as part of the threat and crisis management planning process but is instead provided so CPAs can be aware of the types of issues to be considered.

The following case study provides an example of an effective threat and crisis management plan that was put to the test on September 11, 2001, and in the days shortly thereafter.

Fiduciary Trust's Recovery from Total Destruction Case Study

When the South Tower of the World Trade Center crashed to the ground on September 11, 2001, the five-floor office of Fiduciary Trust Company International and the lives of 87 of its 647 employees were destroyed with it. Thanks to a comprehensive threat and crisis management plan, however, the company was able to provide its main services the next day and was in full operation in less than a week.

The plan had been developed in 1987 to address management's concerns about business interruption from a power outage and expanded following the bombing of the WTC in 1993. Since then, it had been reviewed and practiced annually. In the event, when a disaster beyond the imagination of even the most forward-looking planner struck the company on September 11, this well-thought-out plan met almost all expectations. It covered everything from making sure that each employee had a flashlight with fresh batteries to how and where to relocate the computer systems to minimize any disruptions in the company's ability to manage \$44 billion of securities for pension plans, endowments, and wealthy individuals.

The plan included the following:

- Identification of at least two escape routes for each employee
- Assembly points for exiting the building and regrouping outside
- Arrangements for post-trauma counseling services
- Authorization of three key executives to declare a disaster independently
- Arrangements for temporary office space, telecommunications and computer systems at a site in New Jersey provided by Comdisco, a disaster recovery company
- Daily offsite backups of the company's transactions and balances
- Arrangements for delivery of the previous day's backup computer tapes
- Guidelines for booting up the systems
- Establishment of Internet access and an additional backup system

- Offsite storage for Fiduciary Trust's client list
- Guidelines for dealing with clients during the crisis
- Briefing manuals with the home and cellphone numbers of crucial staff

Two dozen key people knew how to recover all the electronic records of client accounts, trades and money transfers, and how to get servers and PCs up and running. These people were able to work effectively following September 11 because company policy required the plan be tested annually; the most recent annual test had been completed in late August 2001.

Bear in mind that Fiduciary Trust was in the South Tower. Within minutes of the North Tower being hit, the company's crisis management plan was being put in motion by employees offsite as well as onsite. Within an hour, president Bill Yun and chief technology officer Stephen Tall were at Comdisco's disaster recovery site in New Jersey. (Yun had been at a client meeting in New Jersey at the time of the attacks and Tall had been driving to work from his home in New Jersey.) As soon as the two executives reached their new temporary headquarters, they began work to reestablish their computer systems and contact their key clients. During these calls, management received overwhelming support as the first thought of each client was for the safety of Fiduciary Trust's employees.

Comdisco, one of the three biggest companies in the disaster recovery industry, has thirteen large facilities across the United States providing logistical support in the form of temporary office space, telecommunications, and computer systems to companies forced out of their premises by disasters ranging from earthquakes, fire, and flood to, in this case, an unprecedented terrorist attack. Comdisco's new facility in Carlstadt, New Jersey, for instance, is a 302,000-square-foot site capable of supporting 1,000 workers and up to sixteen different computer systems. Within days of September 11, this site was filled to overflowing. Numerous companies from the World Trade Center as well as others from the surrounding downtown area called on Comdisco and other similar firms to help them reestablish operations. By September 13, Fiduciary Trust had issued an announcement to the media "that operations are up and running at our disaster recovery center in New Jersey supported by Franklin Templeton Investments' offices in Short Hills, NJ."

Although Fiduciary Trust's threat and crisis management plan was comprehensive and well thought out, the unprecedented events of September 11 caused more destruction than anyone could have imagined. Many people had died and enormous buildings had been completely destroyed. The following were some of the operational issues that had not been considered as part of Fiduciary Trust's crisis management planning process. Instead, as the enormity of the disaster unfolded, they were addressed by Fiduciary Trust's management, as follows:

1. Comdisco and other disaster recovery firms found that even their hundreds of thousands of square feet of available office space proved insufficient for a crisis requiring the relocation of the entire operations of so many clients simultaneously. Fiduciary Trust had to act quickly to secure additional premises not just for the long term but for the short term as well.

2. Most comprehensive threat and crisis management plans address the need for temporary office space for its critical personnel but do not consider the need for permanent office space to house a company's entire operations. Fiduciary Trust's plan was no exception. Its executives immediately realized, however, the need to secure suitable permanent office space. Finding new offices quickly would be critical to the whole recovery process not only for company operations but also for the emotional well-being of its personnel. By September 15, only four days after the disaster, management of Fiduciary Trust had secured new premises for its New York operations; within weeks, its personnel started moving into their new location.
3. Established counseling services were insufficient to meet Fiduciary Trust's needs since the threat and crisis management plan had not contemplated the loss of so many lives. Nor had the plan contemplated the gravity of the situation and the extent to which people felt threatened not only by the terrorist acts themselves but also by the new risks associated with war. Fiduciary Trust's parent helped to fill this need by seconding personnel from its own human resources staff.
4. Communications were disrupted to a greater extent than had been anticipated in the plan. Additional support was required from the parent.
5. Fiduciary Trust's Web site had not been backed up to an offsite location. Its parent had a new Web site up and running the following day.
6. Fiduciary Trust's management had not anticipated the degree of media interest in the company and its employees, especially the hounding of employees for personal stories. The company countered this media pressure by installing a security system on its Web site that prevented any outsider from obtaining information about its employees.

The events of September 11 showed that even the unimaginable can sometimes happen and that it is important for companies to have a well-practiced threat and crisis management plan in place long before disaster strikes. In hindsight, this tragedy proved the effectiveness of the plan that Fiduciary Trust had developed over the preceding fourteen years. Despite the tragic loss of life and the complete destruction of its offices, the company was operational the day following the disaster even though the plan had not covered every contingency as, indeed, no plan could have. Total chaos was, however, averted and both Fiduciary Trust and its employees were soon well on their way to a speedy recovery.

The Fiduciary Trust case illustrates several important points regarding threat and crisis management plans:

1. A comprehensive threat and crisis management plan is critical to the quick restoration of a company's business after a crisis strikes. It is an excellent tool to assist in restoring order to chaos. This is not only because many key operational decisions have already been made but also because it enables employees to understand their role in the restoration process.
2. A plan that sits on a shelf is of little value to an organization. It is only of value if it has been tested and a company's employees know how to implement it.

3. An effective threat and crisis management plan addresses how and where to relocate and restore a company's premises and equipment in times of crisis; how a company's personnel will escape from a crisis and where they are to report; how information will be protected before a crisis and then restored afterwards; and how to communicate with its personnel, clients, and the public at large.
4. When a crisis affects many companies simultaneously, companies that provide disaster support services such as counseling and temporary relocation services may not be able to fulfill all the needs of their clients. An effective crisis management plan should identify a contingency plan to provide backup support as needed.
5. Even the most comprehensive plans cannot cover every contingency.

Other aspects of a comprehensive threat and crisis management plan that are not addressed in the Fiduciary Trust case study described above, but which should be part of an effective plan, are described below:

Premises

The threat and crisis management plan should cover incidents at all facilities—including the head office location, storage facilities, data processing facilities, call centers, manufacturing plants, and sales centers.

People

The threat and crisis management plan should identify who will be in command during the crisis and who will continue to be involved in running the day-to-day operations of the business. The plan should identify clear lines of authority for those in central command; the roles and responsibilities of each person should be defined and understood. Typically, the crisis team would include at least one representative from each of the critical functional areas of the business as well as someone from human resources, legal, security, occupational health, public affairs, the CFO's office, and a union representative.

The threat and crisis management plan should identify a designated threat assessment team to assess and respond to the following:

- *Bomb threats.* The plan should identify the tasks and responsibilities associated with determining whether the threat is real or not and who should be contacted to defuse and remove the bomb.
- *Hazardous materials contamination.* The plan should identify the tasks and responsibilities necessary to contain the hazardous materials and prevent further contamination.
- *Medical emergencies.* The plan should identify the paramedics and medical specialists to treat or decontaminate victims and provide antibiotics/antidotes to hazardous materials contaminants.
- *Fire emergencies.* The plan should identify the firemen and medical specialists to contain the fire and treat victims for burns and smoke inhalation.

The threat and crisis management plan should identify who should be called in to help from outside the company, including crisis management consultants, insurance companies, insurance brokers, call center services companies, and other service and professional resources such as engineers and restoration specialists.

The threat and crisis management plan should identify who should be responsible for communicating with employees and their families, clients, suppliers, insurers, and the media and should also identify the types of communications to be provided.

Information

Whether implemented as part of the threat and crisis management planning process or as a standard business practice of the information technology (IT) department, it is advisable to have more than one backup location for a company's transactional data, client, and staff lists, and the software used to process such information. Companies using courier services between offices can include backup disks along with the mail going to outlying offices.

The threat and crisis management plan should include the creation of a manual for recovering the company's computer systems. Such a manual should identify all key software and hardware required by the business and should identify how to recover or restore each system. This manual should be the basis for regular testing and should be upgraded as required to keep current with any new technology.

Reputation

A company's reputation must be considered as part of any comprehensive threat and crisis management plan. This involves developing appropriate strategies for communicating with all the people who could be affected by a crisis. It would also involve developing strategies for communication with those who could have an interest in the handling of the crisis, including the company's employees, customers, suppliers, shareholders, the general public, the media, and regulatory authorities.

The actions of a company in a crisis—how it handles the actual crisis and how quickly it responds—are critical to maintaining its reputation. The nature and timing of the communications issued by the company are also important but these are secondary to its actions. Such communications could take the form of damage control or could be positive messages regarding how the company is averting or minimizing the impact of the crisis.

11.4.2 Denial of Insurance Coverage for Terrorist Acts

September 11, 2001 convinced many managements that disaster could be just around the corner for their business and that it was important to have an effective and up-to-date threat and crisis management plan to minimize the disruption and losses that would otherwise be suffered from such a disaster.

The actions of insurance companies after September 11 further convinced management of this need as many insurance companies rewrote their policies to exclude coverage for terrorist acts.

This prompted many executives to realize how vulnerable they were and prompted them to establish or upgrade their threat and crisis management plans to minimize the disruptions and losses to their ongoing operations.

Campbell Electronics Case Study

Subsequent to September 11, 2001, Campbell Electronics, an electronics manufacturing company with head offices in California and manufacturing facilities in several foreign jurisdictions including the Pacific Rim, retained a risk consulting firm to assess its risks and vulnerabilities. This assessment included examining the company's existing response and business continuation plans to determine their efficacy.

This risk assessment revealed that Campbell Electronics had well-developed security procedures related to computer security, fire, and theft but was ill-prepared for catastrophic events such as those of September 11. For example, there were no plans for dealing with bomb threats or chemical contaminants. The company also had no contingency or business continuation plans for incidents that might deny them access to their facilities because of the destruction of their headquarters.

This weakness represented a significant risk to the company since it was critical for head office staff to be able to coordinate the activities of each of its manufacturing facilities. This was accomplished through sophisticated communications systems using their computer and telecommunication systems. These systems were networked and integrated and allowed for the secure exchange of financial and strategic information on a real-time basis. Their operations relied heavily on this communications network to control inventory levels and manufacturing schedules as well as accounting and human resource functions.

Based on the results of the risk assessment, Campbell Electronics modified its crisis management plans to address this critical risk by incorporating contingency plans to provide for business continuation in the event of a denial of access to its corporate head office facilities near San Francisco. The contingency plan identified the departments and personnel that were critical to the operations of the business in the US and internationally and also identified all the computer, telephone and office equipment necessary for these departments and personnel to function effectively at the backup site. This evaluation was based on input from several employees within the company.

The company then made arrangements with a reputable disaster recovery facility to provide sufficient temporary office space, computer equipment, telephones, and office equipment to enable the critical operations team to function effectively. The contingency plan also identified how to mobilize such resources. For personnel who were not part of the critical operations team, the plan provided guidelines for supporting the continued operations.

Training programs were integrated into a comprehensive program to prepare the company's management team and staff to respond to any crisis. Such training included the introduction of crisis simulation exercises to ensure that the contingency plans were understood by the key decision makers involved in implementing the plan and to provide a forum for the plan to be discussed and improved upon.

The Campbell Electronics case illustrates several important points regarding threat and crisis management plans:

1. Threat and crisis management plans need to include more than just an evacuation plan and whom to call in the event of fire. They need to consider what to do when an entire facility is destroyed or otherwise becomes unavailable for use.
2. As part of the threat and crisis management planning process, it is important to consider what aspects of a business are critical and to tailor the threat and crisis management plan to enable the critical components of the business to be restored immediately after the crisis.
3. Employees who are not part of the critical operations team still have an important role to fill in the event of an emergency. They need to be available for deployment in whatever roles are considered important by the crisis management team.
4. Crisis simulation exercises are an important part of the preparation of management to handle a threat or crisis and are also an important part of the process of improving and refining the threat and crisis management plan.

Sanvista's Kidnapping Crisis Case Study

Sanvista Consumables, a multinational consumer products company operating in the Middle East, engaged a risk consulting company to expand its crisis management plan. It wanted the plan especially to cover the threat to senior management personnel of kidnapping or hostage taking. Sanvista's head offices were in the United States, and it was widely known to be a United States-led operation. The company had operated in the Middle East for years without any major incident; the Gulf War in 1991 created uneasiness, however, and raised the level of apprehension among the company's executives as to Sanvista's ability to deal with a kidnapping or hostage-taking crisis.

The risk consulting company provided training for Sanvista's senior executives at home and abroad in crisis management and incident control. Response procedures were established to make critical decisions and retain organizational control. Such procedures were documented in the crisis management plan and were the subject of simulation exercises to prepare management for a kidnapping or hostage-taking incident.

Several months later, one of Sanvista's top executives in Dubai left his home for an early morning walk to a convenience store around the corner. He didn't return.

Two days after he disappeared, a phone call was received at the company's head office in the United States demanding a ransom for the return of the executive. A call was placed to a risk consulting firm for assistance.

Within twenty-four hours, a risk consultant was on location providing expertise and support to the Sanvista's crisis management team. The team followed the crisis management plan, which enabled them to address the situation effectively:

1. They established an emergency operations center that operated twenty-four hours a day.
2. From this location, they worked with local government officials and enforcement officials to negotiate the executive's release.
3. They also assigned a liaison to provide information and support for the kidnapped executive's family and to deal with the media effectively.

Three days later the executive was returned tired and shaken but otherwise unharmed.

The Sanvista case illustrates several important points regarding kidnapping and hostage-taking incidents:

1. It is important for all senior personnel to try to avoid becoming the victims of a kidnapping or hostage taking. If prevention fails, it is important for the safety of the kidnap victim as well as for the reputation of the company to have a crisis management plan to effect the safe return of the victim.
2. Training in crisis management and incident control are critical for maintaining calm in the face of danger.
3. A command center with round-the-clock communications capabilities is essential for comprehensive management of the crisis.
4. Competent professionals with significant experience with kidnapping and hostage-taking incidents should be brought in to assist with strategy and communications at the command center.

11.5 CORPORATE SECURITY CHECKLISTS

CPAs can use the checklists in this section to assist them in understanding the security needs of their organization or their clients. *No* answers require follow-up, the results of which should be documented. Use the "Ref" column to cross-reference the checklist to the appropriate supporting working papers. Some sections in these checklists may not be applicable and should be identified as such in the "N/A" column. The "Ref" column can be used to cross-reference any notes made regarding why such sections are not applicable.

The checklists in this section are intended for general guidance and information only. Use of these checklists does not guarantee the prevention or detection of security breaches. Those with vital concerns about security or who have a security-related crisis should seek the advice of a competent risk advisory services practitioner.

11.5.1 Comprehensive Risk Assessment

Comprehensive risk assessments are best performed by a competent risk advisory services professional with many years' experience in not only identifying but in dealing with the types of risks described earlier in this chapter. Table 11.2, Comprehensive Risk Assessment

Checklist, is provided to assist CPAs in understanding the types of issues that need to be considered as part of this process. This checklist collates several of the concepts presented in this chapter but does purport to present all issues that need to be considered as part of a comprehensive risk assessment process. Further, this checklist is not intended as a substitute for engaging a competent risk advisory services professional.

TABLE 11.2 COMPREHENSIVE RISK ASSESSMENT CHECKLIST

| Comprehensive Risk Assessment Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| <i>A no answer to any of the following questions warrants further follow-up:</i> | | | | |
| 1. Security Department | | | | |
| a. Does your company have a security department? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Does the security department report to head office? And are the costs related to security part of the head office budget? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Does the head of security have at least ten years' experience? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Does the security department have security personnel at each location? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. Nature and Location of Operations | | | | |
| a. Do appropriate security procedures exist to protect the personal safety of employees who handle hazardous materials? To prevent a contamination? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. If your organization has facilities that are visited by the public, or has transportation equipment that the public uses, do appropriate security procedures exist to protect the public from danger, and to evacuate the public in the event of danger? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. If any of your facilities are located in the third world, have any additional security procedures been implemented there beyond those that are implemented elsewhere? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Emergency Preparedness | | | | |
| a. Has a threat and crisis management plan been developed for your organization? If so, has it been reviewed and tested in the last year? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Does the threat and crisis management plan cover evacuation procedures? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Does the threat and crisis management plan cover business resumption planning? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 4. Premises and Equipment (Consider the following questions for each location.) | | | | |
| a. Does this location have locks and alarms to prevent unauthorized entry? Are they monitored? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 11.2 (continued)

| Comprehensive Risk Assessment Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| b. Is card access technology used? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. If card access technology is used, are these cards also used for photo identification purposes? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Is closed circuit television (CCTV) used at all access points to the facility? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Does reception have an alarm button that is continuously monitored whenever reception is open? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. Do controls exist to prevent unauthorized access from the loading dock? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| g. Do controls exist to prevent unauthorized access via the freight elevator and stairwells? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| h. Have improvements been made to the security system related to any past security breaches? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| i. Have you looked into where to obtain temporary equipment to keep your business going? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| j. Do you know how you would quickly replace your inventories, if lost? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| k. Do you know where you would maintain your inventory if your storage facility was damaged? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| l. Do you know where you would manufacture your product or operate your business if your primary location was irreparably damaged or destroyed? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 5. People (Consider the following questions for personnel at each location.) | | | | |
| a. Have evacuation procedures been documented and distributed to all personnel? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Have crisis management procedures been developed and distributed to all key personnel? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Are all new employees screened through a background checking process? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Is travel advisory information provided to traveling executives that advises on political and other risks in the countries they are traveling to? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Have all key personnel been trained in how to avoid becoming a victim of a kidnapping? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. Have procedures been documented and distributed related to how to handle bomb threats or biohazards? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

TABLE 11.2 (continued)

| Comprehensive Risk Assessment Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| 6. Critical Operations and Personnel | | | | |
| a. Do you know which employees perform functions that are critical to the survival of your business? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. If certain employees were unable to work, have you identified replacements, either within the organization or through the use of temporary employment agencies? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Do at least two other employees know how to perform the critical functions performed by these people? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Do you maintain up-to-date procedure manuals regarding the performance of the business's critical functions? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 7. Information (Consider the following questions for information stored electronically and in hard-copy format at each location.) | | | | |
| a. Do access controls exist to protect each computer at this location and the information stored in them? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Are laptops secured at night? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Are daily backups taken of all data on servers and mainframes? And are these backups stored offsite? Is more than one backup taken? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Do you regularly back-up all computer programs? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Are current copies of customer lists, employee lists and procedures manuals maintained offsite? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 8. Insurance Coverage | | | | |
| a. Do you periodically review your insurance coverage, know exactly what your insurance policy covers and keep a copy of the policy offsite? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Have your insurance policies been reviewed within the last year? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 9. Reputation | | | | |
| a. Are press releases controlled? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Are newspapers monitored for information about your company? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Are chat rooms monitored, and are there procedures in place to handle any reputational slurs? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Do policies exist related to the consequences of committing an act that is adverse to the interests of the company such as committing a fraud, or destroying property? Are all personnel required to sign a statement acknowledging they have read and agree to the policies? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

11.5.2 Threat and Crisis Management Planning

The threat and crisis management planning process is best performed by a competent risk and crisis management professional, with many years' experience in not only planning for, but also addressing the types of threats and crises described in this chapter. Table 11.3, Threat and Crisis Management Checklist, is provided to assist CPAs in understanding the types of issues that need to be considered as part of this process. This checklist is not intended as a substitute for engaging a competent risk crisis management professional.

TABLE 11.3 THREAT AND CRISIS MANAGEMENT CHECKLIST

| Threat and Crisis Management Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| <i>A no answer to any of the following questions warrants further follow-up:</i> | | | | |
| 1. Existence of a Crisis Management Plan | | | | |
| a. Is there a Crisis Management Plan? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Has it been reviewed within the last year? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Has it been tested within the last year? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Have all the recommendations for improvement been implemented since the plan was last tested? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Is a copy of the Crisis Management Plan maintained in both hard copy and electronically? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. Is the Crisis Management Plan accessible to at least ten key personnel per location, in both electronic and hard-copy form? And have two copies of the plan been provided to each person—one for the office, and a backup copy for their homes? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| g. Does the plan accommodate local, regional, and international incidents? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| h. Does the plan accommodate incidents at all types of facilities of the company (for instance, storage facilities, production plants, head office, sales offices)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. Roles and Responsibilities | | | | |
| a. Does the Crisis Management Plan identify who will perform the following roles in the event of a crisis along with alternates for each position (if yes, identify names)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Crisis Management Chairman | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Incident and Intelligence Coordinators | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Loss Prevention and Risk Manager | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Security Coordinator | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● General Counsel | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Finance Coordinator | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

TABLE 11.3 (continued)

| Threat and Crisis Management Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| ● Computer Recovery | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Human Resources | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Public Relations and Media Coordinator | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Crisis Management Coordinator | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Recorder | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Floor Warden—Male | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Floor Warden—Female | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Does the Crisis Management Plan provide a description of the responsibilities for each of the following personnel? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Crisis Management Chairman (person with authority to make decisions on evacuation and related to the allocation of funds, etc.) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Incident and Intelligence Coordinators | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Loss Prevention and Risk Manager | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Security Coordinator | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● General Counsel | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Finance Coordinator | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Computer Recovery | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Human Resources | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Public Relations and Media Coordinator | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Crisis Management Coordinator (coordinates all activities of support personnel during the recovery efforts) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Recorder (records critical information during the recovery efforts—for instance, who is accounted for and who is missing) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Floor Warden—Male | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Floor Warden—Female | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Does the Crisis Management Plan make it clear who will speak to employees, the media, victims and families after a crisis? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Personnel Evacuation, Identification, and Recall | | | | |
| a. Does the Crisis Management Plan designate evacuation points that have protection from weather? Are there restroom facilities? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 11.3 (continued)

| Threat and Crisis Management Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| b. Do the evacuation points have access to appropriate communication methods? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Does the Crisis Management Plan include accountability lists per department, or identify where the current version of such lists are located? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Does the Crisis Management Plan identify where employees are to “call in” to report their whereabouts in the event of a catastrophe? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Does the Crisis Management Plan include emergency contact numbers for the next of kin of employees in each department, or identify where the current version of such information is located? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Does the Crisis Management Plan identify a recall method regarding when it is safe to return to work? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 4. Operational Facilities and Personnel | | | | |
| a. Does the Crisis Management Plan identify which operations are critical for the ongoing operations of the business? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. Does the Crisis Management Plan identify which employees perform functions that are critical for the ongoing operations of the business? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Does the Crisis Management Plan identify at least two replacement personnel for each critical employee—either within the organization or through the use of temporary employment agencies—in the event that certain of the critical employees are unable to work? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Does the Crisis Management Plan identify the location of the <i>primary</i> Replacement Operational Facility? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Does the Crisis Management Plan identify the location of the <i>alternate</i> Replacement Operational Facility? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Does the Crisis Management Plan identify how to restore operations? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. Are the primary and alternate Replacement Operational Facilities located off-site? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| h. Are the primary and alternate Replacement Operational Facilities located within two miles of the existing operational facility? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| i. Is the space sufficient in the primary and alternate Replacement Operational Facilities? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

TABLE 11.3 (continued)

| Threat and Crisis Management Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-------|
| 5. Crisis Command Center | | | | |
| a. Does the Crisis Management Plan identify the location of the <i>primary</i> Crisis Command Center? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| b. Does the Crisis Management Plan identify the location of the <i>alternate</i> Crisis Command Center? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| c. Are the primary and alternate Crisis Command Centers located offsite? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| d. Are the primary and alternate Crisis Command Centers located within two miles of the existing facility? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| e. Is the space sufficient in the primary and alternate Crisis Command Centers? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| f. Do the primary and alternate Crisis Command Centers have the following: | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Copies of the Crisis Management Plan Manual | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Telephones, including unlisted outside lines (multiple lines, multiple phones) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Answering Machine(s) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Pagers | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Cellular Phones | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Computer with Printer | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● White Paper | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Typewriter | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Copier | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Fax Machine | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Recorder | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Shredder | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Overhead Projector | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Bulletin Boards | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Easels | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Television Sets (at least three) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● VCRs (at least three) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Video Camera | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| ● Digital Camera | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

(continued)

TABLE 11.3 (continued)

| Threat and Crisis Management Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|-----|
| ● Tape Recorder | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Basic Office Equipment and Supplies (pens, pencils, erasers, staplers, markers, tape, masking tape, duct tape) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Flashlights | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Safe or other secure storage facility, which can be secured when the center is unoccupied for storing sensitive files and materials | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 6. Crisis Support Numbers | | | | |
| Does the Crisis Management Plan include phone numbers for the following services? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Local Hospitals | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Local Ambulance Services | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Burn Center | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Centers for Disease Control | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Counseling Services | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Local Bomb Squad | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Local Police Department | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● FBI Office | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Fire Department | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Red Cross | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● FEMA (Federal Emergency Management Agency) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● US Embassy or Consulate | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Passport and Visa Office | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 7. Data Recovery and Replacement Computer Equipment | | | | |
| a. Does the Crisis Management Plan identify where a replacement computer system is located? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Does the Crisis Management Plan identify where back-up data is located? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Does the Crisis Management Plan identify how to restore the computer system with the back-up data? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Does the Crisis Management Plan identify how to restore the company's Web site in the event that it is no longer available? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 8. Equipment Requirements | | | | |
| a. Does the Crisis Management Plan identify the equipment that is essential for the operation of the business? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

TABLE 11.3 (continued)

| Threat and Crisis Management Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| b. Does the Crisis Management Plan provide authority for the procurement of essential equipment? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 9. Incident-Specific Crisis Management Plans | | | | |
| Are there individual appendices to deal with each of the following types of incidents? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Systems Intrusion | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Building Evacuation | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Cyber-terrorism | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Computer and Telecommunications Failures | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Fire and Explosion | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Bomb Threats and Searches | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Hazardous Materials | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Civil Disorder | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Workplace Violence | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Armed Attack | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Kidnap and Extortion | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Employee Disappearance | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Hostage Taking | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Water and Power Outages | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Flood | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Earthquake | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Tornado | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| ● Hurricane | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

11.5.3 Financial Issues to Deal With When Disaster Strikes

There are a number of financial issues that arise when disaster strikes. The quicker these issues are dealt with, the quicker a business will be able to return to normal operations and prevent further losses from occurring. Table 11.4, Financial Issues to Address When Disaster Strikes, is provided for general guidance to CPAs to address the financial aspects of the disaster-recovery effort. This table is not intended as a substitute for engaging a competent crisis management professional to assist in the event of an actual disaster.

TABLE 11.4 FINANCIAL ISSUES TO ADDRESS WHEN DISASTER STRIKES

| Financial Issues to Address When Disaster Strikes | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| <i>A no answer to any of the following questions warrants further follow-up:</i> | | | | |
| 1. Cash Flow and Financing | | | | |
| a. Are alternate means of payroll processing and delivery available? Are all health and disability insurance issues addressed? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Are you still able to obtain payments from your customers? (If not, make arrangements for alternate postal delivery services/banking arrangements with customers.) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Is your cash position adequate? Can you access the cash? Can you meet your immediate cash needs? Can you keep up with your anticipated cash-burn rate? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Have you informed your creditors, bankers, suppliers, joint venture partners, and strategic partners of the recent events? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Are you aware of all available financial assistance such as credit lines, disaster loans and grants? (Make arrangements as required.) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. Insurance | | | | |
| a. Have you informed your insurer and insurance broker regarding the recent events? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Do you have a copy of your insurance policies covering, for example, key individuals, other life, property, business interruption, and disability? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Do you know the deadlines for submissions of an insurance claim? Have you gathered and submitted the required information? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Business Operations | | | | |
| a. Are you able to operate right now? Determine, for example, immediate or impending deadlines, due dates, customer and supplier needs. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Are you aware of your company's current operational risks, such as work-in-progress, cancellations, no-shows, refunds, lost revenues, and undeliverable materials? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Are you able to meet all the needs of your customers? If not, consider contacting competitors to outsource production to them until you are able to meet your customers' needs. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 4. Information Backup | | | | |
| a. Do you know when the last backup of your computer information took place? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

TABLE 11.4 (continued)

| Financial Issues to Address When Disaster Strikes | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| b. Do you know where your backup data is stored? Has it been retrieved yet? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| c. Do you have a copy of the last available financial statements? (If not, check with auditors and attorneys.) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| d. Have you inquired of your attorneys and auditors to determine whether they have any other information that could be useful for ongoing operational purposes (copies of contracts and agreements)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| 5. Business Plan Assessment | | | | |
| a. Is your most recent business plan still valid? Have you considered what can/cannot be executed? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| b. Has your business plan been updated to reflect the current situation? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| c. Have you provided a copy of your updated business plan to your financiers, creditors or bankers (if required)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

11.6 THE KROLL OCTOBER 2001 SURVEY ON SECURITY RISK MANAGEMENT

Kroll

The Risk Consulting Company

October 2001

Survey on Security Risk Management Post September 11, 2001

September 11, 2001 has prompted businesses to abruptly re-assess their ability to deal with security threats, according to a recent survey of executives, conducted by Kroll, a leading risk consulting company.

In New York, Boston and Toronto, businesspeople expressed a heightened sense of vulnerability to possible emergencies, both man-made and natural. Before September 11, information protection and employee integrity were the top security priorities. Since then, concern with emergency planning, business resumption planning and physical security has increased dramatically.

Although most have formal plans for fire and systems disasters, many organizations would be forced to improvise if confronted by a bomb threat, hazardous material scare or utility outage. Despite widespread doubt about the adequacy of controls to manage security risks, almost everyone has indicated that their organizations will upgrade security over the next six months. This apparent commitment to improve security should be welcome news to employees, customers and shareholders alike.

Objectives

This survey was designed to:

- Assess whether the security priorities of business have changed since September 11, 2001 – and if so, how;
- Measure the extent to which business is ready with emergency plans and security measures; and
- Gauge the adequacy of security risk management by business.

Methodology

Kroll invited executives and professionals from a broad range of sectors – including financial services, consumer goods and services, utilities, energy, and real estate – to complete a confidential “Security Preparedness” questionnaire at *Threat and Crisis Management* seminars held in October 2001 in New York, Boston and Toronto. Approximately 100 of the participants gave details on their organizations’ readiness to deter, detect and respond to security threats. There appears to be a strong consensus on most security issues.

Key Findings

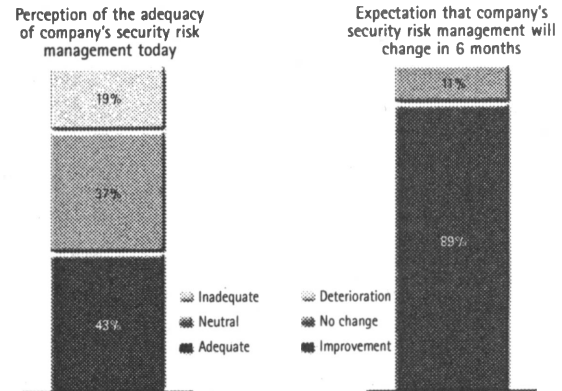
The key findings are summarized below under five headings:

1. Adequacy of security risk management today – and in six months
2. Security priorities
3. Importance of preparedness
4. Incidence of formal emergency plans
5. Incidence of specific security measures

1 Adequacy of Security Risk Management Today – And In Six Months

While many businesspeople question the adequacy of their organizations' management of security risks – most believe this security will improve over the next six months.

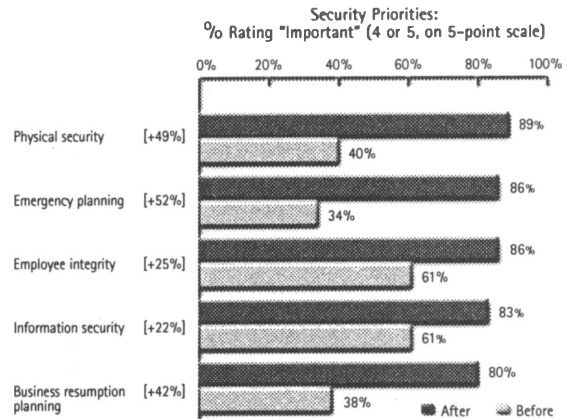
- When asked about their organizations' "ability to manage security risks," only 43% gave positive ratings (4 or 5, on a 5-point scale). Another 37% were uncertain or neutral on the question, while 19% indicated outright criticism.
- Most (89%) expect security risks to be better managed in six months time, suggesting that many businesses are committed to upgrading their risk management systems by addressing perceived shortcomings.



2 Security Priorities

Priorities have shifted. Before 9/11, information security and employee integrity led the list of concerns. Since then, preoccupation with all aspects of security has intensified dramatically, particularly with emergency planning, business resumption planning and physical security.

- Most businesspeople (86%) now view emergency planning as "important" (4 or 5 on a 5-point scale), whereas only 34% said this was a priority before September 11.
- Similarly, 80% say business resumption planning is "important," while only 38% held this opinion before 9/11.
- Likewise, 89% think physical security is an "important" priority, up from 40%.

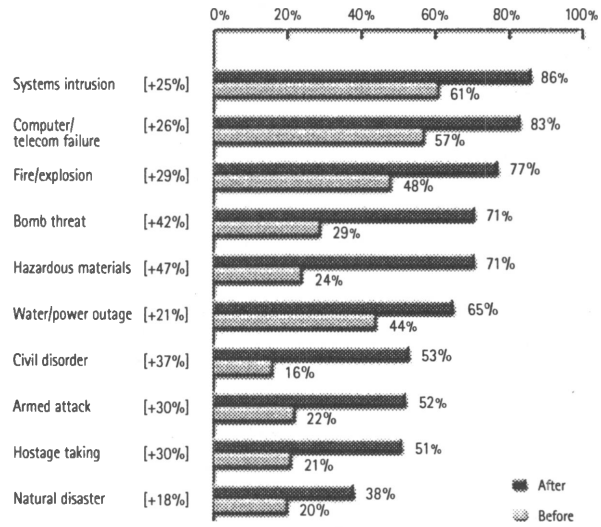


3 Importance of Preparedness

The survey confirms a heightened sense of vulnerability to a wide range of emergencies, both man-made and natural.

- The importance of “preparedness” has risen since September 11 for all ten types of emergencies covered by the survey. In addition to increased concern with terrorist bomb threats, hostage-taking and armed attacks, businesses are also more worried about coping with fire, utility outages, computer intrusions – and even civil disorder and natural disasters.
- Not surprisingly, preparedness to deal with bomb threats and hazardous materials saw the greatest jump in importance (i.e., up 43 and 47 percentage points, respectively) since September 11. Only 24% of respondents said readiness to deal with hazardous material was important before the US terrorist attacks, compared with 71% afterward.
- System intrusion was rated the most important issue both before and after September 11.

Emergency Preparedness:
% Rating "Important" (4 or 5, on 5-point scale)



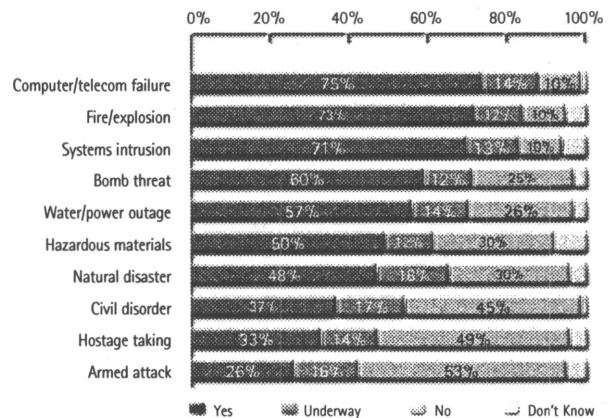
[+xx%] indicates percentage point difference between ratings before and after Sept. 11, 2001.

4 Incidence of Formal Emergency Plans

Most organizations have formal plans for fire and computer disasters, but many would be forced to improvise if struck by other types of catastrophe:

- A majority of (though not all) organizations have documented emergency procedures for fire (73%), telecom/computer outages (75%) and systems intrusions (71%).
- Readiness to address other emergencies is less common, such as the ability to cope with bomb threats (60%), utility outages (57%) or hazardous materials (50%).
- Only 48% currently have formal plans to deal with any form of natural disaster, although another 18% say such plans are now being developed.

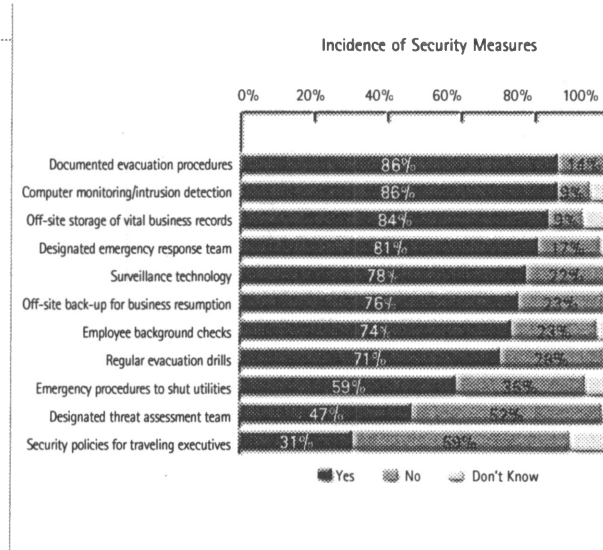
Incidence of Formal Emergency Plans



5 Incidence of Specific Security Measures

Certain standard security measures are quite prevalent; for example, most organizations have evacuation procedures and many hold regular drills. Computer monitoring and off-site storage of vital business records are also widespread, as is electronic surveillance. On the other hand, there are some notable shortcomings:

- Just 59% of organizations have procedures to shut down utilities in an emergency.
- Only half (47%) have designated threat assessment teams.
- Security policies for traveling company executives are comparatively rare (31%), despite being relatively straightforward to implement.



Kroll Inc. is a global leader in providing risk consulting services to corporations, financial institutions and governments. Drawing on a broad range of professional disciplines and experience – including security, law enforcement, forensic accounting, information technology and competitive intelligence – Kroll’s services include:

- Physical security assessment
- Emergency procedure consulting
- Security staff training
- Surveillance technology consulting
- Business intelligence and investigations
- Employee integrity checks
- Country risk assessments
- Traveler security advisories
- Kidnap response
- Executive protection
- Systems intrusion detection
- Computer network assessment

For more information regarding Kroll’s services, please visit www.krollworldwide.com or contact one of Kroll’s offices.

Kroll
The Risk Consulting Company

CHAPTER 12:

Bankruptcy Fraud

| | |
|---|----|
| 12.1 Overview | 3 |
| 12.2 The Bankruptcy Process..... | 3 |
| 12.2.1 Insolvency..... | 3 |
| 12.2.2 Filing for Bankruptcy..... | 3 |
| 12.2.3 The Bankruptcy Petition | 4 |
| 12.3 Fraud in Bankruptcy Filings | 4 |
| 12.3.1 Materiality | 5 |
| 12.3.2 Knowledge and Fraudulent Intent..... | 5 |
| 12.3.3 Criminal Prosecution..... | 6 |
| 12.4 Elements of Bankruptcy Fraud | 8 |
| 12.4.1 Nondisclosure or Concealment of Assets..... | 8 |
| 12.4.2 False Information in Filing..... | 10 |
| 12.4.3 False Claims Filed in a Bankruptcy..... | 11 |
| 12.4.4 Transfer of Assets Before a Bankruptcy Filing..... | 12 |
| 12.4.5 Transfer of Assets After a Bankruptcy Filing | 14 |
| 12.4.6 Bribery or Threats..... | 15 |
| 12.4.7 Concealment, Destruction, or Withholding of Documents..... | 16 |
| 12.5 Kinds of Bankruptcy Fraud | 17 |
| 12.5.1 Bust Out and Bleed Out..... | 17 |
| 12.5.2 Embezzlement by a Trustee or Officer..... | 18 |
| 12.5.3 Serial Filings | 18 |
| 12.5.4 Service Petition Mills..... | 19 |
| 12.5.5 Ponzi Schemes..... | 19 |
| 12.6 Punishment Provisions..... | 20 |
| 12.7 Referral of Bankruptcy Fraud..... | 21 |
| 12.8 Bankruptcy Fraud Checklist..... | 22 |

CHAPTER 12:

Bankruptcy Fraud

12.1 OVERVIEW

Some people believe that any attempt to discharge legitimate debts through the bankruptcy process is, at best, a questionable moral act and, at worst, a crime. The right to remove one's debts through a bankruptcy filing has, however, been long established in American law. Unfortunately, among the huge number of bankruptcies filed annually, some are based on *fudged* accounting that may create an outright criminal fraud. Criminal bankruptcy fraud is often complex and not readily understood by the public or even by CPAs who are skilled in financial accounting. CPAs who act as auditors of a company that later goes bankrupt often find themselves embroiled in an audit or negligence action concerning whether they should have known about the fraudulent transactions that led to the collapse.

To the CPA untutored in the arcane lore of bankruptcy, the entire process may seem intended primarily to move the bankruptcy through the system quickly and not necessarily to uncover and prosecute fraudulent filings. Nevertheless, those associated with the administration of the bankruptcy system are keenly aware of the possibilities of fraud and are willing to act promptly on learning of its existence.

12.2 THE BANKRUPTCY PROCESS

To understand bankruptcy fraud, it is necessary to understand the basic elements of the bankruptcy process. That process is supported by various concepts, most of which seem relatively simple on the surface, but become increasingly complex for a number of reasons.

12.2.1 Insolvency

Although insolvency is not an absolute requirement, bankruptcy starts with the presumption that liabilities exceed assets or that existing cash flow is insufficient to service debts. This simple concept can be agonizingly complex in larger bankruptcies because of the wide variety of valuation methods. Nevertheless, by and large, most insolvency is determined by this test. Insolvency does not need to be reached before filing a bankruptcy petition.

12.2.2 Filing for Bankruptcy

The actual bankruptcy commences with the filing of a bankruptcy petition. Concurrent with the filing of the petition or shortly thereafter, the debtor, that is, any person or entity that is the subject of the bankruptcy, is required to file a Schedule of Assets and Liabilities and a Statement of Financial Affairs. These documents, which are often referred to as

bankruptcy schedules, are a somewhat tailored set of financial statements containing a list of the debtor's assets and liabilities plus specific written intentions regarding the disposition of assets and the payment of liabilities.

For instance, if a debtor owns a TV or automobile in which a creditor holds a security interest, the debtor must state his or her intention to surrender that asset or make arrangements to pay for the asset in accordance with the terms of the contract.

Examples of bankruptcy schedules are included as Exhibit A, Bankruptcy Schedules, on the *Fraud Prevention Checklists CD-ROM*. These particular forms (in PDF-format, viewable with Adobe Acrobat) are used by the Central District of California, but may be considered typical since bankruptcy forms are relatively uniform throughout the United States.

12.2.3 The Bankruptcy Petition

A bankruptcy petition requesting one of two prescribed courses of action must be included with the filing. Under the first option, the debtor may reorganize his or her financial affairs under Chapter 11 or Chapter 13 (or Chapter 12 for a family farmer) and remain in some form of control, albeit under strict court supervision.

The second choice is to file a simple liquidation under Chapter 7 and allow a trustee to liquidate his or her assets and pay the remaining sums to creditors in accordance with the priorities established under the bankruptcy code. Although some classes of creditors may receive a higher priority due to a statutory right, that is, taxes versus general unsecured creditors, creditors cannot be subject to any arbitrary discrimination on the part of the debtor.

The bankruptcy schedules are filed under a penalty of perjury. Consequently, any intentional misstatement included in the bankruptcy schedules may subject the debtor to criminal penalties.

Within a short time following the filing of a bankruptcy petition, a time, date, and place will be arranged for the debtor to be placed under oath and answer the questions of any creditors wishing to ask questions. This examination is called a 341a meeting, that is, a First Meeting of Creditors, as mandated by the bankruptcy code.

If an individual debtor (primarily a person) files his or her schedules and statements in good faith and complies with all other requirements, he or she will be allowed a *discharge* of their debts in accordance with bankruptcy law. A corporation is not allowed a discharge under the same provisions afforded an individual debtor.

12.3 FRAUD IN BANKRUPTCY FILINGS

Tens of thousands of persons seeking to be relieved of their debts follow the above-referenced procedure every year. There are, however, many who seek to avail themselves of the protection afforded under the bankruptcy code without complying with all the applicable bankruptcy code requirements.

Many CPAs can recognize fraud when they encounter it. CPAs who have not had direct experience with the criminal justice system, however, may find themselves on uncertain ground as they try to understand the distinction between civil and criminal fraud.

The following sections will provide some limited assistance in this area, but the exact demarcation between civil and criminal matters in any particular case is best left to legal counsel or law enforcement. The CPA should develop the facts and underlying supporting documentation of any alleged fraud and allow the lawyers to make that distinction. CPAs should keep in mind the following concepts that relate to bankruptcy fraud.

12.3.1 Materiality

Materiality is a concept that CPAs must deal with routinely. CPAs believe that financial statements must be materially correct and materiality is often defined as an omission or misstatement within five percent of the correct amount. However, the five-percent materiality rule does not apply in bankruptcy fraud.

Failure to Disclose Assets

If, for example, a debtor files bankruptcy schedules and knowingly fails to include a one-third interest in a small boat valued at \$30,000, with ownership shared by other members of the family, that oversight may be deemed material in the accounting sense, especially if the debtor's total net worth is small. The knowing exclusion of such an amount may technically qualify as a bankruptcy crime but the act may not rise to the level of prosecutorial merit in the opinion of the United States Attorney. However, if a debtor somehow conveniently forgets \$1 million in a Swiss bank account, that oversight will not be similarly forgiven, even if such a large sum constitutes only two percent of the debtor's total assets.

Geographical Differences

The meaning of materiality may also vary according to location. What may deeply offend the moral and legal sensibilities in Topeka, Kansas, may be dismissed with a wave of the hand in Los Angeles or New York.

Providing a Complete Report

The best course of action when faced with the dilemma of whether or not an action will be deemed material is simply to provide a complete report of the findings and allow others to make that decision. Of course, that full reporting concept should be tempered with financial and cost considerations such as the cost required to uncover such omissions fully.

12.3.2 Knowledge and Fraudulent Intent

Knowledge and intent are legal concepts probably best left to be discussed by lawyers. There are, however, some common-sense elements that may offer assistance to the CPA when analyzing various elements of bankruptcy fraud.

Debtor Knowledge

The government is not required to demonstrate that the debtor knew his or her acts or omissions were unlawful, but the government is required to demonstrate that the defendant acted knowingly and fraudulently. In fact, a debtor should be very careful about the contents of any documents he or she signs. If those schedules are later found to be fraudulent, the debtor will probably be unable to assert complete ignorance as a defense.

The courts have routinely characterized such action as *willful blindness* and have deemed them nonexculpatory, although an *inadvertent* mistake will not support a violation.

Circumstantial Evidence

It is also possible to demonstrate fraudulent intent through circumstantial evidence and inferences can be drawn through observing a course of conduct. In fact, circumstantial evidence and inferences from behavior often constitute the bulk of the evidence in bankruptcy fraud. If a bankruptcy is filed for a retail business and there is a later determination that the schedules omitted substantial levels of inventory previously listed on the books and records of the debtor, it would be natural to question such an omission, especially if there was no visible cash from the sale of the inventory.

In one instance, the president and former owner of the company volunteered that he had sold the inventory in the ordinary course of business just before the bankruptcy and had deposited the funds in the bank account of a creditor, pursuant to a prior agreement. Such action may be unwise but is not in and of itself a criminal act. It would be difficult to assert that such action was a premeditated attempt to deprive the creditors of funds to enrich the former owner of the company at their expense since the cash was still available but simply deposited erroneously into a creditor's account according to a procedure in place before the bankruptcy.

If, on the other hand, the former owner of the business had filed a police report alleging theft of the entire inventory just before the bankruptcy, and it was later determined that the former owner had secretly removed the inventory with the help of accomplices and pocketed the proceeds from its sale, such action would clearly have been knowing and fraudulent. It would be difficult to believe otherwise.

12.3.3 Criminal Prosecution

Judicial Discretion

It is important for any CPA to understand that what may seem a very clear bankruptcy fraud worthy of incarceration may not necessarily draw a federal prosecutor to the same conclusion. The decision of a federal prosecutor as to whether or not to prosecute a bankruptcy fraud may hinge on a number of factors such as those listed below.

Law Enforcement Staffing Limitations

The United States Attorney's Office and the FBI or other investigative agencies have staffing limitations similar to those of any organization. For instance, the day after the World Trade Center attack, it would have been difficult to generate a lot of enthusiasm for removing FBI agents from the terrorism investigation to pursue a bankruptcy allegation. Granting that most priorities are not as clearly defined as this, normal personnel-allocation matters are a daily problem. Prosecution priorities are often established on a national basis but local offices can decide to pursue any number of violations they deem to be of great importance to that locale. The issue of materiality or the amount of money involved in the fraud is clearly a determining factor—the larger the loss, the greater the likelihood of an investigation. Some offices may choose to emphasize violent crimes they consider more dangerous to the citizens of their communities than nonviolent bankruptcy crimes. Bankruptcy cases often require a significant investment of hours before a successful

indictment can be brought, whereas other cases may require fewer hours and still produce the desired indictment.

Self-Incrimination Issues

A person subject to a bankruptcy fraud investigation may choose to invoke their rights under the Fifth Amendment, which gives them the right not to answer any questions on the premise that they do not want to incriminate themselves.

Even though CPAs usually do not face this issue, should it arise, the following are among the points that should be remembered:

1. Should you wish to obtain information from the debtor and he or she chooses not to speak with you, be careful not to compel or threaten him or her. Respect his or her Fifth Amendment rights. In any accounting investigations of this nature, it is far better to focus your efforts on the accounting records, at least in the early stages.
2. The issue of self-incrimination may arise during your attempts to obtain the accounting records. Debtors may assert that privilege to prohibit the CPA from reviewing their records. The CPA should seek competent legal counsel in such cases. As a general rule, however, access to debtor records is not necessarily protected under the Fifth Amendment if the existence of the records is undisputed. The CPA should provide a reasonable basis for requesting the records and make certain that such a request is both sensible and within the appropriate realm of inquiry.
3. The Fifth Amendment is a personal right, not a blanket right to be extended to all associates of the debtor. For instance, a CPA or bookkeeper employed by the debtor will generally be far more helpful in providing information than even the debtor. Also, even though the bookkeeper can assert his or her own individual privilege under the Fifth Amendment, he or she has no power to extend that privilege to his or her employer, the debtor.
4. The right to seek records in a bankruptcy is rather broad. If the debtor, a bank, or other party, refuses to provide records voluntarily, an order to compel production of documents, a Rule 2004 examination request, is filed in the bankruptcy court. The Rule 2004 examination is found in the Federal Rules of Bankruptcy Procedure. It is somewhat similar to a subpoena but can be broader. The bankruptcy judge will usually issue a Rule 2004 examination order without a hearing upon application from any party in interest. If the party to whom the 2004 examination is directed objects, a hearing will be scheduled. The assertion that the records of the debtor may be incriminating is not likely to draw a sympathetic response from the court if the existence of those records is undisputed.
5. Be patient and methodical in your attempts to collect and review documents. The process is never quite as neat or fast as depicted on television. It is possible to pursue both a civil and a criminal bankruptcy fraud investigation at the same time. The existence of a criminal investigation may make the normal review of records somewhat more difficult. Keep focused on the task and do not be dissuaded from your right to review them.
6. Finally, in appropriate civil cases, the debtor's invocation of his Fifth Amendment privilege may support an adverse inference by the bankruptcy court. The court is

allowed to take note of such an adverse inference if they so choose, and independent evidence exists of the fact to which the party refuses to answer.

12.4 ELEMENTS OF BANKRUPTCY FRAUD

There are a number of possible ways for an individual to engage in bankruptcy fraud. The list below, while not exhaustive, is an example of the main types of fraud used to circumvent the bankruptcy code.

12.4.1 Nondisclosure or Concealment of Assets

Asset concealment consists of knowingly concealing the existence of an asset by not disclosing the asset in the schedules and statements filed in the bankruptcy. The FBI estimates that approximately 70 percent of all bankruptcy crimes are committed through asset concealment.

Title 18, Section 152 of the United States Code defines as criminal

a person who—(1) knowingly and *fraudulently conceals* from a custodian, trustee, marshal, or other officer of the court charged with the control or custody of property, or, in connection with a case under title 11, from creditors or the United States Trustee, *any property* belonging to the estate of the debtor [emphasis added].

Kinds of Concealed Assets

The following are examples of commonly concealed assets:

1. Potential gain or loss from a personal injury lawsuit
2. Interest held by a debtor in real property
3. Bank and investment accounts not disclosed on the schedules
4. Investments in nondebtor entities
5. Art or other valuable collectibles
6. Investments in any assets that include both a beneficial or recorded interest in behalf of the debtor
7. Intentional undervaluation of assets to convince creditors or the Chapter 7 Trustee to abandon any interest in the property and allow the debtor to retain the asset for use after the bankruptcy (An example of undervaluation may be to list an asset, such as a piece of real estate, but to *knowingly* attach a minimal value to the property by excluding some element of value such as a valuable right of way or possible mineral rights.)

Uncovering Concealed Assets

The most important fact to remember when trying to uncover concealed assets is that they were not always concealed. There were probably times during the period preceding the bankruptcy when those assets were listed in the financial statements and general ledgers of the debtor, or both. You must backtrack until you reach the period when the asset was either fully or partially disclosed.

The following is a list of steps CPAs can take to uncover concealed assets:

1. As a debtor's financial difficulties begin, it is usual for him or her to seek financing from traditional financial institutions to ease the problems. When seeking a loan at such a time, most individuals make extensive disclosure of their assets. In other words, they put everything possible into their balance sheet to convince the financial institution of their creditworthiness. Therefore, a good step is to find all banks that may have received such a financial statement within the last five years and obtain a copy of those loan applications. Credit reports often identify requests or applications for credit and list the bank from which the credit was sought. A number of financial institutions may have had a long history with the debtor and may even be creditors in the bankruptcy. Prior applications for credit should be sought from those banks. Also, banks often have prior tax returns of the debtor. Such returns are not privileged in the hands of third parties. However, always consult legal counsel before attempting to obtain bank, credit, or other records to avoid violating laws, regulations, and the debtors' rights.
2. Obtain tax returns for as far back as possible, preferably for at least five years. Review those tax returns for any hidden income that might be reflected in K-1 forms from partnership accounts or 1099 forms from either financial institutions or other income sources.
3. Engage a licensed investigative firm to conduct a background search of property and business records for the debtor over the last few years. Because so many records are contained on computerized databases, a significant amount of information can be obtained from this source, and at a reasonable cost. Such analysis may include credit-report services that generally provide significant information that can be used to supplement information from other sources.
4. Review various listing agencies such as Network Solution for URLs to determine whether the debtor is holding any valuable URLs that have not been recorded on the debtor's books and records.
5. Ultimately, the most complete analysis for the discovery of concealed assets is a review of all cash flowing in and out of the debtor's accounts over the last four years, or longer if necessary. The decision to undertake such an analysis is not made routinely. In fact, it is seldom done unless there exists some unexplained loss or another compelling reason from an accounting viewpoint. The expense of performing a complete cash analysis of a debtor will need to be justified on a cost basis and will certainly not be feasible except in larger bankruptcies wherein the financial benefits outweigh the expense. The process to complete such an analysis is outlined below.

If a cash-flow analysis is contemplated, it is necessary to obtain the debtor's bank statements and all related entities for the period being analyzed in order to create a database of all receipts and disbursements. A materiality level reflecting the number of bank accounts, the activity in each account, and overall cost-benefit issues should be established prior to preparing such a database. While analyzing the bank statements, the CPA should keep the following issues in mind:

- Look for large or unusual receipts and disbursements, or both, and trace those transactions to supporting documentation within the records of the debtor. It is entirely possible that these payments may represent the purchase of assets or the payment of liabilities not recorded by the debtor.

- Review monthly or periodic payments of equal amounts that could represent regular loan payments. Make certain that the assets represented by such payments are included in the records of the debtor.
- Ascertain whether any monthly or periodic payments are being made to related parties. Such payments may either represent a transfer of assets for little or no consideration or create a situation in which a related party is able to acquire assets belonging to the estate for return to the debtor at a later date.
- Review payments made for real and personal property taxes. The information from invoices and check details may provide supporting documentation regarding assets not listed in the records of the debtor.
- Analyze payments to insurance companies. The record of these transactions can reveal information concerning insured assets. The invoices and check details may provide additional insight into what may be unlisted assets rightfully belonging to the estate.
- Analyze unusual expense items that might point to assets not included in the debtor's records. For example, monthly payments for hangar rental might indicate the existence of an airplane.

12.4.2 False Information in Filing

The filing of a bankruptcy petition calls for a declaration under penalty of perjury that all information included therein is true and correct. United States Code (USC) Section 152 and Section 157 prohibit making a "false oath or account" or a "false declaration, certificate, verification, or statement under penalty of perjury." Such false information can include any number of items such as false social security numbers, fictitious addresses, and even fake names.

The "knowingly and fraudulently" portion of Section 152 is not intended to encompass an inadvertent transposition of the existing social security numbers or minor misspelling of names, but contemplates the willful intent usually evident in identity thefts.

It should be noted that the debtor cannot simply assert that he or she failed to pay attention to the bankruptcy documents when signing, since the debtor is also required to declare orally and under penalty of perjury at the 341a meeting that all information included in the schedules and statements is true and correct in every way.

All information included in a bankruptcy filing must be accurate. Any *knowing* exclusion or misstatement could be considered a *false declaration or statement*. Such information includes understating the level of postpetition income as required in the bankruptcy schedules. Should income be sufficiently large and debts sufficiently small, a motion may be filed to set aside the bankruptcy as a bad-faith filing.

One example of false information in filing would be identity theft, a violation of Section 157, wherein a person essentially *steals* the identity of another, incurs substantial credit card or other debt, and then files a bankruptcy under the stolen person's name and social security number to forestall the actions of creditors. This kind of theft is increasing as the volume of Internet shopping grows.

The deliberate and intentional misstatement of income is another example of false information. A well-compensated salesman who knowingly convinces some clients to defer

commissions on sales to be completed before the bankruptcy will necessarily understate projected income as reported on Schedule J. This understatement would allow the debtor to receive the deferred income after his discharge from bankruptcy.

Uncovering Concealed False Information

The following is a list of steps CPAs can take to uncover concealed false information:

1. Engage a licensed investigative firm to provide a background check on past addresses and social security numbers.
2. Review information gleaned from investment accounts and credit card accounts to ascertain spending practices.
3. Review tax returns for inconsistencies including a large variation in income between present and prior years.

12.4.3 False Claims Filed in a Bankruptcy

Following the filing of a bankruptcy petition, in cases where assets are available, creditors are generally required to file a *proof of claim* specifying the nature and amount of their claim. Exhibit B, Proof Claim Form, used in the Central District of California, is included on the *Fraud Prevention Checklists CD-ROM*.

Knowingly filing a false claim in bankruptcy is a serious matter that can result in criminal action. The filing of such a claim must generally be exceptional to warrant the imposition of criminal action. However, the filing of a false proof of claim could be as simple as trying to hide a small proof of claim among a large number of nondescript claims.

On the other hand, it could be as complex as a creditor and debtor conspiring to cure a defect in a security interest to allow the creditor a secured priority to which he or she would not be entitled under normal conditions. Often, this is done because a debtor may have a personal guarantee and wishes to avoid a call on that guarantee by granting the creditor a superior access to assets in the bankruptcy.

An example may be an agreement between the debtor and a creditor during the bankruptcy for the creditor to provide a false invoice for services or assets not delivered. Under normal conditions, most postpetition bankruptcy invoices would be paid, thereby granting the creditor payment to which he or she would not be entitled were it not for the filing of a false invoice. One of the most common false claim methods is to file an inflated claim. For instance, a \$100 valid claim could be filed for \$1,000.

Uncovering False Claims

The following is a list of steps CPAs can take to uncover false claims:

1. Conduct a review of the accounts payable subsidiary ledgers for intermittent periods prior to the bankruptcy and compare those ledgers to existing claims to determine inconsistencies. Many debtors will have open invoice files. It is likely that the accounts payable subsidiary ledgers have not been updated for all open invoices. Many creditors will continue to send invoices that can be used for comparative purposes long after the bankruptcy has been filed.

2. Analyze the payments made to creditors for the three to six months before the bankruptcy to determine whether any of the claims filed in the bankruptcy had been paid previously.
3. Review the payments made during the year before the filing to ensure that the creditors have applied the payments correctly. For example, a creditor could have both secured and unsecured claims with a debtor. Payments could be inappropriately applied to the unsecured claim so that the secured claim could retain its priority status after the filing.
4. Request supporting documentation from any creditor filing a questionable claim and conduct a detailed review of such documentation.
5. If the information available leads you to believe that a creditor has engaged in the filing of a false claim, it may be advisable to schedule a Rule 2004 examination, in which the creditor provides documents relating to the claim and is placed under oath, and subjected to questioning. When asked to answer questions under oath, especially any questions concerning the validity of those claims, the creditor will often withdraw the claim to avoid close scrutiny.

12.4.4 Transfer of Assets Before a Bankruptcy Filing

One of the more common methods of concealing assets in violation of bankruptcy laws is to transfer assets without consideration before the actual bankruptcy filing. Should this scheme go undetected, the debtor could retrieve the assets from the conspiring party following the bankruptcy.

For example, the debtor in contemplation of bankruptcy agrees to sell an interest in a fledgling company to a friend for an insignificant sum on the basis of an unwritten agreement whereby the debtor can reacquire the interest in the company for a similarly insignificant sum.

Uncovering Transfer of Assets Before a Bankruptcy Filing

The following is a list of steps CPAs can take to uncover transfer of assets before a bankruptcy filing:

1. Many of the steps covered in this section are similar to those discussed in the section on the nondisclosure or concealment of assets. As in that section, it is important to understand that there was probably a period preceding the bankruptcy during which those assets were listed in the records of the debtor. Therefore, you should examine the debtor's balance sheets at different dates prior to the bankruptcy and make certain you can account for assets that have been transferred or otherwise disposed of.
2. Locate all banks that may have received a financial statement from the debtor within the last five years and obtain a copy of the loan applications they supported. Review those assets listed in the earlier financial statements and make certain they have been properly accounted for or adequate consideration has been received for them. It may be appropriate to trace the receipt of cash from the sale of those assets into the bank statements of the debtor.

3. Obtain tax returns for as far back as possible, preferably for at least five years. Review them for any hidden income that might be reflected in the K-1 forms from partnership accounts or 1099 forms from either financial institutions or other income sources. Determine whether those assets have been sold in the period just prior to the bankruptcy and whether adequate consideration was provided.
4. Engage a licensed investigative firm to conduct a background search of property and business listings for the debtor over the last few years.
5. Review various listing agencies for URLs to determine whether the debtor is holding any valuable URLs that have not been recorded on the debtor's books and records.
6. Look for large or unusual receipts and disbursements, or both, and trace those transactions to supporting documentation within the debtor's records. It is entirely possible that these payments may represent the purchase of assets or payment of liabilities not recorded by the debtor.
7. Review monthly or periodic payments of equal amounts that could represent regular loan payments. Make certain that the assets represented by such payments are included in the debtor's records.
8. Ascertain whether any monthly or periodic payments are being made to related parties. Such payments may represent a transfer of assets to the related party for little or no consideration or create a situation in which a related party is able to acquire assets belonging to the estate that will be made available to the debtor at a later date.
9. Review payments made for real and personal property taxes. The information from invoices and check detail may provide supporting documentation regarding assets not listed in the debtor's records.
10. Analyze payments made to insurance companies to find information concerning any insured assets. The invoices and check detail might provide additional insight into what could be unlisted assets rightfully belonging to the estate.
11. Analyze unusual expense items that might indicate assets not included in the debtor's records. For example, monthly payments for hangar rental might indicate the existence of an airplane.

Skimming the Cream Case Study

Cable & Wireless Broadcasters, Inc. (CWB), was a cable and satellite program distributor whose lenders had reason to question its financial soundness. CWB was materially late in making payments against its \$35-million debt. In fact, it was late in paying just about everybody. Additional financing from the principals was not forthcoming. Other creditors were threatening to cease providing essential services to CWB, including the means of transmitting the programming. The lenders were expecting CWB to collapse. Under the terms of the loan agreement, CPAs were called in to stanch the liquidity hemorrhage and discover what had happened to the \$35 million.

CWB's accounting records, correspondence, contracts, and computers were effectively controlled and inventoried, and copies immediately made of some of the

most critical records. These records revealed many instances of suspicious cash disbursements prior to the collapse:

- Payments to the principals' families for personal matters. Although the amounts were small, the fact that they were paid at all suggested that there might be improprieties in the accounts.
- *Loans* with no repayment record.
- Transfers without any obvious business purpose to offshore and overseas accounts.

Further investigation revealed collusion among the principals and the chief accounting officers. Business records, including cash disbursements and journals, were incomplete. The chief financial officer and controller were adept at concealing improper expenditures and describing them as legitimate business expenses. However, an expert search of the electronic documents contained on the hard drives of their computers discovered a secret bank account into which *commissions* had been deposited.

These commissions were applied against the loans received from the lenders, which benefited the principals who had established an offshore account in the name of an apparent charity. Nearly \$4 million was deposited into this *charity* from the CWB's main bank account. These findings were presented to the lender's counsel who then began negotiations with the principals' counsel.

To placate the lenders, avoid bad publicity and attacks against reputation, as well as criminal charges, CWB's principals quickly and quietly settled by being suddenly able to *find* the funds to repay the debts. The lenders were made whole without protracted and expensive litigation.

The Skimming the Cream case illustrates several important points regarding asset transfers before a bankruptcy filing:

1. The perpetrators of such a crime are usually desperate and, while they may cover their recent tracks, they often leave a trail behind that can easily be unraveled if the CPA starts his or her investigation early enough.
2. Fraudulent transfers or fraudulent conveyances, wherein an asset is converted to another form, often cash, are often connected to a fraudulent concealment of assets.
3. It is important for CPAs to be alert to the possibility that, in times of financial crisis, the principals of a company could be tempted to transfer assets in an attempt to protect themselves, notwithstanding the fact that the company may be doomed to failure.

12.4.5 Transfer of Assets After a Bankruptcy Filing

A debtor in functional control of his or her estate while in a Chapter 11 bankruptcy must obtain court approval, following notice to interested parties, to dispose or sell any assets owned by the estate. A Chapter 7 bankruptcy is not applicable in this instance as the debtor relinquishes control of the estate assets, if any, to an appointed Chapter 7 Trustee.

Although not as common as the surreptitious concealing of assets before filing a bankruptcy, certain debtors transfer assets for inadequate or, in some cases, no consideration, without notice to any parties or bankruptcy court approval. This insidious practice has the same ultimate goal of depriving creditors of a fair and equitable allocation of assets.

For example, a debtor conspires to transfer significant amounts of retail inventory to a noncreditor third party for little or no consideration. The intention is to allow the debtor to benefit from the third party after the bankruptcy.

Uncovering Transfer of Assets After a Bankruptcy Filing

The following is a list of steps CPAs can take to uncover transfers of assets after a bankruptcy:

1. The best way to discover transfers of inventory for no consideration is to conduct a physical inventory following the bankruptcy and reconstruct the inventory numbers that would be expected under historic operating margins.
2. The manner of maintaining control of assets after bankruptcy is not much different from the way of control prior to bankruptcy. One should employ audit-like controls and procedures and test their validity.

12.4.6 Bribery or Threats

A creditor might use bribery, threats, or intimidation to secure the promise of the debtor to pay his or her debts to the exclusion of all others. Such agreement is a violation by both parties.

There is also the possibility that both the debtor and a creditor could engage in a separate *side-bar* agreement wherein the creditor agrees not to take certain action in return for property, money, or some other improper advantage.

For example, upon hearing of a bankruptcy filing, a creditor threatens the debtor with physical harm unless arrangements can be made to assure payment of his prepetition claim. The debtor, fearing for his or her safety, agrees to pay the creditor from postpetition proceeds and ultimately does so.

In another case, a creditor discovers that the debtor has secreted funds in violation of the bankruptcy code. Rather than informing the appropriate authorities of that knowledge, the creditor threatens to expose the action unless the debtor agrees to pay him or her from the ill-gotten funds. The debtor, sensing the criminal and civil penalties consequent on such a deviation from ethical behavior, agrees to pay the creditor to the exclusion of all other creditors.

Uncovering the Existence of Bribery or Threats

The following is a list of steps CPAs can take to uncover the existence of bribery or threats:

1. It is difficult to ascertain the existence of bribery or threats solely from the accounting records. Most of the transactions that occur as a direct result of such behavior tend to be *off-book* transactions. In other words, such payments are often completed through cash or checks from other sources not readily identifiable from the records of the debtor.

2. It may be advantageous to review the liabilities of the debtor before the bankruptcy and determine whether any of the creditors failed to file claims or were somehow disregarded following the bankruptcy. Upon ascertaining the existence of any such creditors, interviews with both the debtor and creditor should be conducted to determine whether any threats or bribery were involved.
3. Since the bribery or threat might include an attempt to discourage open bidding on the sale of assets, special efforts should be made to be certain that the open bidding process is maintained during the bankruptcy and that all interested parties are allowed to participate fully. The CPA may wish to review the process to establish procedures for bidding and conduct a limited inquiry to make certain that fair value was obtained in all asset sales.

12.4.7 Concealment, Destruction, or Withholding of Documents

The records of the debtor should be available for review by the creditors of the estate as well as a trustee or any party that can establish a right of review. The retention of such documents is vitally important to the efficient administration of the estate. It is also a violation to withhold documents even though the documents have not been destroyed.

Section 152 Para. 8, specifically states, whoever, "after the filing of a case under title 11 or in contemplation thereof, knowingly and fraudulently conceals, destroys, mutilates, falsifies, or makes a false entry in any recorded information (including books, documents, records, and papers) relating to the property or financial affairs of a debtor," shall be fined under [18 U.S.C. Section 5371], imprisoned not more than five years, or both.

It would also be a violation to interfere with electronic records by destroying, deleting, or altering computer files of the debtor.

Even if documents are destroyed in violation of the law, many of the original records, such as bank statements and canceled checks, can be obtained by subpoena from third parties. The cost of so doing can, however, be prohibitive, especially in small cases.

Uncovering or Preventing the Destruction or Withholding of Documents

The following is a list of steps CPAs can take to uncover or prevent the destruction or withholding of documents:

1. The retention of adequate accounting records is vital. Therefore, as soon as practicable after filing the bankruptcy or determining that a review must be made of the records, it is imperative that an inventory be made of all existing records. Should there be any possibility of the debtor destroying the records, it may be wise to engage a copy service to obtain a separate copy of all relevant records.
2. While the inventory of documents is being taken, all electronic evidence, that is, all data on computer hard drives, should be preserved by a computer forensics expert. This is an extremely important step. Electronic files might be difficult or impossible to recover afterwards.
3. It is possible to obtain copies of federal and state tax returns by first obtaining power of attorney and then submitting the appropriate forms to both the Internal Revenue Service (IRS) and the state taxing authorities. A bankruptcy trustee can obtain copies of

federal and state tax returns by simply making a written request supported by a notice of the trustee appointment.

4. Upon completion of the inventory analysis, a secure location must be obtained for the safekeeping of program diskettes and CDs as well as data diskettes, CDs and backup tapes, or any other storage devices. In more complex cases, it may be important to create a separate and secure location to store all of the records and control access.
5. An immediate contact should be made with the debtor's banks, outside CPA firm, and legal counsel as they often have important records and documents in their possession.
6. If the records have been seized by a government agency pursuant to a subpoena, it is often very difficult to obtain access because of secrecy provisions inherent in the grand jury process. However, it still may be possible to obtain copies of certain records, especially, if the government chooses to rely upon the nongovernment accountant's analysis as supporting documentation for their own criminal case.

12.5 KINDS OF BANKRUPTCY FRAUD

12.5.1 Bust Out and Bleed Out

The systematic pillaging of assets while increasing the liabilities of a successful company is often referred to as a *bust out*. This procedure is used by the more seasoned element of our criminal population and is usually brazen and easily identified.

The destruction of a company can be accomplished relatively quickly or can drag on for years as the owners methodically bleed the company of assets while steadily increasing liabilities. This slower process is generally referred to as a *bleed out*. Such a blatant and criminal abuse of the bankruptcy protections can often provoke the draconian penalties found in the Racketeer Influenced and Corrupt Organizations (RICO) statute.

Conducting the necessary accounting analysis to prove that a company was the victim of a bust out or bleed out scheme to defraud creditors is a very time-consuming and laborious proposition.

For example, a formerly successful retail clothing business with an excellent credit rating is in arrears with its clothing suppliers. The usual liquidity ratios suffer drastic reversals as inventory and other liquid assets inexplicably disappear and bills remain unpaid.

Meanwhile, the operating capital normally retained for paying day-to-day expenses and purchasing inventory are transferred to a separate account for the personal benefit of the owner. The company ultimately files bankruptcy and provides a minimal level of assets while listing an extremely large number of unsecured creditors. The hope of the debtor is that the bankruptcy will pass quietly through the system with a minimum of scrutiny.

Uncovering a Bust Out or Bleed Out Before a Bankruptcy

The following is a list of steps CPAs can take to uncover a bust out or bleed out before a bankruptcy:

1. Perform a detailed ratio analysis to discover asset or liability accounts for which further analysis is warranted. These ratios may point the CPA to an inventory or accounts receivable problem.

2. Review the salaries and consulting fees paid to owners, family members, and other related parties. Look closely at bonuses or other types of compensation.
3. Analyze the travel and entertainment expense records to determine whether the company is paying for significant personal items. An analysis of such expenses may reveal that large personal expenses are being paid for the benefit of the owners, their family, or related parties.
4. Analyze the company's debt to discover whether the proceeds of any issue were actually received and used in internal operations.
5. Review transfers of assets or liabilities. The determination should be made as to whether such transfers were made "knowingly and fraudulently."
6. Analyze rents and lease payments. In circumstances such as these, it is common for parties to lease physical facilities, equipment, or vehicles to the debtor at inflated rates in not *arms-length* transactions.

12.5.2 Embezzlement by a Trustee or Officer

If a trustee or other officer appropriates assets of the estate *to a person's own use*, he or she is violating his or her fiduciary duty. It is important to note that it is also a violation for a trustee, officer, or similarly situated person to secrete or destroy any document belonging to the estate.

It is a violation of the law to purchase any property directly or indirectly from the estate of which he or she is an officer even if adequate consideration is provided

It is improper for the trustee to allow no reasonable opportunity for inspection of documents and accounts relating to the affairs of estates in his or her charge by parties in interest when directed to do so by the court.

A CPA should follow the same steps and procedures in uncovering and validating embezzlement during bankruptcy as he or she would in an embezzlement investigation at an ongoing business. The principles and methods are similar.

12.5.3 Serial Filings

One of the most pernicious acts in bankruptcy is a procedure intended primarily to take advantage of the automatic stay to prevent foreclosure on certain assets and collection of other debts.

For example, an individual in significant financial distress has not made payments on a house for an extended period of time. After a notice of default and just prior to the actual foreclosure, the following occur:

- The debtor files a bankruptcy.
- The lienholder files a motion for relief from the automatic stay citing lack of equity and lack of payments.
- The court grants relief.
- The foreclosure process begins again.

- Just before completion of the second foreclosure attempt, the debtor's wife, who is listed as a co-owner on the property, files a bankruptcy thereby stopping the foreclosure action once again.

This procedure can continue indefinitely as other parties holding an arguable interest in the property file a succession of bankruptcies until the judge imposes various restrictions including sanctions on those parties filing bankruptcies in bad faith.

The same procedure can be used in differing degrees, but under the same concept by those facing eviction in rental units or management companies operating commercial real property.

12.5.4 Service Petition Mills

Lawyers represent a significant number of those filing bankruptcy. As such, they are governed by standards and procedures established by the regulatory bodies of their profession. Lawyers, by definition, are not included in service petition mills.

Another group assisting in the filing of bankruptcies is the qualified personnel working for legal aid services who, although not attorneys, are nevertheless competent and provide a lower cost alternative.

There are, however, a number of unscrupulous services that set themselves up primarily in low-income areas and engage in heavy advertising offering their services as a solution to financial problems. They often charge an excessive amount for a very limited service, namely, typing the petition with minimal assistance. These services often prepare but do not file the bankruptcy. Since their names are not mentioned as having prepared the petition, they disappear quickly should problems with the filing ensue. Occasionally, they step over the line into complicity by filing fraudulent and inaccurate petitions.

The proper response upon uncovering a practice of this nature is to report the findings promptly to both the United States Attorney and the local Office of the United States Trustee. The U.S. Trustee usually takes action promptly even making legal filings if necessary to drive unethical practitioners from the market.

12.5.5 Ponzi Schemes

A Ponzi scheme is conceived as a *pyramid* (and often referred to as a pyramid scheme). As the early investors recruit new investors and these investors, in turn, recruit yet others, the large number of investors forming the base support the small number of scheme organizers and early investors at the top. Investors are induced to join by the promise of returns exceeding market rates. These promised returns are actually paid out at the beginning of the fraud to lure new prospects to invest their money. Payments to previous investors are made from the funds paid in by later investors. As the number of investors grows exponentially, soon there is not enough money available to pay all investors the promised returns. In the end, the majority of investors are left with millions of dollars in claims against a paltry amount of assets.

As the number of investors grows, the amount of assets declines, and lawsuits commence, the debtor files for bankruptcy claiming that an economic setback and not the pitiless mathematics of the pyramid scam itself was the cause of the financial collapse.

The creation of a Ponzi scheme does not constitute a violation of the bankruptcy law in and of itself. The filing of a bankruptcy to conceal the existence of a Ponzi scheme does, however, violate the bankruptcy law.

A review of accounting records to establish the existence of a Ponzi scheme can prove to be extremely difficult. It is not, however, impossible and in fact has been done many times.

Uncovering a Ponzi Scheme

The following is a list of steps CPAs can take to uncover a Ponzi scheme:

1. Ponzi schemes are usually of short duration. The CPA should be aware of the possibility, however, that a Ponzi scheme could keep operating for many years. It is also possible that a legitimate business could become a Ponzi scheme as specific financials deteriorate, government regulations change, or the general economy declines.
2. Because a Ponzi scheme by its very nature is fraudulent, the CPA cannot always use the financial statements as a guide because of the likelihood they may contain significant misstatements. The best source of information may actually be the cash receipt and disbursement activity.
3. An analysis of the balance sheet at various dates in the past can provide meaningful information regarding the existence of a Ponzi scheme if the difficult problem of eliminating material misstatements can be overcome. The net equity section of the balance sheet can reflect a change over time from a positive balance to negative equity. This is usually the result of growing losses, diminishing assets, and increasing liabilities. It is even possible that the entity was in a negative equity position for the entire period of analysis with the result that the insolvency continued to deepen.
4. An historical analysis of the income statement often reflects little or no legitimate business activity. Once again, material misstatements must be identified and adjusted to provide meaningful results. Revenues may actually decline while expenses increase exponentially. A detailed analysis of the cash receipts may demonstrate that the majority of cash flow is provided by new debt and new investors with very little emanating from operations.
5. In the typical Ponzi operation, an analysis of cash receipts and disbursements should reveal a constantly growing need for cash. Cash from new investors or new debt is never enough to stop the endless need for more and more cash to meet ever-increasing obligations.
6. A month-by-month analysis of the general and subsidiary ledgers may demonstrate the replacement of old debt and old investors with new debt and new investors.
7. It is common for the cash receipt and disbursement analysis to show significant amounts paid to the owners and/or insiders. Because the perpetrators of Ponzi schemes recognize their entity is doomed to self-destruct, they often engage in an orgy of cash disbursements in the period just prior to its inevitable collapse. A review of cash receipts and disbursements during this critical time can lay bare such an illegitimate outflow.

12.6 PUNISHMENT PROVISIONS

As discussed in greater detail below, the harshness of punishment for bankruptcy fraud may vary to a considerable degree for any number of reasons.

Usually, for each single criminal violation of the bankruptcy code as detailed in most of the matters and examples listed above, the penalty prescribed shall include a fine and imprisonment for *not more than five years, or both*.

12.7 REFERRAL OF BANKRUPTCY FRAUD

If you are a trustee, judge, or receiver, the code requires that you *shall* report to the United States Attorney whenever you have reasonable grounds to believe that a criminal violation has occurred and that an investigation is warranted. That duty is mandatory. If you are not serving in any of the capacities referred to above, you should seek legal counsel as to your obligation to report criminal activity.

Once you have determined that a referral is necessary, the fraud should be reported to both the United States Attorney and the United States Trustee in your jurisdiction. The referral should be in the form of a written report. An oral report will be insufficient. Exhibit C, Bankruptcy Referral Letter, is included on the *Fraud Prevention Checklists CD-ROM*.

The referral report should contain the following:

1. *A short summary of the alleged crime.* For example, this referral concerns concealment of assets in violation of Section 152 or concealment or destruction of records in violation of Section 152.
2. *The name or names of the subjects involved.* If there was a corporation or partnership involved, all owners or partners should be included in the report. If available, you should include the dates of birth and social security numbers of those involved.
3. *A complete and factual presentation of the evidence supporting the assertion of the violation.* Keep in mind that a general statement that a person or entity has filed multiple bankruptcies may be relevant in establishing intent. The underlying evidence, however, must be compelling and specific. Generalized allegations will not be sufficient.
4. *The estimated total loss or amount of harm caused by the alleged bankruptcy violation.*
5. *The names of the witnesses or potential witnesses.* If available, provide addresses and telephone numbers.
6. *A list of the documentary evidence that is available supporting the allegation and the location of such evidence.*

The referral report need not include every scintilla of information constituting the facts and the evidence. You can provide additional information to the investigative agency should an affirmative decision be made to conduct an investigation based on the referral.

It is important to note that a fully prepared referral and subsequent analysis will greatly increase chances for a successful criminal investigation and indictment. Simply put—the more complete the report, the better.

As already discussed, investigative agencies are always mindful of the personnel requirements necessary to complete an investigation. There are never enough people to get all the jobs done immediately.

Finally, the CPA should not engage in judgmental categorizations that imply that the United States Attorney is compelled to take action based on the referral.

12.8 BANKRUPTCY FRAUD CHECKLIST

Table 12.1, Bankruptcy Fraud Checklist, is designed to assist CPAs in addressing bankruptcy fraud. Generally, all *No* answers require investigation and follow-up. The results should be documented. Use the *Ref* column to cross-reference the checklist to any additional working papers. The checklist is intended for general guidance and information only.

TABLE 12.1 BANKRUPTCY FRAUD CHECKLIST

| Bankruptcy Fraud Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| 1. Non-Disclosure or Concealment of Assets | | | | |
| <i>A no answer to any of the questions in this section indicates a greater likelihood of potential nondisclosure or concealment of assets.</i> | | | | |
| a. Have the known assets been fairly valued? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. Have the debtor's bank statements for the last five years been obtained? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Has a cash-flow analysis of the debtor's accounts been made for the last four years at least on the basis of these bank statements? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Are there any unusual receipts or disbursements? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Are there any regular periodic payments of equal amounts that cannot be accounted for by an automobile or other asset? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Have income tax returns from previous years been reviewed for undeclared income sources? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. Have property tax returns from previous years been reviewed for undeclared property ownership? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| h. Are there any unsettled personal injury lawsuits outstanding? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| i. Does the debtor hold any real interest in any real properties other than his or her residence? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| j. Are there any bank or investment accounts not disclosed on the schedules? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| k. Are there any works of art or other collectibles? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| l. Are there any investments that include either a beneficial or recorded interest on the debtor's behalf? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| m. Have insurance premium payments been examined for any insured but undeclared assets? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| n. Have the debtor's financial statements filed with former lenders been reviewed? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

TABLE 12.1 (continued)

| Bankruptcy Fraud Checklist | Yes | No | NA | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| o. there any assets revealed on the balance sheets of previous fiscal periods that have not been accounted for? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| p. Has a licensed private investigative firm been engaged to search property and business listings for assets of the debtor owned over the last few years? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| q. Does the debtor hold any valuable unrecorded URLs? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. False Information in Filing | | | | |
| a. Has there been a background check on the debtor's past addresses and social security numbers? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Have investment and credit card accounts been reviewed to find spending patterns? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. False claims filed in bankruptcy | | | | |
| a. Have the accounts payable subsidiary ledgers for intermittent periods in the past been examined and compared for inconsistencies? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Have any payments to creditors already made within the last six months reappeared in the bankruptcy schedules? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Have payments made within the last year been correctly applied to secured and unsecured claims so that the priority of the creditors' claims has been properly maintained? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Have claims from dubious creditors been thoroughly examined? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. If suspicious claims are being pressed vigorously, has a Rule 2004 examination been scheduled to examine the creditor under oath? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 4. Transfer of Assets Before a Bankruptcy | | | | |
| a. Have financial statements for past years been examined for the ownership or disposition of assets not present in the current statements? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Have the loan applications supported by these financial statements been examined? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Have previous tax returns been examined for income in the K-1 forms from partnerships or the 1099 forms from financial institutions or elsewhere? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Have any assets revealed on these earlier statements been sold just prior to the bankruptcy filing? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 12.1 (continued)

| Bankruptcy Fraud Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| e. Have property and business listings of the debtor been searched? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. Is the debtor holding any valuable URLs? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| g. Have there been any recent large receipts or disbursements recorded by the debtor? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| h. Are there any periodic equal payments unaccounted for by the recorded assets? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| i. Are there any regular payments to related parties? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| j. Can all invoices and check detail be explained by the recorded assets? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| k. Are insurance premiums being paid for unrecorded assets? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| l. Are there any unusual expense items unaccounted for? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 5. Transfer of Assets After a Bankruptcy | | | | |
| a. Was a physical inventory conducted immediately after the bankruptcy? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Have any assets been transferred for no consideration? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Have effective audit-like accounting controls been applied to monitor the disposition of financial assets after the bankruptcy? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 6. Bribery or Threats | | | | |
| a. Have any creditors failed to file claims against the debtor? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Have any creditors been disregarded following the bankruptcy? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Has the open bidding process been impaired in any way or by any person? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Has the open bidding process been reviewed for fairness? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Was fair value received for all goods sold? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 7. Concealment, Destruction, or Withholding of Documents | | | | |
| a. Has an inventory been made of all records? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Have copies been made of all relevant records? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Have the debtors' electronic records been preserved by a qualified computer forensics expert? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Have copies of federal and state tax returns been applied for? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

TABLE 12.1 (continued)

| Bankruptcy Fraud Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| e. Are program and data diskettes and CDs safely and securely stored? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Have records at the offices of the debtor's banks, outside CPAs, and lawyers been located and identified? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. Has application been made to acquire copies of documents under subpoena in cases of criminal bankruptcy? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 8. Bust Out and Bleed Out | | | | |
| a. Have detailed ratio analyses been performed on accounts receivable and inventory? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. Have salaries, bonuses, and consulting fees been analyzed for payments to owners, family members, or other related parties? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Are travel and entertainment expenses within historic norms? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. How have the proceeds from any loans or financings been used? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Are all asset and liability transfers readily explicable? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Are all rent and lease payments for facilities, equipment, and vehicles needed directly in the operations of the debtor? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 9. Ponzi Schemes | | | | |
| a. Have cash receipts and disbursements been analyzed for unusual trends? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. Are there material misstatements in the financials? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Is net equity growing or shrinking? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Does an analysis of the income statement show an unexpectedly low level of business activity? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Is most cash flow generated from debt and new investment rather than from operations? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Is there an unusually high rate of turnover among lenders and investors? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. Is an unusually high level of cash disbursements being made to the owners and insiders? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

CHAPTER 13:

Detecting Procurement Fraud

| | | |
|--------|--|----|
| 13.1 | Overview of Procurement Fraud | 3 |
| 13.2 | Characteristics of the Procurement Process | 4 |
| 13.2.1 | Procurement Contracts Defined | 4 |
| 13.2.2 | Stages in the Procurement Process at Risk for Fraud | 6 |
| 13.2.3 | Records Related to Each Stage in the Procurement Process | 9 |
| 13.2.4 | Who Is Involved in the Procurement Process? | 11 |
| 13.3 | Types of Procurement Fraud..... | 12 |
| 13.3.1 | Procurement Fraud Schemes—by Perpetrator..... | 12 |
| 13.3.2 | Procurement Fraud Schemes—by Stage in the Procurement Process..... | 17 |
| 13.4 | Procurement Fraud Detection & Investigation..... | 18 |
| 13.4.1 | Detection & Investigation—A Disciplined Phased Approach..... | 19 |
| 13.4.2 | Procurement Fraud Investigations—A Team Approach..... | 19 |
| 13.4.3 | Identifying the Indicators of Procurement Fraud..... | 20 |
| 13.4.4 | Facilitating the Detection & Investigation of Procurement Fraud..... | 20 |
| 13.5 | Screening Procurement Contracts | 21 |
| 13.5.1 | Screening the Requirements Definition Stage..... | 22 |
| 13.5.2 | Screening the Bidding & Selection Stage | 23 |
| 13.5.3 | Screening the Contract Performance & Evaluation Stage | 30 |
| 13.5.4 | Screening the Billing & Payment Stages | 32 |
| 13.5.5 | Screening for Off-Book Frauds | 34 |
| 13.6 | Scrutinizing Suspect Procurement Contracts..... | 35 |
| 13.6.1 | Scrutinizing the Requirements Definition Stage | 36 |
| 13.6.2 | Scrutinizing the Bidding & Selection Stage..... | 37 |
| 13.6.3 | Scrutinizing the Contract Performance & Evaluation Stage | 39 |
| 13.6.4 | Scrutinizing the Billing & Payment Stages | 40 |
| 13.6.5 | Scrutinizing for Off-Book Frauds | 41 |

| | | |
|--------|---|----|
| 13.7 | In-Depth Examination of Suspect Procurement Contracts..... | 44 |
| 13.7.1 | In-Depth Examination of the Requirements Definition Stage | 45 |
| 13.7.2 | In-Depth Examination of the Bidding & Selection Stage..... | 46 |
| 13.7.3 | In-Depth Examination of the Contract Performance & Evaluation Stage | 46 |
| 13.7.4 | In-Depth Examination of the Billing & Payment Stages | 47 |
| 13.7.5 | In-Depth Examination for Off-Book Frauds | 48 |
| 13.8 | Analytical Techniques..... | 48 |
| 13.9 | Reporting Fraud In Procurement Contracts..... | 51 |
| 13.9.1 | Organization of Evidence | 52 |
| 13.9.2 | Working Paper File Sections | 52 |
| 13.9.3 | The Formal Report..... | 54 |
| 13.9.4 | Evidence | 54 |
| 13.9.5 | Practical Issues | 55 |
| 13.10 | Procurement Fraud Checklist | 56 |

CHAPTER 13:

Detecting Procurement Fraud

13.1 OVERVIEW OF PROCUREMENT FRAUD

Procurement is the process of contracting to acquire goods and services. *Procurement fraud* is the unlawful manipulation of this process to obtain an advantage. This form of fraud is especially common in government and industries, such as construction, where lucrative contracts are awarded, and management is reliant on a process that may be corrupt.

The first fact about procurement fraud that must be recognized is that it is one of the most difficult white-collar crimes to detect because much of it is “off-book,” that is, the fraud happens and there’s no specific entries to cover it up. Hence, understanding the nature of the procurement process is the first step in being able to detect, investigate, and ultimately prevent, procurement fraud.

The second fact is that all too many companies refuse to entertain the thought that their team of loyal employees could harbor fraudsters. When fraud occurs, management is taken by surprise; then, only after the event and after the insurance company has refused to pay the employee fidelity claim, decides to implement tighter controls. The sad truth is that much procurement fraud could be prevented by simple measures such as the separation and/or rotation of duties and surprise audits.

Unfortunately, as corporations downsize in a difficult economy or reconfigure responsibilities through technological changes, layers of managerial control are often removed and new opportunities open up for the imaginative fraudster. The remaining staff is usually overburdened with work and no longer attentive to the subtle indicators of irregularity in the company’s business practices or the behavior of their fellow workers that can be the first signs of fraud.

There are two key aspects to effective fraud prevention. The first is addressing the human side of fraud by taking steps to minimize the likelihood of hiring fraudsters, and establishing and maintaining an ethical workplace where honesty is respected. Employees must understand that fraud will not be tolerated; it can cost jobs, lower profits, eliminate bonuses, and even close businesses. Fair treatment and competitive compensation also play a role in prevention.

The second key aspect to effective fraud prevention involves addressing the environmental factors related to procurement fraud. This includes the development of an internal control system that can either prevent or detect anomalies. Regular review of such controls would include ensuring that the different kinds of signing authorities are not abused. Each override should be investigated to make sure it was justified by the circumstances and not part of a scam. Surprise audits are an essential element of internal control and should be

conducted by persons unconnected to the department under review. Everyone, including senior management, must be subject to surprise audits.

But human and environmental control systems cannot be established in a vacuum. To be effective in preventing and detecting procurement fraud, management must be knowledgeable about:

- The characteristics of the procurement process;
- The stages in the procurement process at risk for fraud; and
- The fraud risk indicators related to each stage in the procurement process.

With knowledge about each of these areas, then and only then, can management be effective in designing a suitable procurement fraud strategy to prevent, detect and/or investigate procurement fraud.

13.2 CHARACTERISTICS OF THE PROCUREMENT PROCESS

To be effective in dealing with procurement fraud, both in designing tests to detect it and in designing controls to prevent it, one needs to first consider the types of goods or services that can be purchased and the types of contracts related to such purchases, the stages of the procurement process and the types of activities that are meant to occur at each stage, the records related to each stage in the procurement process, and who is involved in the procurement process.

13.2.1 Procurement Contracts Defined

The purchasing process within an organization takes many forms—ranging from formal procurement contracts, to informal arrangements based on oral agreements to supply goods or services. For the purpose of this *Handbook*, although much of the discussion is directly applicable to the formal procurement contract process, the concepts discussed are equally applicable to informal arrangements.

To gain a better understanding of the vulnerabilities in the procurement process and the type of information that should be available relative to any particular procurement transaction, it is useful to study different types of procurement contracts, which can be classified in three broad ways:

1. Types of goods or services
2. Pricing method
3. Method of award, that is, competitive or non-competitive (sole-sourced)

The variations in each of these procurement processes impact not only the nature of the records that should exist for each procurement transaction, but also the motivations and weaknesses that should be tested when conducting the screening phase of a procurement fraud investigation.

Types of Goods or Services

1. *Construction Contract.* A construction contract is a contract entered into for construction, repair, renovation, or the restoration of any work.

2. *Goods Contract.* A goods contract is an agreement for the purchase of assets, inventory, commodities, equipment, goods, materials, or supplies.
3. *Service Contract.* A service contract is a contract for the provision of services by persons other than employees. There are several different types of service contracts:
 - a. *Professional Services Contract.* A contract for services provided by individuals with significant training, qualifications and expertise in a professional, scientific, technical, or managerial field (for example, legal services, engineering services, accounting services).
 - b. *Consulting Services Contract.* A contract for the provision of advice (e.g. management consulting, computer consulting).
 - c. *Nonconsulting Services Contract.* A contract for the provision of services other than the provision of advice or consulting. (for example, travel, entertainment, advertising placement, cleaning services, waste removal).
4. *Lease Contract.* An agreement whereby a company acquires a leasehold interest in real property, including a tenancy agreement or a license in respect of real property.

Method of Pricing

1. *Fixed Fee, Firm Fee or Lump Sum Contract.* A fixed fee, firm fee or lump sum contract specifies the total payable based on a fixed lump sum. Both parties agree on the price before the contract is awarded. Deviations are not allowed regardless of the volume of materials/labor used in the contracting process.
2. *Cost Per Unit.* A cost per unit contract specifies the total payable by multiplying identical units of work or items delivered by a fixed unit price.
3. *Cost Plus.* A cost-plus contract has a payment arrangement whereby the contractor pays actual costs incurred plus either an agreed fee or a percentage of cost. A variation on this type of contract would be a cost-plus contract with a guaranteed maximum.
4. *Time & Material.* A time and material contract varies based on the extent of materials and labor used to complete the contract.

Method of Award: Competitive Versus Sole-Sourced Contracts

Competitive Contract. Competitive contracts are generally awarded after at least two valid bids have been received based on the following criteria:

- *Construction.* Bids at firm prices, lowest accepted
- *Goods.* Lowest accepted
- *Consulting services.* Lowest or offering the best value accepted
- *Professional services.* Lowest or offering the best value accepted
- *Nonconsulting services.* Lowest accepted
- *Lease.* Lowest or offering the best value accepted

Sole-Sourced Contract. Sole-sourced contracts are a type of non-competitive contract for which bids have not been solicited or, if they have been solicited, the conditions of a competitive contract were not met. Such contracts are generally awarded for reasons other than price.

13.2.2 Stages in the Procurement Process at Risk for Fraud

The procurement process has a few key stages. The words used to describe the various stages in the process may differ, but the activities performed do not.

Each stage of the procurement process has different types of risks. In order to understand and minimize such risks, it is useful to consider the different stages separately.

For the purpose of this *Handbook*, the procurement contracting process is divided into the following five stages (see Table 13.1) for both competitive and non-competitive contracts:

1. Requirements definition
2. Bidding and selection
3. Contract performance and evaluation
4. Billing
5. Payment

TABLE 13.1 COMPETITIVE & NON-COMPETITIVE (SOLE-SOURCED) CONTRACT STAGES

| | Competitive Contracts | Non-competitive (Sole-Sourced) Contracts |
|---|-------------------------------------|---|
| 1 | Requirements Definition | Requirements Definition |
| 2 | Bidding and Selection | Selection |
| 3 | Contract Performance and Evaluation | Contract Performance and Evaluation |
| 4 | Billing | Billing |
| 5 | Payment | Payment |

Requirements Definition Stage

The requirements definition stage is the first stage in the procurement process; it is also the first step in the decision-making process related to whether to purchase the goods or services. This is when the job to be done is defined and decisions are made regarding whether to procure the goods or services required.

If a competitive contract is selected as the method of procurement, the specifications must be formulated in a way that will attract multiple bidders. The requirements definition stage therefore involves planning, budgeting, and decision making to avoid jeopardizing the integrity of the bidding process. Otherwise, the company may enter into an unnecessary contract or competition may be compromised by setting specifications that can be met by only one potential vendor.

The following are the components of the requirements definition stage:

- Identify the need.
- Specify the requirements as to time, cost and/or performance criteria.
- Assess alternatives to meet the need (including contracting).
- Prepare bid information if a competitive contract is the selected means to meet the requirement.

- Plan the procurement process.
- Establish the award criteria.

Key Control Features

- The need should be defined within the mandated objectives of the department.
- The standards or other measurement criteria should be articulated so that it can be used during or after the completion of the contract to establish that the contract has been performed to an acceptable standard.
- An alternatives assessment should be completed regarding availability, time and cost estimates.
- Research should be conducted regarding the most appropriate procurement method (for example, identifying whether the contract should be awarded based on a competitive process or a non-competitive/sole-sourced process).
- A procurement schedule and management, production, and logistical plans should be developed for later comparison purposes.

Bidding & Selection Stage

During the bidding and selection stage of the procurement process, purchasing or materials management staff identify sources of supply; develop and issue a request for proposals or quotations (known as an RFP or RFQ); analyze responding proposals, quotations or bids; communicate with likely candidates as necessary; select the final contractor; define the terms of the contract; and otherwise ensure the proper authorization for acquisition of the contractor's services. This stage of the procurement process is the second major decision of the procurement process.

Once again, if this stage is not executed properly, the integrity of the entire procurement process is in jeopardy.

The following are the components of the bidding and selection stage:

- Bid solicitation and evaluation
- Contract approval and award
- Contract documentation

For non-competitive or sole-sourced contracts, the bidding and selection stage doesn't involve a bidding process, but there is still a selection process, where justifications are generally provided in support of a particular contractor.

Key Control Features

- Where it is cost effective to do so, all qualified firms should have an opportunity to compete for procurement contracts. Firms will be considered to be qualified that:
 - Have the technical, financial, and managerial competence to perform the contract.
 - Meet criteria established by company policies and objectives. Contracts should be approved according to pre-approved levels of authority.
- The draft procurement contract should be compared to the original requirements definition.
- Legal counsel should be involved in the drafting process.

Contract Performance & Evaluation Stage

During this stage of the procurement process, the contracted services/goods are provided/supplied, and evaluations are performed to compare the actual completion of the contract to the time and performance criteria specified in the contract as defined in the requirements definition stage.

This is the third major step in the procurement process, that is, the operational step in the process.

Management and support staff with primary responsibility for contract evaluation would perform the technical evaluations to ensure that the contracted goods/services were delivered as agreed in the contract. Such staff would also provide input into the billing and payment stage of the contract—to ensure that the progress reports on the financial status of the contract match the technical reports. They may also resolve contract disputes and ensure that any contract amendments receive as much scrutiny as the original contract.

Each contract should be evaluated to ensure the supplier met the terms of the contract and the product fulfilled the program requirements as specified. Line managers play a key role in monitoring service contracts. They are responsible for the day-to-day management of the contract and certification that services have been received.

The following are the components of the contract performance and evaluation stage:

- Contract monitoring
- Contractor and technical evaluation
- Progress reports review
- Amendments and change orders review

Key Control Features

- The contractor should provide technical progress reports.
- Contractor performance should be evaluated regularly to ensure that the contract addressed the identified requirements.
- Bid protests/contract disputes should be addressed and resolved with minimal delay.
- Contracts should not be amended unless in the best interests of the company.

Billing Stage

During the billing stage of the procurement process, the contractor submits invoices or progress payments that are then evaluated to ensure that contract costs are appropriate—as agreed in the original contract or contract amendments, and the cost is established as a liability of the company to the contractor.

This is the fourth stage in the procurement process, which occurs after the project is completed, or it could occur after a portion of the project is completed. During this stage, the liability for the goods or services would typically be established based on the invoice submitted.

The following are the components of the billing stage:

- Invoices received from contractor
- Financial controls related to the amounts billed

- Costs established as a liability
- Dispute resolution
- Amendments and change orders review

Key Control Features

- Contracts should be administered in accordance with company financial policies, procedures, and accepted financial control practices.
- The contractor should provide financial/technical progress reports.
- Bid protests/contract disputes should be addressed and resolved with minimal delay.

Payment Stage

During the payment stage of the procurement process, the company makes payment(s) to the contractor based on the invoices/progress payment requests submitted.

This is the fifth and final stage of the procurement process. During this stage, the liability for the goods or services is discharged as the invoice submitted in the preceding stage is paid.

The following are the components of the billing stage:

- Payments issued to the contractor
- Financial controls

Key Control Features

- Payments should be made in accordance with company financial policies, procedures, and accepted financial control practices.

13.2.3 Records Related to Each Stage in the Procurement Process

One of the most important aspects to realize when considering how to prevent, detect or investigate procurement fraud, is that only the last two stages of the procurement process, namely the billing stage and the payment stage, involve accounting records.

The requirements definition stage, bidding and selection stage, and contract performance and evaluation stage each have certain types of records that would typically be produced, but such records are ordinarily maintained by a company's purchasing department, not the accounting department, and are therefore not the types of records that most accountants examine when assessing the costs incurred by a company.

Accordingly, success when dealing with procurement fraud involves examining more than just accounting records, as the other business records are more likely the records that will be useful in proving procurement fraud.

The following are the types of records that are typically produced at each stage in the procurement process:

Requirements Definition Stage

- Needs assessment documentation (or needs justification documentation)
- Requirements "specs"—including performance criteria, quantities required, due dates, type of goods/services to be provided
- Internal communications approving the need for the purchase/service

Bidding & Selection Stage

- Potential contactor research
- List of contractors invited to submit a proposal
- Request for proposal, quotation, or any other bid solicitation records (these are essentially similar documents; certain organizations have different names for them)
- Tender packages including proposals/quotes/bids submitted by potential contractors
- Written communications issued to the potential contractors, either before or after the deadline for bid submission
- Notes from oral communications with potential contractors, either before or after the deadline for bid submission
- Analysis of tender package records
- Contract acceptance records
- Price list(s) from prior contracts, competitors in order to evaluate the pricing of the contract
- Contract documentation, including drafts of the contract, as well as the final approved contract
- Notes from communications with counsel regarding the legal issues arising in the proposed contract

Contract Performance & Evaluation Stage

- Progress reports from the contractor
- Internal progress reports evaluating the stage of completion of the contract
- Written correspondence, or notes from oral communications, with the contractor
- Deficiencies list(s)
- Evaluation reports on the supplier's performance under the contract
- Technical documentation required to evaluate the goods/services provided
- Change orders and communications related to the need for the change order
- Amendments to the contract

Billing Stage

- Invoices or progress payments submitted by the contractor
- Documentation submitted by the contractor in support of the invoices submitted (related to proof of performance, or to establish the quantity delivered, etc.)
- Written correspondence, or notes from oral communications, related to approval of the invoices/progress payments
- Entries in the purchases journal and/or general ledger related to establishing the liability and expense for the costs incurred

Payment Stage

- Check(s) or transfer(s) used to pay the invoice(s) of the contractor
- Entries to record the payment and relieve the general ledger of the liability for the costs incurred

In addition to operational and accounting records, procurement processes are often well documented by the internal audit department of an organization. The internal audit process would typically generate:

- Overview fact sheets
- Internal control evaluation questionnaires for the purchases, payables, and payments system
- An audit program
- Audit data
- An audit report
- A responding management report

13.2.4 Who Is Involved in the Procurement Process?

The procurement process of an organization typically involves a team of people both within an organization and external to an organization.

The people involved in the procurement process that are inside an organization include purchasing agents or buyers, the users of the goods or services, management, and accounts payable or other accounting personnel.

The people involved in the procurement process that are external to an organization include suppliers and their sales personnel, and accounts receivable or other accounting personnel at the supplier organization.

Each of these people have an important role to fulfill relative to the procurement process of an organization, and are therefore each in a position to be able to commit procurement fraud.

Procurement fraud can be committed by:

1. Internal employees or management acting alone or in collusion with other employees
2. Employees acting in collusion with vendors/contractors
3. Vendors acting against the company
4. Vendors acting in collusion as a group

Internal Employee/Management Fraud

Procurement fraud involving employees or management, either acting alone or in collusion with other employees/management, often involves undisclosed conflicts of interest, false or inflated expense reports, or schemes involving diverted payments.

Many employee/management frauds are “on-book” frauds, where the fraud itself, and the coverup thereof, can typically be traced through the accounting records of the company.

Collusion Between Employees and Vendors

Procurement fraud involving collusion between employees and vendors often involves off-book bribes, secret commissions or kickbacks of cash, gifts, free trips, dinners at fine restaurants, and other inducements to give favorable treatment on an upcoming bid, to approve transactions with vendors that should not otherwise be approved, or simply to retain existing business. Such activity is generally off-book, and is much harder to detect

because of the hidden nature of the transactions involved. It is also much harder to detect because of the enhanced ability of the perpetrators to cover-up the situation.

Essentially this form of collusion involves “cozy business relationships” where decision-makers are enticed to “look the other way”. A pair of courtside NBA tickets now and again or a bottle of single-malt Scotch at Christmas might not be a problem, but a two-week trip to the Bahamas for the director of purchasing and his wife is inappropriate.

Vendor Fraud Against the Company

Vendor fraud often involves false billing or substitution of goods or services inferior to the contract specifications, and can be either on-book or off-book frauds. In other words, it may or may not be possible to prove the fraud using the books of the company that hired the vendor/contractor.

These types of fraud often occur in organizations where the procurement-related internal controls are weak, and an external party sees a weakness and then exploits it.

Collusion Among the Vendors Within an Industry or Bidding Group

Procurement fraud involving collusion among vendors often occurs when vendors communicate/scheme to engineer bids higher than market rates. This type of procurement fraud is typically known as an off-book fraud, and is very difficult to prove, because it is difficult to establish what the market rate actually is.

13.3 TYPES OF PROCUREMENT FRAUD

There are numerous different types of procurement fraud schemes that can be perpetrated; the variations relate to who is involved in perpetrating the fraud, and the stage in the procurement process that is being compromised.

13.3.1 Procurement Fraud Schemes—by Perpetrator

Internal Employee/Management Fraud:

Conflict of Interest. A conflict of interest involving internal employees/management occurs when a procurement contract is awarded to a firm in which such employees or their families have an undisclosed financial interest. Such conflicts become fraudulent when they are detrimental to the interests of the company that awarded the contract. For example, there would be a conflict of interest in contracts awarded to a company that is owned by the employee. This conflict of interest would be fraudulent if the invoices submitted were inflated, and the employee was involved in the invoice approval process.

Payment Diversion. Payment diversions involve employees or management who:

- Cash the check or redirect where the payment that was intended for submission to the contractor will be made, and
- Adjust the accounting records to either engage in a lapping scheme, or to make the accounting records appear as if the payment had, in fact, been made.

For example, a payment diversion fraud could occur if the employee changes the payee on a check, and then changes the accounting records to make it appear as if this particular payee was paid.

Phantom Contractor. Phantom contractors are fictional companies created by employees/management that were set up to enable internal personnel to submit an invoice(s) for payment. For example, corrupt employees create invoices similar to the actual invoices submitted by legitimate contractors.

Purchases for Personal Use. An employee may purchase items for personal use or make excess purchases for personal use. For example, an employee has a family business whose stationery is printed as part of his employer's contract for printing stationery.

Collusion Between Employees and Vendors:

Bribery. Bribes are typically offered or paid to unduly influence a particular decision or outcome that would be favorable to the payer of the bribe. Bribes are similar to secret commissions and kickbacks, and bribes are an "off-book" transaction; the primary distinction is that a bribe is typically offered before influence has been improperly exercised, whereas secret commissions and kickbacks are generally paid after. For example, a building inspector receives plain envelopes filled with cash as a bribe to entice him to approve substandard construction work.

Conflict of Interest. A conflict of interest involving collusion between employees and vendors occurs when a contract is awarded to a firm employing company employees or their families, or to a firm in which such the family members of such employees have an undisclosed financial interest. Such conflicts become fraudulent when they are detrimental to the interests of the company that awarded the contract. For example, there would be a conflict of interest in contracts awarded to the brother-in-law of a company employee. This conflict of interest would be fraudulent if the invoices submitted were inflated, but were approved by the company employee nonetheless.

Information Theft or Bid Fixing. Information theft or bid fixing occurs when a company employee releases unauthorized information to third parties that would provide them with an unfair advantage in a competitive procurement process. For example, a contractor receives information concerning the amounts bid by competing contractors before submitting his or her bid. The favored contractor then submits a lower bid.

Small Purchase Order Fraud or Split Purchases. Small purchase order fraud, or split purchases fraud usually occurs in order to circumvent the requirement for a formal competitive procurement process. In such circumstances, purchases are split into two or more segments so that the cost of each segment is lower than the authorized procurement limit. For example, five purchase orders are issued, each below the limit instead of one large order assessed as a single contract.

Secret Commissions and Kickbacks. Secret commissions and kickbacks are typically paid by vendors to company employees in the form of money or gifts to reward the employee for providing business or favorable treatment. Secret commissions are typically paid as a percentage of the transaction the secret commission related to, whereas the amount of a kickback is typically not directly linked to the amount of the underlying transaction or fraud. Secret commissions and kickbacks are primarily "off-book" frauds in which the amount of the secret commission or kickback is disguised or otherwise hidden in the books as part of the transaction to which they are related. For example, a building inspector receives plain envelopes filled with cash after the approval of substandard construction work. The funds for this payment are accounted for as a materials cost.

Unnecessary Purchases. Procurement fraud involving unnecessary purchases occurs when bids are solicited for unnecessary goods or services or for the duplication of other contracts. For example, a contract is awarded for a consulting group to study the impact of a fire on the water supply after such a study had already been included as part of a larger review prepared by other consultants.

Collusion Between Employees and Vendors Case Study

An anonymous letter and supporting documents arrived on the desk of the president of a small gas producer alleging that the plant manager was colluding with a local contractor in contracts for pipeline repair and maintenance. The letter claimed the local contractor had been awarded a disproportionate number of contracts and that more work and supplies were being billed for than were ever performed or delivered. Police assisted by forensic investigators discovered that the contractor owned five additional companies and that two regularly submitted competitive bids for work at the gas producer. Records showed that the plant manager and other senior staff had circumvented the internal controls governing the procurement process and had contracted for more materials from the local contractor than had been needed to repair retaining walls on a river bank and rebury pipeline exposed after severe flooding. The plant manager also accepted a time card two weeks late that billed \$50,000 for 2,500 hundred hours at \$20 per hour. By using the right-to-audit clause in the contract, the forensic investigators found that the contractor had only paid its employees \$24,000 for 1,200 hours work. A portion of the difference had been kicked back to the plant manager for influencing the selection of the contractor. A review of the contracts showed them to be poorly worded, imprecise and open to abuse; other records were found to be inaccurate. A lifestyle review of the plant manager showed him and his wife to be living far beyond the means provided by his salary.

Vendor Fraud:

Change Order Abuse. Change orders or changes requiring additional funds are typical in the procurement process, but are abusive if they are issued in order to compensate for the initial low bid. For example, many subsequent stages of work may be required to fulfill the original contract specifications.

Co-mingling of Contracts. Co-mingling occurs if a contractor bills for the same work in more than one component of the contract. For example, the same demolition costs are billed four times in relation to separate contracts for the construction of foundations, walls, ceilings, and floors.

Duplicate Payments. Duplicate payment fraud occurs when a contractor intentionally submits more than one original invoice for the same goods or services, and the company pays both invoices without realizing that such invoices were duplicated. For example, a second invoice is sent by a contractor without identifying it as a second copy.

False Invoices. False invoice fraud occurs when a contractor submits an invoice for goods or services that were not provided. For example, an invoice is issued for goods delivered to a different fixed-price contract job and charged on a cost-plus contract.

False Representations. The contractor misrepresents the quality of the products to be supplied or his ability to perform contracted services. For example, a contractor claims he has equipment to dig a hole with a 90-degree turn, but charges for the labor required to dig the turn manually.

Front-End Loading. Front-end loading (or advance payment fraud) typically occurs in a percentage of completion contract when the contractor inflates the costs of the initial stage of work in order to receive inflated cash flows when the percentage of completion billing method is applied. The costs of later work are understated in the expectation that change orders will be approved to make up for the shortfall. For example, details relating to labor usage are embellished.

Inflated Pricing. Inflated pricing fraud occurs if the contractor submits invoices at prices higher than agreed in the contract. For example, an invoice issued for 1,000 units at \$105 each instead of \$102 each. Cost mischarging occurs when the contractor charges for costs that are not allowable, unreasonable, or cannot be allocated to the contract. For example, labor charges are allocated from a fixed price contract with no remaining budget to another contract on a cost-plus basis.

Product Substitution. Product substitution refers to supplying goods or services that do not conform to the procurement contract specifications. For example, a lower grade of lumber and cement is used in the construction of a building than was specified in the contract.

Progress Payment Fraud. Progress payment fraud occurs if the contractor requests progress payments based on falsified information regarding the progress of the project. For example, the invoice details supporting the progress payment include charges for payroll costs not incurred because of layoffs or the reassignment of personnel.

Vendor Fraud Case Study

A large manufacturing company decided to build a new factory. Contracts were let through the usual bidding process and construction began. After substantial cost overruns, a forensic investigation was initiated. Investigators found that about four months into the project, requests began to appear for changes to the original contracts, usually involving supplemental charges. Questions began to arise about the quality of some materials, especially about the volume of washroom tiles purchased and the amount of breakage. The expense accounts of the procurement manager were examined and numerous curious entries were found. For example, expenses were submitted for meals and rooms at restaurants and hotels in New York and New Orleans for conventions that had not taken place and without any accompanying expenses for airline tickets or other transportation. The names that appeared on the receipts were known to be associated with the successful bidders on the factory construction contract.

The investigation revealed that the vendors had flown the procurement manager and his wife as well as other people in the procurement department and their spouses to vacation destinations. Relatives of the manager had been employed by the vendors and the vendors had done renovations on the manager's home free of charge. For this, the manager

approved changes in the contracts, approved the use of materials such as the tiles that were inferior to the specifications and accepted invoices sometimes as much as 40 percent above the actual cost of the materials and labor. At the end of the investigation, the manager and others in the procurement department were dismissed and charged with fraud.

Collusion Among the Vendors:

Bid Rigging, Collusive Bidding, or Price Fixing. Bid rigging, collusive bidding, or price fixing are similar forms of fraud. In each, a group of two or more prospective contractors have a private arrangement to coordinate their bidding to eliminate or limit competition. In bid rigging, the “winning bidder” is predetermined based on an agreement between the vendors. In collusive bidding, the bidders share information with each other prior to issuing their final bid and collaborate on the amount of each bid. In price fixing, the ultimate price is agreed among a group of vendors.

The purpose of each of these types of arrangements is to raise the ultimate price above what it would otherwise be, thereby effectively destroying the competitive process. For example, contractors agree in private that one of them will be the low bidder. Each then submits an inflated bid that includes a higher level of profit than would otherwise be achieved if the contractors were legitimately competing against one another.

In some circles, this type of “collusion” or “cooperation” among a group of vendors is considered to be market practice. Hence, it is important to note the factors that would cause such market cooperation to be considered fraudulent:

- Collusion among vendors
- Dishonest elimination of competition
- Deprivation to company purchasing goods/services—i.e. higher prices

The last element is difficult to prove, however, because it is difficult to establish what the market would have been if the vendor group had not collaborated on the price.

Collusion Among the Vendors Case Study

During the European construction boom of the late 1980s, two wealthy businessmen saw an opportunity to make money in the market for cement powder. The key to beating the price of local manufacturers was to purchase powder from low-cost producers in Greece, Turkey and Romania and import it into European ports on leased self-unloading ships. When the ships began arriving at French ports, the dockworkers refused to unload them. Unable to discharge their cargo, they anchored offshore for months while the owners argued with the local harbor authorities and the unions. After the two men realized they were not going to get permission to dock and unload, they decided to sell the cement powder in Africa at a loss rather than have the wet sea air harden it in the holds of the anchored ships. The whole venture cost them about US\$300 million by the time the ships' leases had expired.

A few years later the two businessmen discovered it was not the French unions that had caused their project to fail. An extensive investigation by governments and law enforcement agencies across Europe revealed that some of Europe's largest cement makers had been engaged for more than a decade in a conspiracy to fix the market for cement and ready-mix concrete. Construction companies all across Europe had been paying substantially more than they should have because of the collusion among the cement producers. The Competition Directorate of the European Union fined the members of the conspiracy US\$300 million as punishment.

13.3.2 Procurement Fraud Schemes—by Stage in the Procurement Process

Table 13.2 summarizes the stages of the procurement process that are being compromised for each of the different types of procurement fraud described in the previous section of this chapter.

TABLE 13.2 TYPES OF PROCUREMENT FRAUD BY STAGE

| Types of Procurement Fraud | Requirements Definition | Bidding & Selection | Contract Performance | | |
|---|-------------------------|---------------------|----------------------|---------|---|
| | | | Billing | Payment | |
| INTERNAL EMPLOYEES & MANAGEMENT: | | | | | |
| Conflict of Interest | x | √ | o | o | o |
| Payment Diversion | o | x | o | o | √ |
| Phantom Contractor | x | √ | o | o | o |
| Purchases for Personal Use | x | √ | o | o | o |
| COLLUSION BETWEEN EMPLOYEES & VENDORS: | | | | | |
| Bribery | x | √ | o | o | o |
| Conflict of Interest | x | √ | x | o | o |
| Information Theft or Bid Fixing | x | √ | o | o | o |
| Small Purchase Order | x | √ | o | o | o |
| Fraud or Split Purchases | | | | | |
| Secret Commissions and Kickbacks | o | √ | x | o | x |
| Unnecessary Purchases | √ | x | o | o | o |
| VENDOR FRAUD: | | | | | |
| Change Order Abuse | o | x | x | √ | o |
| Co-mingling of Contracts | o | x | x | √ | o |
| Duplicate Payments | o | x | o | x | √ |
| False Invoices | o | x | o | √ | o |
| False Representations | o | √ | x | o | o |
| Front-End Loading | o | x | o | √ | o |
| Inflated Pricing | o | x | o | √ | o |
| Product Substitution | o | x | √ | o | o |
| Progress Payment Fraud | o | x | o | √ | o |
| COLLUSION AMONG VENDORS: | | | | | |
| Bid Rigging, Collusive Bidding or Price Fixing | x | √ | o | o | o |
| <i>Legend:</i> | | | | | |
| √ Occurs most often at this stage | | | | | |
| x Sometimes occurs at this stage | | | | | |
| o Rarely occurs at this stage | | | | | |

13.4 PROCUREMENT FRAUD DETECTION & INVESTIGATION

Procurement fraud investigations can be difficult and costly. Accordingly, procurement fraud investigations should be done in a disciplined manner, where the extent of work performed is commensurate with the risks involved, and where the cost of further investigation is justified by the results of the investigation to date.

This is best accomplished using a phased approach where the first phase involves performing limited testing to find the areas of concern or indicators/red flags of fraud; the second phase involves performing additional analyses to confirm/refute the red flags or indicators identified in the first phase; and the third phase involves determining the full

extent of the fraud and proving the allegations so that the suspect can be confronted—either informally or formally via criminal or civil court proceedings.

13.4.1 Detection & Investigation—A Disciplined Phased Approach

For the purposes of this text, we have divided the fraud detection and investigation process into the following three phases:

1. *Screening*: The first phase is the detection phase, which involves limited testing and/or interviews to identify fraud risk indicators or “red flags” indicative of possible areas of concern, and to identify issues that should be further scrutinized for possible fraud.
2. *Scrutinizing*: The second phase is the allegation testing phase, which involves performing certain analyses, comparisons, interviews or other investigative procedures to confirm or refute the allegations identified as red flags in the screening phase, and identify issues that should be subjected to a rigorous in-depth examination of all the available evidence.
3. *In-Depth Examination*: The third phase is the investigation phase, which involves an in-depth investigation including detailed document analysis, analytical techniques and interviews to determine the full extent of the fraud as alleged in the screening and scrutinizing phases, and to do so in a way that can withstand cross-examination via a formal process (beyond a reasonable doubt for criminal proceedings, and at a high enough level to be convincing for other civil proceedings or an insurance claim).

What is the primary difference between the procedures performed in the screening phase, the scrutinizing phase, and the in-depth and examination phase? Each of these phases involves investigative procedures and interviews, and the distinction between each phase can sometimes get a little blurred. This occurs because the process of conducting a procurement fraud investigation is an art, not a science. In addition, investigations are conducted by human beings who can easily “get caught up in the chase” of pursuing a fraud investigation, thereby losing the discipline of a cost-effective phased approach. To simplify the distinction between the three phases, the differences between the three phases are outlined in Table 13.3:

TABLE 13.3 PHASED INVESTIGATIONS

| Phase | Primary Objective | Nature of Testing | Nature of Interviews |
|----------------------|---------------------------------------|--|---------------------------------------|
| Screening | Establish/collect evidence | Determine areas of possible concern | Systems/procedural interviews |
| Scrutinizing | Test the allegations | Establish whether fraud has occurred/who involved/how done | Fact-finding interviews re: who & how |
| In-Depth Examination | Obtain final proof for court purposes | Detailed testing/beyond a reasonable doubt | Accusatory interviews |

13.4.2 Procurement Fraud Investigations—A Team Approach

The process of detecting and investigating procurement fraud is enhanced by using people with several different skills—including people with investigative skills, legal skills, accounting skills, and business skills, and the investigation would be further enhanced by

using client staff—possibly from internal audit—who can help smooth the way in terms of gaining access to information. People with a purchasing background would also be useful for the team, as such people typically have good insight into how the purchasing process is meant to work, and are therefore alert to how the procurement system could be compromised.

13.4.3 Identifying the Indicators of Procurement Fraud

No indicator alone confirms the existence of procurement fraud. Rather, the presence of several indicators should raise the suspicion of improper activity. The issue then, is how first to detect such indicators, and what is an indicator of fraud? What does an indicator of fraud look like?

The process of looking for red flags involves looking for oddities that “don’t smell right.”

Red flags are found by applying intuition and judgment that come from experience and knowledge of inappropriate activity. Red flags are generally something different than expected in time, place, personality or amount.

In order to find the red flags of fraud, the following questions are typically asked:

1. Are there any oddities relating to:
 - Time (of day, week, month, year, or season)
 - Frequency (too many, too few)
 - Places (too near, too far, or too far out)
 - Amount (too high, too low, too inconsistent, too alike, too different)
 - Parties or personalities (related parties, oddball characters, strange relationships, estranged relationships, unusual functions performed)
2. Where are the weakest links in the chain? Or how could the systems of internal control be compromised?
3. What deviations are possible, how are they handled, and who can authorize such transactions?
4. What control features can be bypassed/overridden by higher authorities, and how?

These questions, combined with knowledge of the stages of the procurement process, enable a comprehensive examination of the red flags of procurement fraud. This is the process that has been followed in the remaining sections of this chapter and the red flags identified are presented in tabular form throughout the remainder of this chapter.

13.4.4 Facilitating the Detection & Investigation of Procurement Fraud

Checklists are often helpful in the process of identifying and investigating red flags, because they typically provide a broader range than might otherwise be considered, and therefore heighten awareness as to:

- Whether there are any red flags.
- The type of fraud that might have occurred.

- Other red flags that may have occurred, which could further substantiate that fraud has occurred.

But checklists should be used with caution as they could stifle creativity and could ultimately limit the awareness of the user of such checklists.

The material in the remainder of this chapter has been organized in a sequence that could be followed during an actual investigation, but the steps to be undertaken would depend on the nature of the allegations identified. Red flag indicators are provided in tabular form and are further explained after each table. The types of fraud likely indicated by the red flags are also identified—so that further scrutinizing can be performed to further confirm/refute whether the red flags are, in fact, indicative of fraud.

13.5 SCREENING PROCUREMENT CONTRACTS

| <i>Phase</i> | <i>Primary Objective</i> | <i>Nature of Testing</i> | <i>Nature of Interviews</i> |
|--------------|----------------------------|-------------------------------------|-------------------------------|
| Screening | Establish/collect evidence | Determine areas of possible concern | Systems/procedural interviews |

As discussed earlier in this chapter, screening is the “detection phase” of the procurement fraud detection and investigation process. This phase involves performing limited testing and/or interviews to identify “red flags” indicative of possible areas of concern, and to identify issues that should be further scrutinized for possible fraud. In this phase, evidence is collected to determine areas of possible concern, and information is gathered to identify systems/procedural weaknesses that would enable such concerns to exist.

Documentation Required

In screening procurement contracts for potential fraud and applying the red flag approach, the following documents would be useful to gather and review.

Contract Files. Gather and review contract files including:

- Plans and reports defining the requirement
- Request for proposal or any other bid solicitation records
- Tender packages
- Assessment of tender package records
- Contract acceptance records
- Final approved contract
- Progress reports
- Invoices charged against the contract
- Amendments to the contract
- Evaluation reports on the supplier’s performance under the contract

Internal Audit Working Papers. Gather and review internal audit working papers including:

- Overview fact sheets
- Internal control evaluation questionnaires for the purchases, payables, and payments system
- Audit program
- Audit data
- Audit report
- Management report

13.5.1 Screening the Requirements Definition Stage

The acquisition of goods and services usually begins only after the completion of a proper needs assessment. Although the lack of or an inadequate needs assessment does not in itself constitute fraud, it often provides an opportunity for fraudulent activity.

Fraudulent schemes predicated on a poor needs analysis usually involve the misuse of employee discretionary power to define requirements. The type of misuse varies according to the nature of the scheme. The contracted goods and services may deliberately exceed those required or, in extreme circumstances, may not be needed at all. An employee may even decide to dispose of goods that need not be replaced. The level of documentation in the files for any of these schemes could range from deliberately falsified figures or facts in an elaborate analysis to a very sketchy outline that leaves the employee with significant opportunity for fraudulent maneuvering.

For fraud to be established, dishonest intent must be demonstrated. Therefore, an employee could not be prosecuted for fraud for conducting an inadequate needs analysis since incompetence is not a criminal offense. If, on the other hand, the employee or a related party were to receive a benefit as a result of this “incompetence,” dishonest intention may be provable and fraud may be established.

Red Flags in the Requirements Definition Stage

The following red flags could be indicative of fraud involving the requirements definition stage of the procurement process:

1. *Excess Stock Acquired.* Unneeded stock is acquired from certain contractors or in excess of inventory requirements.
2. *Marketing Information in Files.* Department files include marketing information provided by the successful contractor prior to the issuance of the contract. The presence of such material may indicate the department is purchasing goods or services in response to aggressive marketing efforts by contractors and possible favors, secret commissions, or benefits, rather than to meet valid requirements. The file should show how the two parties first made contact.
3. *Narrow Requirements Definition.* The requirements definition is so narrow it eliminates certain suppliers or there is an unjustified or unreasonable eligibility constraint.
4. *Official Involvement.* A senior official exceeds his/her responsibilities by going beyond their job descriptions—for instance, by assisting in the preparation of the needs definition.

5. *Replacement Period Unreasonable.* The replacement cycle for goods is shorter than indicated by manufacturers' recommendations, departmental standards, or the level of utilization.
6. *Rushed Timing.* The time allocated to the requirements definition stage is unreasonably short in comparison to the size of the project. Rushed timing can indicate someone trying to circumvent the usual controls in the contracting process.
7. *"Surplus" Goods Replaced.* Goods originally sold as surplus are subsequently replaced.
8. *Thin File Syndrome.* Needs assessments are not adequately or accurately documented. The needs assessment may be nonexistent, or may describe the desired product without justifying its acquisition or is vague about its performance standards.

The following table (Table 13.4) shows the types of fraud most commonly committed in the requirements definition stage of the procurement process, and the types of red flags that are indicative of such fraud.

TABLE 13.4 RED FLAGS: SCREENING THE REQUIREMENTS DEFINITION STAGE

| Red Flags | TYPE OF FRAUD THAT MAY BE INDICATED | | |
|------------------------------------|-------------------------------------|--------------------------------|-----------------------|
| | Conflict of Interest | Secret Commissions & Kickbacks | Unnecessary Purchases |
| 1. Excessive Stock Acquired | √ | √ | √ |
| 2. Marketing Information in Files | | √ | √ |
| 3. Narrow Requirements Definition | √ | √ | |
| 4. Official Involvement | √ | √ | |
| 5. Replacement Period Unreasonable | √ | √ | √ |
| 6. Rushed Timing | √ | √ | √ |
| 7. Surplus Goods Replaced | √ | √ | √ |
| 8. Thin File Syndrome | √ | √ | √ |

13.5.2 Screening the Bidding & Selection Stage

The request for a proposal (RFP) provides contractors with an opportunity to submit bids for the provision of goods or services that meet the terms of the requirements definition and bid specifications. This process is intended to maximize the use of competition to ensure the company obtains the right goods and services at the best possible price.

The documents in a RFP provide prospective bidders with details on the eligibility of contractors, the specific work to be performed, and the type of goods to be delivered. They provide bidders with a complete guide to the preparation and submission of bids. Every interested bidder should be provided with identical tender documents.

After the proposals have been received and the deadline has passed, the award of the contract is based on many factors including price, responsiveness, and responsibility.

Carelessly written bid specifications and contracts make it easier for a contractor to claim more money if the company later defines what it really wants. Vague specifications can suggest collusion between a company employee and the contractor. Similarly, an increase in price immediately after the award of the contract could suggest a possible problem.

For the sake of clarity and completeness, the red flags of fraud for competitive contracts are discussed separately from the red flags of fraud for sole-sourced or non-competitive contracts.

Red Flags in the Bidding & Selection Stage of Competitive Contracts

The following are the types of fraud that typically relate to the bidding and selection stage of competitive contracts:

- Bid rigging, collusive bidding or price fixing
- Bribery
- Conflict of interest
- False representations
- Information theft or bid fixing
- Phantom contractor
- Secret commissions and kickbacks

The following red flags could be indicative of such fraud:

1. *Award Patterns.* Certain contractors are consistently successful in one particular territory, or the same bidder is usually successful when contracting with one particular department but not with others.
2. *Bidding Patterns.*
 - Certain contractors always bid against each other or, conversely, certain contractors never bid against one another.
 - Bid prices drop when a new or infrequent bidder submits a bid.
 - A certain contractor appears to be bidding substantially higher on some bids than on others with no logical cost difference to account for the increase.
 - Certain companies within a group of contractors appear to submit the lowest bid. (This might indicate a market division by class of customer.)
3. *Bid Fixing Correspondence.*
 - The file contains letters, notes, or memos by employees, former employees, or competitors that refers to the existence of agreements to fix bids and prices or otherwise restrain trade.
 - A contractor states that he “does not sell in a particular area” or that “only a particular firm sells in that area.”
 - A bidder or contractor states that it is not their turn to receive a contract.
4. *Bid Specifications Unclear or Vague.* Bid specifications are unclear or vague with respect to the standards of performance, timing, quantity or quality. Unclear bid specifications create potential fraud opportunities because they:

- Open the door to the exercise of discretion by company employees in selecting a suitable contractor.
 - Provide an opportunity for the contractor to recoup otherwise unrecompensable losses by falsely attributing them to the unclear bid specifications.
5. *Bid Specifications Unrelated to Requirements Definition.* Bid specifications are not consistent with the needs determination or requirements definition.
 6. *Changes to Specifications After Award but Prior to Contract Signing.* New contract specifications that create the opportunity for overcharging are developed in consultation with the successful bidder and incorporated into the final contract.
 7. *Company/Alumni Involvement with Contractor.* The involvement of former employees who own the company awarded the contract, or who commence working for the successful bidder subsequent to the contract award date.
 8. *Company Personnel Related to Contractor.* Relationships involving a company manager or employee who has close professional or personal ties with a particular bidder/contractor or its officials, or is related, either by birth or by marriage, to a particular bidder/contractor or its officials.
 9. *Comparison of Bid Package Details.*
 - Bidders that ship their product a short distance bid more than those who must spend more to ship their product long distances.
 - Identical bid amounts are specified for certain contract line items by two or more contractors.
 - Identical calculations or spelling errors appear in two or more competing bids.
 10. *Competition Restricted.* Proposal requests are made orally to only a few contractors, rather than published in a newspaper, or they appear in obscure publications, during a holiday period or on a weekend.
 11. *Consultant Involvement with Contractor.* A consultant or the employee of a consultant who has close professional or personal ties with a particular bidder/contractor or its officials, is related, either by birth or by marriage, to a particular bidder/contractor or its officials, or is engaged to help develop the requirements, and then accepts a job with a potential bidder or acts as consultant to a potential bidder on the same requirements definition they helped develop for the company.
 12. *Contractor Meetings.* Competing contractors regularly socialize or appear to hold meetings more frequently than regular trade and association meetings.
 13. *Contractor Selection Unjustified.* The lowest bidder is not accepted even though the lowest bidder meets all the requirements for the contract, or the contract is awarded to a contractor with a history of poor performance.
 14. *Contractor/Subcontractor Relationships.*
 - A low bidder who withdraws from the contracting process later becomes a subcontractor of a higher bidder.
 - The successful bidder repeatedly subcontracts to companies that submit higher bids or are qualified to act as prime contractors but do not submit bids.
 - One contractor's tender package includes the bids of subcontractors who are actually competing for the main contract.

- The successful contractor subsequently uses unsuccessful bidders as subcontractors on the same project.
15. *Dummy Bids.*
 - A bid is accepted from a contractor unqualified to meet the bid specifications.
 - Bids were submitted that do not comply with obvious provisions of the bid specifications or contract requirements.
 - Only one bidder has put forward a complete bid that meets the specifications and requirements in the tender documents while the others have simply thrown together corporate material only tangential to the contract.
 16. *Industry Price Lists.* Competitors exchange price information among themselves from an “industry price list” or “price agreement” to which contractors refer in formulating their bids. Bidders refer to “association price schedules,” “industry price schedules,” “industry suggested prices,” “industry-wide prices,” or “market-wide prices.”
 17. *Narrow Bid Specifications.* Specifications that create unnecessary restrictions in soliciting bids for competitive contracts—that typically fit the products or capabilities of only certain contractors or exclude contractors or products that would otherwise qualify for the contract. Examples include an unusual format for the submission of the proposal, a requirement that the bidder use only certain types of equipment, or limitations or restrictions related to the specific goods or services to be supplied.
 18. *No Audit Terms.* The contract does not provide for an inspection or audit of all the contractor’s records relevant to the performance of the contract (including records of subsidiaries or related companies performing work in connection with the contract).
 19. *Official Involvement.* Certain senior management or employees take an active interest in whether or not a certain bidder is awarded a contract, request information with respect to the details of a proposed contract, get closely involved in a contracting process outside their job responsibilities, or are unusually demonstrative in their support for the successful bidder.
 20. *Preferred/Unpreferred Contractor Documentation.* An unusual amount of affirmative data on preferred contractors or an unusual amount of derogatory data on nonpreferred contractors is maintained in the file.
 21. *Rebid Patterns.* New or supplementary bids are requested as a result of changes in the specifications after the initial bids have been opened, or certain contractors do not rebid when asked to do so.
 22. *Release of Confidential Information.*
 - Confidential contract information is released in advance or selectively to certain contractors.
 - One or more contractors ask to receive the bid package prior to release of the invitation to tender.
 - The successful bid contains specific information from company files that was not supplied in the tender call documents.
 - Information is released to competing contractors by consultants or firms engaged prior to the tendering process.
 - A nondisclosure agreement relating to sensitive information is not included in the files provided to consultants hired prior to the tendering process.

23. *Request for Proposal Mistakes.* The tender call or request for proposal has a mistake (intentional) that would allow for a tender recall if the “preferred” contractor does not submit the lowest bid.
24. *Rushed Timing.* The tender call has an unusually short closing date, so that only bidders with inside knowledge would have the opportunity to prepare an adequate response. The time allotted to prepare the contract specification document or for the contractors to prepare and submit a proposal is short considering the total estimated dollar value of the contract or the complexity of the bid specifications. Rushed timing is often indicative of someone trying to circumvent the usual controls by creating a situation in which only those with advance information have enough time to prepare their bid.
25. *Split Contract.* Contracts have been split into two or more smaller amounts to avoid approval or authorization that would otherwise be required for larger sums.
26. *Tender Changes.* Bid documents appear to have been altered after submission.
27. *Tender Deadline Exceptions.* Tenders are opened prior to the deadline, or are received after the closing date but are not disqualified.
28. *Withdrawals.*
 - The lowest bidder withdraws after submission of their tender.
 - A bidder is allowed to withdraw from the contracting process without justification.
 - A contractor withdraws from the contracting process without justification and is not required to forfeit the bid bond.

How Round Can a Number Be Case Study

A manufacturer of heavy equipment for the mining industry knew how to manage its production schedule so that it was nearly always profitable despite the cyclical nature of metal prices and its effect on demand for new equipment at the mines and smelters. It was noticed, however, that one plant seemed to be suffering gross margin pressure despite a continuing high level of equipment sales. It was also noticed that the onset of lower profitability coincided with the hiring of a new plant manager. An investigation by the internal security department discovered nothing out of the ordinary except that the new manager seemed to want to control everything at the plant, down to the smallest details of day-to-day operations.

As profits continued at inexplicably low levels, head office called in a team of forensic accountants to investigate the manager and the plant accounts. Rumors of the manager’s intrusive operating style caused the investigators to look at all transactions he had initiated or approved. Nothing turned up despite an extensive review of the relevant documents until one of the investigators noticed some peculiar numbers on a copy of the winning contract for a large supply of materials. Of the 52 items on the contract, 45 had unit prices that ended in 5 or 0. Of these 45 items, the price \$1.75 appeared seven times and \$4.30 appeared five times. The three losing bidders had slightly higher prices such as \$1.83 and \$4.37 for the same items but lower prices on the other seven items.

A review of other contracts won by the same contractor and their comparison with those of the losers showed a similar pattern: slightly lower rounded numbers for all but a few items

for which the winning bidder's unit price was higher. Further investigation showed that the few higher-priced items were always bought more frequently and in greater volumes than the many lower-priced items. Because of the higher unit prices and huge number of units purchased of the few items, the winning bidder's contract was much more expensive than any of the losing bids.

Taking advantage of the manager's signed waiver allowing the company to audit his use of company communications equipment, the investigators hired a computer forensics expert to recover deleted voice-mail and e-mail messages. The recovered messages revealed not only that the manager was colluding with the winning bidder but was also developing schemes with several other suppliers. When the manager and winner of the rigged bids were confronted with this evidence, the manager denied everything but the contractor spilled the whole story. The manager left the company voluntarily and agreed to repay the benefits he had received from the supplier. The plant returned to former levels of profitability.

Red Flags in the Selection Stage of Sole-Sourced or Other Non-Competitive Contracts

No bids are solicited for the awarding of sole-sourced or other non-competitive contracts; there is a selection process only. A requirements definition must be developed, and the contractor must meet the performance and evaluation criteria. This section addresses only those red flags involving the selection stage of sole-sourced and other non-competitive contracts.

The following are the types of fraud that typically relate to the selection stage of sole-sourced and other non-competitive contracts:

- Conflict of interest
- Purchases for personal use
- Secret commissions and kickbacks
- Small purchase order fraud or split purchases
- Unnecessary purchases

The following red flags could be indicative of these types of fraud:

1. *Contracts Repeatedly Awarded to One Contractor.*
 - Goods and services are continually purchased from a single source without development of secondary suppliers.
 - Goods or services are purchased from the same source or contractor over a long period of time, without documented verification of market price changes or documentation showing the existence of other providers
 - No time limit set for mandatory review of the single source.
2. *Conversion of Competitive Contract.* A contract initiated in the competitive process is converted into a negotiated sole-source contract.
3. *Documentation Supporting Sole-Source Contractor.*
 - Documentation in the file in support of sole-source or non-competitive contractor does not make sense or is overly descriptive or aggressive.

- Employees working outside their job descriptions sign statements in support of sole-source contractors.
4. *Repeated Small Purchase Orders.*
- Contracts have been split for the purpose of bypassing financial authority, or avoiding other levels of review.
 - Purchases are split that in total would be above authorized spending limits.

These red flags may indicate the presence of fraud as shown in Table 13.5.

TABLE 13.5 RED FLAGS: SCREENING THE SELECTION STAGE OF SOLE-SOURCE CONTRACTS

| Red Flags | TYPE OF FRAUD THAT MAY BE INDICATED | | | |
|--|-------------------------------------|----------------------|----------------------------|------------------------|
| | Secret Commissions & Kickbacks | Conflict of Interest | Purchases for Personal Use | Un-necessary Purchases |
| 1. Contracts Repeatedly Awarded to the Contractor | √ | √ | √ | √ |
| 2. Conversion of Competitive Contract | | √ | √ | √ |
| 3. Documentation Supporting Sole-Source Contractor | √ | √ | √ | |
| 4. Repeated Small Purchase Orders | | | √ | √ |

Detecting Fraud in Sole-Sourced or Non-Competitive Contracts

In these types of fraud, there is usually some form of collusion between a company employee and a contractor. It is difficult, however, to obtain evidence of fraud from company sources during either the scrutinizing or in-depth examination phases. Secret commissions or kickbacks are even more difficult to detect and investigate as they are often considered to be a marketing cost by the contractor, which is one of the costs of doing business.

Contractors in the habit of offering secret commissions, kickbacks or other types of “benefits” will rarely make a direct and blatant offer. Contractors usually begin with subtle overtures as they look for the vulnerabilities of agents or employees, those areas in which they might be most easily exploited. They might begin by discussing the employee’s lifestyle, family, salary, or job satisfaction. They will probe into the hobbies or special interests of the employee. They may learn that the employee is a new homeowner, and then steer the discussion to the high cost of mortgages. They may suggest that a mortgage at a very favorable rate can be arranged perhaps from a related corporation. The employee may not even suspect a connection at the outset. As time goes on, additional benefits will be subtly arranged. Christmas and birthday gifts may arrive from the contractor, or expensive luncheons or dinners may be arranged. Once it becomes a habit for the employee to receive gifts and other minor benefits, the contractor will likely increase the amount. Cash, cars, and travel expenses will likely follow. Job offers and even corporate shares will usually put the employee under full control of the contractor.

Conflict of Interest Case Study

A contractor met a senior manager of a company for the first time at a luncheon, and quickly learned that the manager had a great interest in quarter horses. He had a small farm and the contractor had a 500-acre ranch. As they were parting from the lunch, the contractor invited the manager to fly down to his ranch the next weekend to see a matched pair of quarter horses. The manager accepted without either party mentioning who would pay for the flight.

The following day a first-class return airline ticket arrived at the manager's office. The contractor personally met the manager at the airport and joined him on the flight to the ranch. The manager offered to pay for the tickets, but the contractor said they could deal with money later.

Contrary to what he told the manager at the lunch, the contractor did not have the matched pair of quarter horses on his ranch. Before the manager arrived for the weekend, the contractor ordered two matched horses from a horse dealer and had them delivered to his ranch. The manager returned to the ranch with the contractor on four other occasions. Subsequently, the contractor offered the manager the job as president of his refining and smelting company, along with 60,000 shares of his company, which were valued at more than US\$1.50 per share on the market.

Shortly thereafter, the manager approved a major contract for the contractor's company. In this case, the pattern of conversation and dealings between the contractor and the official demonstrate that a conflict of interest had developed. At the outset, the manager had expected to pay for the airline tickets and other expenses. After the second trip to the ranch, there was no further mention of payment. The contractor had told the manager that he had set up an account receivable in the manager's name and that the manager could pay the amount owed whenever he wished. The manager, of course, never paid any expenses. The process of discovering and proving that this conflict of interest existed was quite involved because little hard evidence was available.

13.5.3 Screening the Contract Performance & Evaluation Stage

During the contract performance and evaluation stage, the contract work is completed and approved, and progress reports and change orders are issued and approved. During this stage, the work specified in the contract is meant to be performed in accordance with the specific terms of the contract, which could include particulars as to the timing and due dates, sizes and quantities, volumes anticipated, and the skills of the people who are meant to fulfill the terms of the contract.

The following are the types of fraud that typically relate to the contract performance and evaluation stage:

- Change order abuse
- Conflicts of interest
- False representations
- Product substitution
- Secret commissions and kickbacks

Red Flags in the Contract Performance & Evaluation Stage

The following red flags could be indicative of fraud involving the contract performance and evaluation stage:

1. *Change Order Issued.* A change order is issued on the contract without a valid justification for doing so.
2. *Changes to Contract After Award.* Changes are made in the definition of services required after the awarding of the contract. This provides the contractor with an opportunity to submit claims for losses based on these changes.
3. *Complaints About Quality.* Documentation in the file expressing concerns over possibly inferior goods or services.
4. *Contract Extension.* An emergency extension allows the contractor to complete the project after the completion date specified in the contract.
5. *No Inspector on Site.* There is no inspector on site to confirm that the contracted work is complete at the appropriate stage of the contract.
6. *Performance Variations.* Foreign-made products are provided where domestic products were required; contractor used untrained employees when skilled personnel were required.
7. *Testing Certificates.* No original test results or reports appear in the contract file (especially if required by the contract specifications), or tests performed by the contractor are not certified by an independent testing agency.
8. *Verification of Contractor Performance.* No formal procedures are in place to ensure the contracted work has actually been performed to specification; there is no formal program for inspection and quality assurance; goods and materials have not been tested as required by the contract specifications; the contracting department relies entirely on the contractor to ensure goods and services meet specifications; and employees rely completely on the contractor to carry out testing and assure the tests will adequately test the requirements of the contract.

The following table (Table 13.6) shows the types of fraud most commonly committed in the contract performance and evaluation stage, and the types of red flags that are indicative of such fraud.

TABLE 13.6 RED FLAGS: SCREENING THE CONTRACT PERFORMANCE & EVALUATION STAGE

| Red Flags | TYPE OF FRAUD THAT MAY BE INDICATED | | | | |
|--|-------------------------------------|-----------------------|-----------------------|----------------------|----------------------------|
| | Change Order Abuse | Conflicts of Interest | False Representations | Product Substitution | Secret Comm'ns & Kickbacks |
| 1. Change Order Issued | √ | | √ | | √ |
| 2. Changes to Contract After It Has Been Awarded | √ | √ | | | √ |
| 3. Complaints About Quality | | | √ | √ | √ |
| 4. Contract Extension | √ | | | | √ |
| 5. No Inspector on Site | | | √ | √ | √ |
| 6. Performance Variations | | √ | | √ | √ |
| 7. Testing Certificates | | √ | | √ | √ |
| 8. Verification of Contractor Performance | | √ | √ | √ | √ |

13.5.4 Screening the Billing & Payment Stages

Fraud in the billing stage usually involves the submission of false, inflated or unsupported invoices by the contractor. Fraud in the payment stage usually involves payment diversions, duplicate payments, or payments being made ahead of schedule.

Red Flags in the Billing & Payment Stages

The following red flags could be indicative of fraud involving the billing or payment stages:

1. *Charges Higher Than Contracted.* The rates actually charged by the contractor are higher than the rates quoted in the contract, or the contractor submits charges for services not included in the contract or in the bid specifications.
2. *Contractor Complaints re: Non-Payment.* The contractor complains that payment has not been made, or that the accounts are not being paid on a regular basis, or that certain invoices have been paid, while others are outstanding.
3. *Cost Overruns.* There are significant cost overruns on the contract.
4. *Invoice Details.* Whiteout is used on a document or contains seemingly irrelevant handwritten details, or products listed on the invoice are referenced by a product number only and provide no description of the nature of the goods provided.
5. *Invoice Identification.* Certain contractor or subcontractor invoices lack telephone numbers and/or have only a post office box as an address, or the contractor submits photocopies of invoices as support for charges on a cost-plus contract.
6. *Invoices Not Certified as Paid.* The contractor does not certify that the subcontractors' invoices submitted on a cost-plus contract were paid.
7. *Materials Not Yet Purchased.* A progress payment claim made for materials is not supported by a paid subcontractor invoice.

8. *No System for Review of Contractor Invoices.* Invoices are not cross-checked to previously submitted invoices for possible duplication.
9. *"Payments" from Contractor to Company Personnel.* The successful contractor provides gifts, parties, meals, or any other benefits to a company employee(s).
10. *Timing of Progress Payment Charges.* Progress payments do not appear to coincide with the contractor's plan and ability to perform the contract.
11. *Uncleared Checks Submitted as Proof of Payment.* The contractor submits photocopies of only the front side of the check to show that the subcontractors' invoices on a cost-plus contract were paid.

The following table (Table 13.7) shows the types of fraud most commonly committed in the billing and payment stages, and the types of red flags that are indicative of such fraud.

TABLE 13.7 RED FLAGS: SCREENING THE BILLING & PAYMENT STAGES

| Red Flags | TYPE OF FRAUD THAT MAY BE INDICATED | | | | | |
|--|-------------------------------------|-------------------------------------|-------------------|-------------------|------------------------|-----------------------------|
| | Duplicate Invoices | False Invoices/ Inflated Pricing | Front-End Loading | Payment Diversion | Progress Payment Fraud | Secret Comm'ns & Kick-backs |
| 1. Charges Higher than Contracted | | √ | √ | | | √ |
| 2. Contractor Complains re: Non-Payment | | | | √ | √ | |
| 3. Cost Overruns | | √ | | | | √ |
| 4. Invoice Details | | √ | | | | |
| 5. Invoice Identification | | √ | | | | √ |
| 6. Invoices Not Certified as Paid | | √ | √ | | √ | |
| 7. Materials Not Yet Purchased | | | √ | | √ | |
| 8. No System for Review of Invoices | √ | | | | | √ |
| 9. Payments from Contractor to Employees | | | | | | √ |
| 10. Timing of Progress Payment Charges | | | | | √ | |
| 11. Uncleared Checks Submitted as Proof of Payment | | | √ | | √ | |

13.5.5 Screening for Off-Book Frauds

For ease of reference, the list of red flags previously outlined that may indicate the presence of off-book frauds such as bribery, secret commissions, kickbacks, and/or conflicts of interest, are listed below.

Requirements Definition

- Excessive stock acquired
- Marketing information in files
- Narrow requirements definition
- Official involvement
- Replacement period unreasonable
- Rushed timing
- "Surplus" goods replaced
- Thin file syndrome

Bidding and Selection

Red flags associated with competitive contracts:

- Award patterns
- Bid specifications unclear or vague
- Bid specifications unrelated to requirements definition
- Changes to specifications after award but prior to contract signing
- Company alumni involvement with contractor
- Company personnel related to contractor
- Competition restricted
- Consultant involvement with contractor
- Contractor selection unjustified
- Contractor/subcontractor relationships
- Narrow bid specifications
- No audit terms
- Official involvement
- Preferred/unpreferred contractor documentation
- Rebid patterns
- Release of confidential information
- Request for proposal mistakes
- Rushed timing
- Tender deadline exceptions
- Withdrawals

Additional red flags associated with sole-sourced or other non-competitive contracts:

- Contracts repeatedly awarded to one contractor
- Conversion of competitive contract
- Documentation supporting sole-source contractor

Contract Performance & Evaluation

- Change order issued
- Changes to contract after it has been awarded
- Complaints about quality
- Contract extension
- No inspector on site
- Performance variations
- Testing certificates
- Verification of contractor performance

Billing & Payment

- Charges higher than contracted
- Cost overruns
- Invoice identification
- No system for review of invoices
- Payments from contractor to employees

13.6 SCRUTINIZING SUSPECT PROCUREMENT CONTRACTS

| <i>Phase</i> | <i>Primary Objective</i> | <i>Nature of Testing</i> | <i>Nature of Interviews</i> |
|--------------|--------------------------|--|---------------------------------------|
| Scrutinizing | Test the allegations | Establish whether fraud has occurred/who involved/how done | Fact-finding interviews re: who & how |

As discussed earlier in this chapter, scrutinizing is the second phase in which the allegations identified as red flags in the screening phase are tested to determine whether or not fraud has occurred. This phase involves performing analyses, comparisons, interviews and/or other investigative procedures of a sample of transactions in order to understand the actions of the parties involved, and to identify whether there are any issues that should be subjected to a rigorous in-depth examination of all the available evidence. As one would expect, there are numerous different types of analyses, comparisons and other investigative procedures that could be performed in the scrutinizing phase; the specific approach to be taken would depend on the circumstances of the case. Rather than describing each of them, this section *introduces* the procedures that could be undertaken when scrutinizing suspect procurement contracts by providing steps or procedures that might be considered for at least one type of procurement fraud per stage in the procurement process as follows:

| | |
|--|--|
| Requirements Definition Stage: | — Unnecessary Purchases |
| Bidding & Selection Stage: | — Bid Rigging |
| Contract Performance & Evaluation Stage: | — Product Substitution |
| Billing & Payment Stages: | — Inflated Pricing |
| | — Progress Payment Fraud or Front-End Loading |

In addition, this section includes procedures that might be considered when investigating off-book frauds such as bribery, secret commissions and kickbacks, and conflicts of interest.

13.6.1 Scrutinizing the Requirements Definition Stage

Table 13.4, *Red Flags: Screening the Requirements Definition Stage*, in Section 13.5.1, (found in 13.5, Screening Procurement Contracts) lists the red flags that may indicate the occurrence of the following types of fraud:

- Conflict of interest
- Secret commissions and kickbacks
- Unnecessary purchases

The steps involved in scrutinizing for conflicts of interest or secret commissions and kickbacks are addressed later in this chapter.

Scrutinizing for Unnecessary Purchases

The steps involved in scrutinizing for unnecessary purchases include performing additional research to confirm or refute the red flags found in the screening phase of the investigative process. The following are the types of procedures that could be performed/questions that could be asked:

1. Research Relative to the Goods or Services Acquired.

- Do the goods or services contracted for fit the profile of the department or division?
- How long has the company been using these particular goods or services?
- Were the goods or services actually delivered/provided?
- Are the goods or services being used by the department/division that originally ordered the goods or services? To what extent?

2. Internal Department or Agency Research.

- What level of employee or management approved or recommended the contract? Is the level too high or too low?
- How long has this “approving person” been in the department? In the company?
- How long has the “approving person” been dealing with this particular contractor?
- Did the company deal with this particular contractor prior to the approving person’s employment with the company?

3. *Contractor Research.*

- Perform a background check to determine when the contracting company was incorporated. A recent incorporation could indicate a lack of stability, and could also indicate the company is a sham.
- Perform a background check on the officials or directors of the contractor's company. This may reveal an association between the contractor and a company employee.
- Examine contractor documentation. Is the address a post office box, for example?
- Call the contractor using the telephone number listed in the files or on invoices.
- Consider the numerous potential sources of documents and information that can be obtained about a contractor from outside the company.

13.6.2 Scrutinizing the Bidding & Selection Stage

Section 13.5.2, *Screening the Bidding and Selection Stage*, lists the red flags that may indicate the occurrence of the following types of fraud:

- Bid rigging, collusive bidding or price fixing
- Bribery
- Conflict of interest
- False representations
- Information theft or bid fixing
- Phantom contractor
- Purchases for personal use
- Small purchase order fraud or split purchases
- Secret commissions and kickbacks
- Unnecessary purchases

Set out below are a number of investigative procedures that could be performed in the scrutinizing phase of the investigative process for bid rigging.

Scrutinizing for Bid Rigging

Bid rigging includes many forms of anti-competitive activity. The common thread running through such activities, however, is arrangements among contractors limiting competition. The variations on this theme are only limited by the imaginations of the contractors involved. Common schemes include the following:

1. *Bid Suppression.* Contractors agree among themselves that at least one will refrain from bidding or agree to withdraw a previously submitted bid to allow another bid to be accepted.
2. *Complementary Bidding.* Contractors submit unacceptably high token bids or bids with special but unacceptable terms. Such bids are not intended to win but to create the appearance of competition.
3. *Bid Rotation.* The colluding contractors submit bids but take turns submitting the lowest bid. Bid rotation schemes often follow a cyclical pattern or a pattern related to the size of the contract.

4. *Market Division.* Contractors refrain from competing in a designated portion of a market divided by government department, customer, or geographic area. Contractors will not bid or will submit only complementary bids to a solicitation from a customer not assigned to them or in a different geographic area.

Bid rigging has been found to be prevalent in a number of industries, including: asphalt paving, bread-making, building construction, cigarettes, coal, dredging, electrical equipment, lumber, milk, retail gasoline, roofing, shipment of household goods, waste disposal, and wholesale produce.

To demonstrate that bid rigging has occurred, it is necessary to establish with a reasonable degree of certainty that an agreement has been made to restrain trade. It is necessary to establish that the contractors had a common arrangement to fix prices or discounts, and/or allocate customers, territories, or markets. The process of scrutinizing bid rigging, therefore, involves refuting or confirming the red flags of such an agreement. The following are some of the investigative procedures that could be performed:

1. *Bidder Information.* Perform corporate searches to find the date of incorporation plus names of directors and officers of each bidder.
2. *Compare Bidder Histories.*
 - Compare specifications with previous similar contracts, perhaps from another department. For example, a contract undertaken in one territory should be compared with a similar contract in another.
 - Review previous contract files to determine timing, amount, and nature of each contractor's involvement in other bids.
 - Prepare a schedule comparing the details of each bid and each winning contractor. Identify whether there are any patterns.
 - Examine each bidder's previous contracts. Look for relationships with other contractors and subcontractors and any patterns of bidding on other jobs. Determine whether contractors switch places as contractor and subcontractor on different jobs.
 - Look for large consortiums among competing contractors. Check each contractor's involvement in a consortium or partnership arrangement on any other contract at the time the competitive bids were submitted.
 - Follow up on any withdrawals to obtain their reasons for withdrawing from the bidding process.
3. *Complaint Review.* Examine all files and correspondence for any unauthorized release of information. Follow up on any complaints by employees or others about this particular contract or group of contractors.
4. *Industry Review.* Inquire of other departments, law enforcement or government agencies about collusive bidding in the contractor's industry. Consider obtaining media searches on the industry/specific contractors. Consider obtaining price lists from other competitors.
5. *Request for Proposal Review.* Compare the requests for proposals with the requirements definition information/bid specifications information. Determine whether the documents are so specific that only certain contractor(s) can fill the requirements.

13.6.3 Scrutinizing the Contract Performance & Evaluation Stage

Table 13.5, *Red Flags: Screening the Contract Performance & Evaluation Stage*, in Section 13.5.3, (found in 13.5, Screening Procurement Contracts), lists the red flags that may indicate the occurrence of the following types of fraud:

- Change order abuse
- Conflicts of interest
- False representations
- Product substitution
- Secret commissions and kickbacks

Set out below are a number of investigative procedures that could be performed in the scrutinizing phase of the investigative process for product substitution.

Scrutinizing for Product Substitution

Product-substitution is a vendor fraud that involves the delivery of goods or services below contract specifications without giving notice of the change but seeking reimbursement based on the higher standard in the contract. Typical instances of product substitution are as follows:

- Providing goods of a lesser quality than specified in the contract.
- Furnishing items produced by a manufacturer other than the original equipment manufacturer as specified in the contract.
- Furnishing items produced in a country other than that specified in the contract.
- Failing to conduct suitability and reliability tests specified in the contract.
- Using staff with lesser skills/qualifications to perform the services required in the contract.

This type of fraud typically occurs in the contract performance and evaluation stage.

The following are some of the investigative procedures that could be performed to determine whether product substitution has occurred:

1. *Research Industry Complaints.* Call competitors to determine the contractor's reputation, and canvas other departments and public sources for complaints of inferior products or service.
2. *Consult Employees and Contract Files.* Ask employees who requested the goods or services whether the goods/services met their requirements; and determine whether the services contracted for were actually performed.
3. *Examine the Inspection/Quality Review Process.* Determine whether an inspection process has been used for other unrelated contracts performed for the company. Determine whether the inspection process was marginalized for this particular contract, or whether the inspection process is simply ineffective for the company as a whole.
4. *Establish Quality of Prior Projects.* Identify any previous contracts performed by this contractor, and establish whether any further contracts/expenditures have been required to remedy any quality deficiencies in previous contracts.

13.6.4 Scrutinizing the Billing & Payment Stages

Table 13.6, *Red Flags: Screening the Billing & Payment Stages*, in Section 13.5, Screening Procurement Contracts, lists the red flags that may indicate the occurrence of the following types of fraud:

- Duplicate invoices
- False invoices/inflated pricing
- Front-end loading
- Payment diversion
- Progress payment fraud and front-end loading
- Secret commissions and kickbacks

Set out below are a number of investigative procedures that could be performed in the scrutinizing phase of the investigative process for inflated pricing/cost mischarging, and in connection with progress payment fraud and front-end loading.

Scrutinizing for Inflated Pricing or Cost Mischarging

Most cost-plus and cost-per-unit contracts require the contractor to submit detailed certified documentation supporting cost or pricing data. The biggest risk relates to charges for unallowable costs that are concealed or misrepresented as allowable costs or are otherwise hidden in certain accounts not usually examined closely.

Labor costs are one of the easiest to mischarge because employees' labor can be readily shifted from contract to contract with the stroke of a pen on their timecards. The only way to be absolutely certain that labor costs are charged to the correct contract is to observe the actual work of each employee, then check the accounting records to ensure the cost is charged to the right contract.

To prove that inflated pricing or cost mischarging has occurred, it is necessary to demonstrate that the suspect entry was not a mistake. Therefore, the process of scrutinizing for inflated pricing or cost mischarging must confirm or deny the contractor's intent.

A few of the investigative procedures that could be performed in scrutinizing for inflated pricing and cost mischarging are identified below.

1. *Competitor Pricing/Rate Reasonableness Testing.* Call competitors that provide similar goods and services and compare prices. Note any large discrepancies.
2. *Scrutinize Subcontractor Invoices.* Look for discrepancies between physical addresses and post office box addresses. Verify the physical addresses. Check the telephone numbers. Look up the subcontractor in a telephone book or business directory and compare spelling, address, and other details to the invoice.
3. *Historical Pricing Analysis.* Compare prices charged on this contract with prices charged on prior contracts. Followup on any unexplained discrepancies.

Scrutinizing for Progress Payment Fraud and Front-End Loading

Progress payments are made as work moves through the stages of a contract. They are based on costs incurred, the percentage of work completed, or the completion of a particular stage of the contract. The purpose of progress payments is to provide contractors

with a continuing source of revenue to meet their contractual obligations. In some cases, the contractor's work may be the subject of an inspection but, for the most part, companies rely solely on the contractor's integrity that the contracted obligations have been carried out. If a contractor requests payment for costs not actually incurred, a fraud or other crime has been committed.

Progress payment fraud or front-end loading therefore occurs when a contractor submits a progress payment request based on false information, usually including a falsified certificate that the required stage of the contract has been completed.

The procedures that could be performed in scrutinizing for progress payment fraud and front-end loading include the following:

1. *Scrutinize Files.* Review monthly contract status management reports and obtain a detailed explanation of any differences between the scheduled completion dates and actual completion dates. Also obtain explanations for any time periods in the contract when the contracted work was performed much quicker than originally anticipated.
2. *Scrutinize Invoices.* Examine invoices to determine whether goods appear to have been shipped on odd dates such as weekends or holidays.
3. *Contractor Review.* Perform corporate searches to determine whether the contractor has declared bankruptcy or otherwise has cash flow difficulties.
4. *Inspection of the Job Site.* Visit personally or send a qualified person such as an engineer to check that work is actually progressing as reported in the contractor's invoices.

13.6.5 Scrutinizing for Off-Book Frauds

In an earlier section of this chapter, we provided basic definitions of the following types of procurement fraud: bribery, secret commissions and kickbacks, and conflicts of interest. Each of these forms of procurement fraud are typically off-book frauds, but what is the difference between them? And if you suspect they're occurring, how do you prove them? What are the elements of proving this type of procurement fraud?

Bribes, Secret Commissions, Kickbacks & Conflicts of Interest: The Differences

A secret commission is something that is paid after the fact—usually based on a percentage of the contract or the amount of the fraud; a bribe is something that is paid in advance—usually on a flat fee basis, or could be in the form of a perk; a kickback is something that is paid after the fact—again on a flat fee basis, or in the form of a perk; and a conflict of interest usually involves ownership of a contractor by an employee.

So essentially, the difference between each of these types of procurement fraud relates primarily to the timing and manner of the payment (see Table 13.8):

TABLE 13.8 COMPARISON OF BRIBES, SECRET COMMISSIONS & KICKBACKS

| | Timing of Payment | Amount |
|----------------------|---|---|
| Bribes | Paid <i>before</i> the contract is awarded, or <i>before</i> the fraud has been consummated | Flat fee or a perk |
| Kickbacks | Paid <i>after</i> the contract has been awarded, or <i>after</i> the fraud has been consummated | Flat fee or a perk |
| Secret Commissions | Paid <i>after</i> the contract has been awarded, or <i>after</i> the fraud has been consummated | % of contract or fraud |
| Conflict of Interest | Paid <i>after</i> the contract has been awarded, or <i>after</i> the fraud has been consummated | Paid indirectly via the employee's ownership interest |

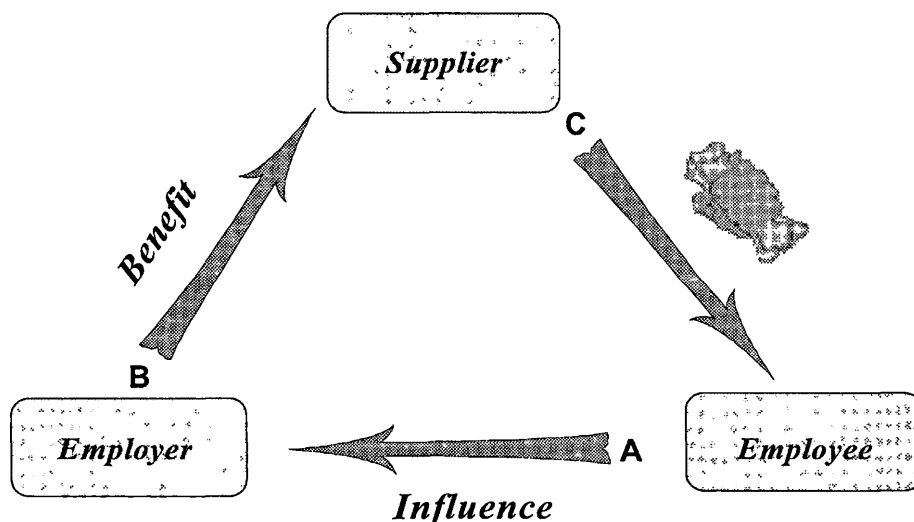
Bribes, Secret Commissions, Kickbacks & Conflicts of Interest: Proving Them

Off-book frauds can be quite difficult to prove... as the records relating to the specific payments involved are all off-book, where the fraudulent payment from the contractor to the employee occurs outside of the books of the business. Proving such off-book frauds therefore involves establishing inappropriate relationships that are to the benefit of two or more parties, and are to the detriment of a third.

But how does one establish that an inappropriate relationship is occurring? What are the symptoms of this? What does an inappropriate relationship look like? What makes a relationship "inappropriate"?

The answers to these questions can be found by studying the following "triangle of dishonesty":

"TRIANGLE OF DISHONESTY"



If an employee exercises "influence" in a way that would benefit a particular contractor in exchange for an "inappropriate perk", they are involved in a triangle of dishonesty.

Influence (A) could be exercised by an employee in a variety of ways at various stages in the procurement process:

- In the requirements definition stage, the employee could provide “justification” for the purchase of goods or services that are not needed.
- In the bidding and selection stage, the employee could engage in influence-peddling regarding the decision to award a contract to one particular supplier over another—through false testimonials, or other internal communications to sway the ultimate decision-maker, or the employee could provide confidential information to the supplier that would enable them to prepare a bid that would appear to be more attractive to the employer from a cost or quality perspective.
- In the contract performance and evaluation stage, the employee could provide false evaluation reports on the supplier’s performance under the contract.
- In the billing and payment stage, the employee could approve invoices for amounts that are higher than appropriate.

The *benefit* (B) to a supplier is generally in the form of a lucrative contract where:

- The supplier can earn a relatively high level of (legitimate) profit; or
- The supplier can earn “extra profits” (with the assistance of the employee) through another form of procurement fraud such as false or inflated invoices, or product substitution.

The *inappropriate perk* (C) could be paid from the supplier to the employee in the form of gifts, cash, travel, entertainment, consulting fees, home renovations, or other types of personal benefits.

Section 13.5.5, *Screening for Off-Book Frauds*, lists the red flags that may indicate the occurrence of these types of fraud.

Such red flags are identified and initially confirmed in the screening process, and must then be scrutinized before establishing that a full-scale investigation is warranted. Falsified records may complicate this process. The investigative procedures that would typically be performed in the scrutinizing include establishing evidence related to each of the three sides of the triangle of dishonesty: the influence, benefit and perk. This often involves examining the relationships of the parties involved, and obtaining circumstantial evidence to confirm or refute the concerns raised in the screening stage of the procurement investigation process. The scrutinizing steps that could be performed include the following:

1. *Review of Supplier Background.* Check out the ownership of the supplier’s company. Identify all the supplier’s related companies or businesses. The supplier may not necessarily be the party who paid the benefit.
2. *Examine the Nature of the Relationship Between Supplier and Employees.* Determine the nature of any relationship between the supplier and the employee suspected of having received a benefit. Discovery of a relationship could establish the motive for the payment of the alleged secret commission.
3. *Review of Employee Lifestyle.* Gather information about employees in an unobtrusive manner to find out if any employees:

- are living beyond their means, that is, have cash, assets such as expensive cars or jewelry, or lifestyles that include expensive vacations or gambling that cannot be accounted for by known sources of income. Salary information may be required.
 - have personal or social commitments involving one or more suppliers.
4. *Review of Employee Roles and Responsibilities.* Establish whether the suspected employee has any authority to sign checks, authorize purchases, or grant credit up to a certain limit. Has that limit been strictly observed?
 5. *Assess the Relationship Between Employee Decision Making and Benefits Gained.* Determine whether the suspected employee has acted beyond the scope of his or her normal responsibilities to approve or influence the approval of transactions. Compare the timing of the benefit with decisions made by the suspected employee. Determine whether the contractor benefited. For instance, did a contractor win a contract around the time of an alleged secret commission payment?

13.7 IN-DEPTH EXAMINATION OF SUSPECT PROCUREMENT CONTRACTS

| <i>Phase</i> | <i>Primary Objective</i> | <i>Nature of Testing</i> | <i>Nature of Interviews</i> |
|----------------------|---------------------------------------|--|-----------------------------|
| In-Depth Examination | Obtain final proof for court purposes | Detailed testing/beyond a reasonable doubt | Accusatory interviews |

As discussed earlier in this chapter, the in-depth examination phase is the third phase, and is the “formal investigation phase.” It involves detailed document analysis, analytical techniques and interviews, to prove the fraud.

In the in-depth examination phase, the investigative procedures performed would include interviewing persons involved in or with knowledge of any apparent fraudulent scheme. The investigative process would include identifying, and then interviewing individuals in possible conflict with the contractor or any of the suppliers or subcontractors. Employees terminated by the contractor, the supplier, or the subcontractor are usually willing to provide details of any wrongdoing.

The in-depth examination phase also requires analyses of a wide range of documentary evidence. Typical evidence examined at this stage includes evidence related to the activities of any suspect including debt levels and servicing, gambling, alcohol or drug use, and any other unusual behavior.

For instance, expense accounts or assets under the control of an employee should be reviewed. Contractors and employees may frequent the same restaurants or belong to the same social or sports clubs. A comparison of the employee expense accounts with those of the contractor may indicate an undisclosed relationship.

The types of investigative procedures that are performed during the in-depth examination phase can be quite intrusive; accordingly, there are numerous legal and ethical considerations that must be addressed in order to ensure that any evidence gathered is, in fact, admissible, to maximize the level of co-operation of those being investigated, and to minimize the likelihood of a legal claim by the parties being investigated:

- How to conduct interviews
- How to gather and preserve evidence
- What is considered relevant evidence
- Legal evidentiary issues
- Employee/employer legal issues

Typical steps undertaken to address these concerns include the following:

1. Establish the care, custody, and control of all available documents relating to the contract.
2. Inform the corporate authorities of the current situation and its direction.
3. Consider the interview process:
 - Should other people within the department or contractor's organization be interviewed?
 - Should other contractors be interviewed?
 - Does the investigator have a right to meet with these people and examine their documents?
4. How far back in time should one go?
5. Is additional documentation necessary and available? If so, where?
6. Does the available evidence form a pattern?
7. Evaluate the evidence and present the results to general counsel for his or her consideration and reaction strategy.
8. Decide whether to consult experts.

Evidence may consist of statements from witnesses, confessions of perpetrators, documents, and perhaps the report of an expert.

13.7.1 In-Depth Examination of the Requirements Definition Stage

There are numerous different types of investigative steps that could be performed in the in-depth examination phase of a procurement fraud investigation. The types of steps chosen, and the degree to which they are successful, will be dependent upon the type of procurement fraud suspected, the extent of evidence available, and the degree to which the investigator is entitled to, and is successful in obtaining, the evidence required.

Set out below are some investigative procedures that could be performed when investigating allegations involving concerns arising at the requirements definition stage specifically related to the possibility of unnecessary purchases.

In-Depth Examination for Unnecessary Purchases

1. *Analysis of Contractor Records.* Obtain the contractor's financial statements and calculate the total dollar value of all contracts awarded to this contractor as a percentage of the contractor's total revenue to measure the contractor's dependence on the company. Calculate the total dollar value of the contracts awarded to one particular contractor as a percentage of all the contracts awarded by the company or department to measure the degree to which the company is dependent on the contractor.

2. *Interviews of Company Employees.* Interview company employees who ordered the goods or services to find out why the goods or services were ordered but not used.
3. *Interviews of Other Suppliers.* Contact other suppliers of the same goods or services to determine their use. Look for excessive support or total rejection of what these goods or services can do.
4. *Interview of Consultants.* Interview consultants who may have carried out pre-contract studies or analyses. Determine the nature of any relationships between such consultants and the successful bidders.
5. *Conflict Analysis.* Examine the involvement of any employee from other divisions or a related department. If these individuals have been involved in obtaining information or preparing the needs or requirements documents, their relationship with the successful bidder must be determined, even if they are senior management.

13.7.2 In-Depth Examination of the Bidding & Selection Stage

Set out below are some investigative procedures that could be performed when investigating allegations involving concerns arising at the bidding and selection stage of the procurement process, specifically related to the possibility of bid rigging.

In-Depth Examination for Bid Rigging

1. *Interview of Employees and Consultants.* The topics addressed during such interviews could include:
 - Checking for any irregularities in the tendering and awarding of the contract. Interviewees may not come out and say there were irregularities, but their demeanor could indicate their feelings.
 - Determine whether any former employee is now employed by the contractor or if there are any other unreported relationships. Excessive support by one employee or senior manager could indicate a relationship with the successful bidder or a relationship with the real beneficiary of a fix in the bid process.
 - Determine whether there is any preference for one contractor over another.
2. *Interview of Unsuccessful Bidders Concerning the Bidding Process.* The topics addressed during such interviews could include:
 - Excessive complaints or no complaint at all, which may indicate further evidence of a problem.
 - Praise of the successful bidder, which could indicate the bidders fixed the process themselves.

13.7.3 In-Depth Examination of the Contract Performance & Evaluation Stage

Set out below are some investigative procedures that could be performed when investigating allegations involving concerns arising at the contract performance and evaluation stage of the procurement process, specifically related to the possibility of product substitution.

In-Depth Examination for Product Substitution

1. *Interview Testing Organization's Employees.* Determine whether testing was actually performed and obtain test results.
2. *Engage Technical Experts.* Have independent experts carry out an examination of the technical aspects of the products or services in question.
3. *Customs Follow-Up.* For contracts specifying only foreign goods, use a qualified investigator to verify the types, quality, and quantity of items imported; compare these to the contracted products. Do a search by type of product and address of importer to determine whether the contractor is importing the contracted goods under another name.
4. *Interview of Company Employees and Management.* Interview users to find out whether the service or goods were satisfactory. Poor performance but continued use identifies a problem.

13.7.4 In-Depth Examination of the Billing & Payment Stages

Set out below are some investigative procedures that could be performed when investigating allegations involving concerns arising at the billing and payment stages of the procurement process, specifically related to the possibility of inflated pricing or cost mischarging, and progress payment fraud and front-end loading.

In-Depth Examination for Inflated Pricing or Cost Mischarging

1. *Interview Subcontractors.* Contact subcontractors and discuss the nature of their work. Obtain evidence of completed work.
2. *Pricing Review.* Compare catalog prices and service rates to the contract prices.
3. *Timecard Review.* Obtain a complete employee list and all timecards for the contracted work. Examine signatures on timecards for forgery or tracing through carbon. Examine timecards for changes to the contract number charged.
4. *Review of Cost Allocations.* Obtain all journal entries and allocation worksheets showing all cost allocations between contracts, particularly between cost-plus and fixed-cost contracts. Investigate any adjustments. Be aware that the contractor may claim the adjustments were necessary because of accounting errors. Examine the alleged accounting errors.

In-Depth Examination for Progress Payment Fraud and Front-End Loading

1. *Contractor Review.* Examine the contractor's subcontractor files for evidence of nonpayment for goods or services charged to the company by the contractor. Obtain financial statements and cash flow projections to determine whether the contractor is able to meet its liabilities.
2. *Company File Review.* Do a complete audit of all cost-plus submissions.
3. *Subcontractor Review.* Telephone or write suppliers to verify their existence and that they supplied the goods and work specified. Verify the prices, quantity, and quality of the goods or services supplied.

13.7.5 In-Depth Examination for Off-Book Frauds

The investigative procedures to be followed in an in-depth examination for secret commissions, bribery, kickbacks or conflicts of interest could include:

1. *Review of Financial Statements of Contractor.* Examine the contractor's financial records to establish the nature of any relationship and the extent of any dealings. Bear in mind that dishonest contractors regard secret commissions as a cost of doing business and will include them in their records suitably disguised as expenses.
2. *Review of Accounting and Banking Records of Contractor.* Determine the form and purpose of the alleged secret commission by reviewing the accounting and banking records of the contractor. Does the alleged secret commission take the form of cash or payments to the benefit of the recipient, e.g., travel or a car? The books of account of the payor or of the appropriate related company will have to be reviewed for supporting documentation such as checks and supplier invoices. This review should also disclose how such payments were recorded by the payor.

In general, these payments are recorded as either an expense or a loan.

- If the payment is recorded as a loan to the recipient:
 - What was the purpose of the loan?
 - Does a promissory note exist?
 - Has any interest been charged on the loan or has any interest been collected?
 - What are the terms of repayment, if any, and have any repayments been made?
 - If the loan has been repaid, was a check presented for payment and did it clear the banking system?
 - If the payment was recorded as an expense:
 - Establish the nature of the expense, for example, promotion travel, and whether such payments are in the normal course of business or reflect an unusual transaction.
 - Obtain documents such as invoices, purchase orders, contract or shipping documents that describe the goods or services being paid for.
3. *Review of Personal Financial Affairs of the Employee.* Review the suspected employee's known assets by performing a search to determine how and when such assets were acquired; obtain any documentation in support of these purchases. Examine the personal financial affairs of the employee; this may help establish a lifestyle inconsistent with income.
 4. *Interview Contractor.* Interview the contractor to discover what he or she knows about the company's need for goods or services or whether the contractor got the contract through a possible link to a particular employee.

13.8 ANALYTICAL TECHNIQUES

There is no one correct method or process for analyzing evidence. The type of analysis required will depend on the nature of the allegations. This section will review some typical types of analysis that should be familiar to the investigator. Some of the types of analysis that can be conducted are:

1. Vertical analysis
2. Horizontal analysis
3. Ratio analysis
4. Net worth analysis
5. Statement of cash-flows analysis
6. Source and use of funds analysis

Vertical Analysis

Vertical analysis, which is sometimes referred to as common-size analysis, examines the relationships between line items on an income statement, balance sheet, or statement of cash flows by expressing components as percentages.

In the vertical analysis of an income statement, for example, net revenues is assigned 100 percent. For a balance sheet, total assets is 100 percent. All other line items are expressed as a percentage of these two numbers. When completing the analyses, the changes must be material.

Horizontal Analysis

Horizontal analysis examines the year-over-year change in individual financial statement line items as a percentage. Each line of the base year is assigned 100 percent. The changes in subsequent years are computed as a percentage of the base year's balances.

Ratio Analysis

Ratio analysis can be helpful in detecting potential errors and other irregularities with respect to various balance-sheet and income items.

Net Worth Analysis

Net worth analysis is used to prove the suspect's assets or expenditures for a given period exceed that which can be accounted for from known sources of income. This tool is most useful when the recipient is taking cash or other payments which cannot be traced directly and when the amount greatly exceeds legitimate income. It is often used by the Internal Revenue Service. Net worth analysis is also useful in bribery and corruption cases (off-books). The two methods for completing net worth analysis are the assets method and the expenditures method, and are described in the following:

Assets Method

The *assets method* should be used when the suspect has invested supposedly illegal funds to increase net worth. The steps to complete this analysis are to:

1. Establish a base period such as the year before the one in question.
2. Compute the suspect's net worth at the end of the base year. Identify all assets at cost and all known liabilities. The difference is the net worth.
3. Repeat the computation for the year in question using the same method.
4. Determine the suspect's known income during year two, and subtract known expenses for year two. The difference between the suspect's income and expenses equals the increase or decrease in net worth from year one to year two attributed to known sources.

5. Subtract the increase in net worth from known sources from the total increases in net worth to determine the amount from unknown sources.
6. Repeat the computations as necessary for subsequent years.

Expenditures Method

This *expenditures method* is best used when the suspect spends allegedly ill-gotten gains on lavish living, travel, and entertainment. Expenditures in excess of known revenues are unexplained income. The steps to complete this analysis are:

1. Establish the suspect's known expenditures for the relevant year. Expenditures include the use or application of funds for any purpose. These expenditures include deposits to bank accounts, purchase of major assets, travel and expenses, payment of loans, and payment of credit cards.
2. Identify all sources of funds available to the suspect. These funds include cash on hand from previous years' loans and gifts.
3. Conclude that the amount in excess of known income shows the expenditures attributable to unknown sources.

Key Points in Determining Net Worth

The auditor should consider the following in determining net worth:

1. All assets should be valued at cost, not fair-market value.
2. Ignore depreciation or appreciation.
3. Give the suspect the benefit of the doubt when estimating income or assets.
4. Factor in expenses for living, such as food and entertainment.
5. Consider interviewing the suspect to identify all alleged sources and to rebut later defenses.

Statement of Cash-Flows Analysis

Cash is the asset most often pilfered. Analysis of the statement of cash flows can be useful in detecting fraud in small businesses. For example, suppose the bookkeeper misappropriated cash instead of paying the company's bills. The statement of cash flows highlights the significant increase in payables. Cash receipts were stolen over a period of years and the statement of cash flows shows one of the following:

- A significant increase in receivables
- Cash, as a percentage of sales, decreasing over time

Source and Use of Funds Analysis

The purpose of a source and use schedule is to provide an overview of the flow of funds. A source and use schedule can show the individuals involved in the transactions and the benefits obtained from the use of the funds. The level of examinable detail will be determined by the availability of documents. There may be a number of disbursements for which the canceled check is missing, or a number of deposits whose origin is unknown. The investigator should ensure the information in the source and use schedule is complete and accurate. The integrity of the investigator's work will be undermined if the schedule contains errors.

Methods of Displaying the Results of Analysis

Chronologies. Chronologies tell the story of events by organizing information along a time line. This narrative can be developed through interviews. A sequencing of all relevant documents can also be prepared. Comparisons of chronologies can expose inconsistencies between witness statements and documentary evidence. Such conflicts may be important to investigations such as bid rigging where the sequence of events is critical.

Chronologies keep the investigation team focused on the relevant events. They can also highlight gaps requiring further investigation. Comparing chronologies may also lead the investigators to a better understanding of the issues. The behavior of a certain person may be explained by a change in their personal situation.

Charts and Graphs. The fundamental purpose of charts is to present complex issues organized into a simple, easy-to-understand format. They can be used in a variety of ways, such as illustrating relationships between individuals and/or companies or visualizing the flow of information within an organization.

Graphs are similar to charts in that they, too, are used to simplify the presentation of information, especially quantifiable information. For example, monthly sales figures may be more easily understood as a line or bar chart than as a column of numbers. Graphs tend to have a greater impact than a column of numbers because the use of pictures puts the numbers in context. A graph of an individual's monthly expenses, for example, may highlight a shift in the spending pattern that corresponds to a known event such as the awarding of a contract. Graphs can be used to play up the strengths of one own position, or point out the deficiencies of one's adversary. They can also be used to great effect in reports and later in court.

13.9 REPORTING FRAUD IN PROCUREMENT CONTRACTS

At the conclusion of the in-depth examination stage of the fraud detection process, the auditor should be in a position to recommend various options:

- A full formal investigation
- A loss recovery action be instituted on behalf of the company
- A disciplinary action be taken against an employee and the case referred to general or corporate counsel
- No further action is necessary since the suspicions were unfounded

Such recommendations should be made in a written report to management. If management decides to take the case further, other reports are likely to be required for legal counsel or government agencies. Once a case is referred to such agencies, a process of loss recovery, criminal investigation, or other action may be contemplated.

If the auditor recommends the case go forward, the reports to management and legal counsel should request a decision on how to proceed. Both reports should thus be written simultaneously and have similar content.

As the case progresses, it becomes more organized and the evidence becomes easier to manage. The reporting process would also be greatly simplified by an organized approach to handling the evidence.

13.9.1 Organization of Evidence

Some cases may produce up to 100 binders of documents and working papers. It is therefore vital to prepare indices for notes on findings. The casebook or working paper files can then list the various documents and issues of the case that forms the basis of the written report.

The preparation of a complete index requires a command of the facts of the case. Such knowledge, however, is usually not gained until near the end of the case. Accordingly, any useful interim index must be capable of expansion and reorganization as the case progresses. As the index expands, it may be necessary to create subindices to group-related documents and issues. Such organization keeps the auditor from becoming lost in the paperwork. The lack of good housekeeping practices is probably the chief cause of misplaced documents or forgotten information.

The documents filed in the working papers would typically include copies of documents used as evidence for the case, file notes, and memoranda prepared by the auditor. The copies used in the working paper files would be one of the two sets of copies taken of the original documents (the other set being retained to prepare the document brief). At the time of copying, post-it notes placed on the original documents would facilitate gathering the original evidence required for submission in court. If one document relates to more than one section of the working paper file, it would be advisable to copy that document for inclusion wherever needed elsewhere in the file.

13.9.2 Working Paper File Sections

Most working paper files would contain similar types of documents. Standardization of the filing method for these documents makes it possible for any auditor to find his way around a given case. Included in this section is a list of documents typically included in a fraud detection file prepared by auditors or designated employees. Since the order of these documents has not been finalized, it is up to auditors or designated employees to determine a suitable organizational standard for their working paper files.

Case Indices

Case indices should be prepared for each file. If a case requires more than one file, master indices should be filed in the front of each file. It may even be necessary to prepare indices of the indices, if the case is unusually complex. The indices should cover not only the issues of the case but also the overview and background records.

Reports

All reports presenting findings in summary form to either management or external agencies, should be filed in the working paper files. Among these reports should be drafts of all reports seen by others.

Outstanding Matters

This section contains all material pertaining to methodology and any incidental materials. Monitoring such loose ends may be crucial to a large investigation especially since there is no standard methodology of fraud detection.

As the case develops, this section will likely be subdivided into a small number of broad subject areas. As procedures are completed, such documents should be annotated and retained to record the methodology when preparing the report.

Case Overview

The case overview should be represented by a chart of the relevant issues or red flags and any conclusions. If the case cannot be represented on one sheet of paper, either the person preparing the overview chart does not understand the case, or the case is too complicated. Such a chart should be prepared right at the beginning of the fraud detection process to show what is known. This overview should change as new information changes the focus of the auditor's attention. This case overview will form the basis for organizing the evidence and the findings section of the working papers file.

Chronology of Events

A case chronology permits new documentation and information to be put into perspective. The chronology may include timing details for all the issues of the case, or, if the case is complex, there may be an overall chronology of significant events and then subchronologies of events relating to particular issues.

Key Player Profiles

The particulars of all witnesses and suspects should be listed together with the details of their involvement. This information is useful in detecting inconsistencies or gaps in later interviews or other evidence.

Contact Lists

All investigators should also be listed along with a description of their role in the fraud detection process and their telephone number(s). This list should be available to all individuals working on the case.

Correspondence

All correspondence and attachments should be filed by date. Correspondence received should be date-stamped. If these documents contain information required elsewhere in the file, copies should be made and filed in the appropriate place.

Diary Entries

This section includes all records of meetings, telephone calls, and interviews. If the case is large enough, such documentation might be split into several files. Meeting records should include the date, time, and place of the meeting; the names of those attending; the topics discussed; and a summary of all points resolved. Telephone logs should record the name of the caller, date, and time of the call; and the topics discussed. Preparatory notes should be filed together with interview transcripts. As new issues come up in the course of the interview, a new working paper should be opened. This practice keeps topics distinct and allows the auditor to build files in the relevant case sections.

Time Estimates

Although time estimates are difficult to prepare, a "best-guess" must be made near the beginning as to the total estimated time for completion. This time estimate can be used in

staffing decisions and in estimating when the case will be ready for the report preparation stage.

Legal Documentation

Copies of all relevant legal documentation should be obtained and filed in the working paper files for future reference. For example, a civil case file would usually include a statement of claim, a statement of defense, and a statement of counterclaim. The attorney on the case should be able to provide such documentation.

Findings and Supporting Documentation

All issues addressed in the case overview should be supported by working papers and their related documents. Flexibility in working paper file organization should permit change as the case overview changes.

Once the working paper file has been completed, the process of preparing a report should be fairly simple, since the working paper file should already include all the findings. During the writing of the report, there should be few, if any, calculations required.

13.9.3 The Formal Report

Most reports issued to either the company or external legal counsel will have similar contents. Below is a list (in no particular order) of the types of things most often included in reports:

1. *Summary of Findings.* All points addressed in the case overview and the auditor's procedural recommendation should be included.
2. *Scope.* The scope of the auditor's examination should be described in any report. This would normally include a list based on the indices of the records and other evidence examined.
3. *Approach.* The methodology used should be patterned after the case overview and may include the completed procedures as documented in the outstanding matters section.
4. *Findings.* The text of the case findings should be written simply and chart summaries and graphs used to support the findings.
5. *Summary Charts and Graphs.* These documents should be filed as appendices to the report and cross-referenced to the supporting documentation.
6. *Document Brief.* A document brief is a collection of documents to be entered as exhibits in court. Document briefs are usually indexed and the pages numbered consecutively to facilitate cross-referencing during the formal investigative process and court proceedings.

13.9.4 Evidence

The in-depth examination phase gathers additional evidence to support the allegations or suspicions noted in the screening and scrutinizing stages. Evidence is required to perform procedures such as the following:

- Summarizing and explaining the accounting or other systems and any paper trail
- Analyzing accounting and other records to identify additional areas of concern

- Describing the position and responsibilities of the suspect within the system
- Demonstrating the control exercised by the suspect on the accounting system
- Showing the suspect's knowledge of the accounting system
- Establishing and demonstrating any patterns of the fraud cover-up
- Establishing and proving the extent of the fraud
- Establishing and proving the financial position of the suspect
- Considering the position of other people within the organization and the possibility of collusion
- Documenting findings fully

Some of the evidence necessary to perform procedures such as these might have been gathered in the screening and scrutinizing phases. Evidence may also be gathered during interviews.

Since oral evidence alone will not support either a criminal or a civil action, the auditor must retrieve other types of evidence. How much evidence is enough? That depends on the type of action to be taken, either civil or criminal.

It is therefore necessary for fraud auditors to be aware of the rules of evidence and other related issues. This knowledge will affect the way an auditor conducts the screening, scrutinizing, and in-depth examination phases of the fraud detection process. Evidence must be gathered and preserved in a form acceptable to the courts.

13.9.5 Practical Issues

In any case involving documentary evidence, the auditor is faced with three questions:

1. What documents should be obtained?
2. What is their source?
3. How should they be handled?

Deciding on What Documentation to Obtain

What documents to obtain should be decided during the screening and scrutinizing phase with a view to the in-depth examination. Such decisions will be based on meetings with witnesses and initial assessments of findings. The types of financial documentation likely to be required include:

- Documents showing the movement of assets into and out of the company, contractor, or third parties during the period under investigation
- Books of account, management reports, and statistical analyses pertaining to the contractor or to an individual for the period under investigation
- Relevant correspondence and personal documents such as bank account records

Obtaining Documentation

Once the auditor has decided what records or other documents must be obtained, a list should be prepared. This list can be used when obtaining permission to take originals or copies or could form the basis of a subpoena. Document descriptions should include at least the type and period required. This description can then form the basis of an

acquisition strategy that avoids “fishing expeditions.” Support may be gathered from sources such as:

- Public documents
- Documents provided voluntarily
- Witness interviews

This material will also be useful for the formal investigation stage.

Handling the Documents

Documents obtained during any stage of the fraud detection process must be carefully handled, properly identified, and cataloged. They must not be written upon, altered, stapled, or unstapled during the course of the examination.

The chain of custody must be recorded for all documentary evidence that may be used in court. All such documents should be marked, identified, inventoried, and preserved to maintain their original condition. If gaps in the chain occur, the evidence may be challenged in court on the theory that the writing or information on the evidence is not original or is not in its original condition and is therefore of doubtful authenticity. For any document to be admissible as evidence, it is necessary to prove that it is the same document that was obtained and in the same condition. It should be marked at the time of seizure for later identification. Because several persons may handle it between acquisition and presentation in court, the complete chain of custody must be recorded. To maintain the integrity of the document, the auditor must follow strict rules of evidence handling.

The auditor must mark the documents for later identification in court that they are indeed the documents seized and that they are in the same condition as when seized. The auditor may, for instance, initial and date each document in the margin, in a corner or some other inconspicuous place. If such marking risks rendering the document open to question on the grounds of defacement or other alteration, the auditor should make a copy for his files, then seal the original in an envelope and write a description on the front.

These techniques should be applied any time the auditor comes into possession of an original document that may be used as evidence in a trial. Steps should be taken to preserve the copy's authenticity in case it is needed to replace the original in court.

Once the documents have been marked, identified, and cataloged, photocopies should be made to provide working copies for use when preparing schedules, completing interviews, and building the working paper files. If one fresh copy is taken which is never marked, the process of preparing a document brief will be that much easier.

13.10 PROCUREMENT FRAUD CHECKLIST

The following Procurement Fraud Checklist is designed to assist CPAs in addressing procurement fraud.

Generally, all *No* answers require investigation and follow-up. Use the *Ref* column to cross-reference the checklist to any additional working papers. The Checklist is intended for general guidance and information only. Use of the Checklist does not guarantee the prevention or detection of fraud and is not intended as a substitute for audit or similar procedures.

TABLE 13.9 PROCUREMENT FRAUD CHECKLIST

| PROCUREMENT FRAUD CHECKLIST | Yes | No | N/A | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| 1. Needs Assessment | | | | |
| a. Is there a real problem that requires a needs assessment? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Does the needs assessment provide sufficient detail to justify the project or the performance specifications required? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. If the need is real, is this contract necessary or could the problem be solved in-house? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Has the alternative been thoroughly examined as to materials, labor, time, etc.? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. The Contract | | | | |
| a. Have contract performance standards been established? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Have in-house levels of authority been set for approval of the contract? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Is tendering necessary or could this contract be let on a sole-source basis? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. If tendering is necessary, has a list of qualified contractors been developed based on technical, financial and management criteria? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Has the draft procurement contract been compared with the original needs assessment? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. Has legal counsel been asked to be involved in the process of drafting the contract? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| g. Does the request for proposal (RFP) contain all the elements of the needs assessment? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| h. Is the contractor expected to provide technical and financial reports? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| i. Is a process in place for monitoring contractor performance? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| j. Is a process in place to resolve disputes? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| k. Is a process in place to review any proposals to amend the contract? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| l. Is some suitable person authorized to approve any amendments? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| m. Does anyone have override authority? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| n. Does the contract allow for audits of the contractor's records? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 13.9 (continued)

| PROCUREMENT FRAUD CHECKLIST | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| 3. Collusion Between Employees and Vendors | | | | |
| a. Are certain contractors consistently successful in winning bids? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Is the lowest bidder not accepted even though it fulfills all the requirements of the contract? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Is the requirements definition so specific that tendering could be improperly restricted to only one or a few companies? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. In reviewing the contract, are there any oddities in the timing of performance, distances to be traveled, frequency of certain activities, expenditures, labor, etc.? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Has the bid of an unqualified contractor won? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. Is any contractor suspiciously aggressive in its marketing? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| g. Do any company employees show an unusual interest in the details of the contract considering their responsibilities? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| h. Is anyone in the tendering company exceeding their authority in assisting in the procurement process? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| i. Is the tendering period too short for the type of project? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| j. Are the bid specifications unclear as to performance and other criteria? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| k. Are the bid specifications inconsistent with the requirements definition? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| l. Have there been any changes to the specifications in the period between the granting of the award and the signing of the contract? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| m. Have the bid proposals been delivered orally rather than published in the usual way? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| n. Are any company alumni, current employees or consultants involved with or related to any contracting party? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| o. Is the material on preferred and unpreferred contractors in company files unusually favorable or derogatory? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| p. Are there any "mistakes" in the RFP that would allow for a tender recall if the contractor desired by the fraudsters did not submit the lowest bid? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| q. Has the contract been split into small amounts to avoid exceeding authorized expenditure limits? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

TABLE 13.9 (continued)

| PROCUREMENT FRAUD CHECKLIST | Yes | No | N/A | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| r. Is there any indication that bid documents have been altered after submission? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| s. Have any bids been opened prior to the deadline or received after the deadline? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| t. Has a competitive tendering process been converted to a sole-source contract? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| u. Has an unexplained changed order been issued on a contract? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| v. Is the replacement period for goods shorter than the manufacturer's recommendations or departmental practice? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| w. Has more stock been acquired than stipulated under the contract? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| x. Have goods already sold as surplus been replaced? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| y. Has more stock been acquired from one supplier than stipulated under the contract? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| z. Are there secondary sources of supply for materials? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 4. Vendor Fraud Against the Company | | | | |
| a. Can all contractors and subcontractors be confirmed at their addresses and telephone numbers? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| b. Are contractor invoices cross-checked with other invoices to detect duplication? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| c. Are the test-result documents on file originals? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| d. Is the contractor's work checked to ensure performance to specifications? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| e. Are unit rates charged by the contractor the same as in the contract? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| f. Is the work completed according to the phases of the contract? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| g. Is there any documentation in the file concerning substandard goods or services? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| h. Have all invoiced materials actually been purchased? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| i. Have domestic products been substituted for more expensive foreign ones? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| j. Has the contractor certified that invoices submitted by the subcontractors have been paid? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| k. Do the progress payments correspond with the contractor's plan? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 13.9 (continued)

| PROCUREMENT FRAUD CHECKLIST | Yes | No | N/A | Ref |
|---|--------------------------|--------------------------|--------------------------|------------|
| l. Have uncleared checks been submitted as proof of payment? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| m. Have the contractor and subcontractors employed the tradesmen with the contracted level of skills? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| n. Are there any delays or cost overruns on the project? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 5. Collusion Among the Vendors Within an Industry of Bidding Group | | | | |
| a. Do certain contractors always bid against each and others never? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| b. Are any bids unusually high or unusually low? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| c. Did the lowest bidder withdraw after submitting a tender offer? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| d. Are any bid package details inconsistent with the known capabilities of the bidder? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| e. Has a low bidder withdrawn from the tendering process but later become a subcontractor to a higher bidder? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| f. Does the successful bidder subcontract with any losing bidders for work on the same project? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| g. Is one bidder's package more detailed than that of any other contractor? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| h. Do certain contractors not rebid after changes in the specifications? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| i. Has confidential information been release to contractors? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| j. Is there a nondisclosure agreement for consultants to the project? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

CHAPTER 14:

Identity Theft and Corporate Identity Fraud

| | | |
|--------|---|----|
| 14.1 | Introduction..... | 3 |
| 14.1.1 | Defining Personal Identity Theft and Corporate Identity Theft..... | 3 |
| 14.1.2 | Common Types of Identity Theft..... | 4 |
| 14.2 | Laws to Combat Identity Theft | 4 |
| 14.2.1 | Fair Credit Reporting Act..... | 5 |
| 14.2.2 | Identity Theft and Assumption Deterrence Act..... | 6 |
| 14.2.3 | Gramm-Leach-Bliley Act of 1999 | 7 |
| 14.3 | How Thieves Steal Your Identity..... | 7 |
| 14.4 | Personal Identity Theft..... | 8 |
| 14.4.1 | Who Are You, Anyway?..... | 8 |
| 14.4.2 | How Do You Become Separated From Your Identity? | 9 |
| 14.4.3 | Protecting Personal Information | 10 |
| 14.4.4 | What to Do If You Become a Victim | 12 |
| 14.5 | Corporate Identity Theft..... | 15 |
| 14.5.1 | Preventing Identity Theft From Affecting a Business | 15 |
| 14.5.2 | Internal Controls..... | 16 |
| 14.6 | Cyber Identity Theft..... | 19 |
| 14.7 | Conclusion..... | 22 |
| 14.8 | Checklist: Detection of Personal Identity Theft and Corporate Identity Fraud..... | 22 |

CHAPTER 14:

Identity Theft and Corporate Identity Fraud

14.1 INTRODUCTION

The theft of a person's name, personal statistics, and unique identifying numbers enables the identity thief to impersonate the victim and behave as if he or she were the person being victimized. The thief can open accounts, apply for a mortgage, get a credit card, rent a car, even get a job using the victim's name, and all without the victim's knowledge. It is estimated that more than \$1 billion is lost through the use of stolen identity every year.¹ In 2002, in the United States there were 161,819 reports of identity fraud to the Identity Theft Data Clearinghouse of the Federal Trade Commission (FTC), an increase of 88 percent from 86,198 in 2001.² California had the greatest number of victims, at 30,738, in 2002 but the District of Columbia had the greatest number of cases per capita.³ Most victims were in their 20s (26 percent) and 30s (27 percent).⁴ The youthfulness of this group reflects the preference of young people for high-risk technologies such as the Internet and online credit card purchases. Of all fraud complaints reported in 2002 to the FTC and the more than 60 other government and non-government agencies in Canada and the United States with which the FTC has data-sharing agreements, identity fraud accounted for 43 percent, compared with 39 percent in 2001 and 22 percent in 2000.⁵

14.1.1 Defining Personal Identity Theft and Corporate Identity Theft

Personal Identity Theft

Identity theft is a growing problem both for individuals and for corporations. For the individual, apart from the financial losses, which can be significant, stolen identity also means a loss of part of a person's public *persona*, the part that represents one's public integrity in financial transactions. In its worst manifestations, identity theft can be a crippling violation that unjustly creates a reputation for unreliability and untrustworthiness. The institutions with which the victim is used to dealing no longer want to do business with him or her even though the victim might have had a spotless record up to that point. The suspicion that now attaches itself to the victim is like a slander that is slowly gaining acceptance and from which there is no escape. The victim now appears to everyone as

¹ <http://financialservices.house.gov/media/pdf/040303gu.pdf>

² <http://www.consumer.gov/sentinel/sentinel-trends/page8.pdf>

³ <http://www.consumer.gov/sentinel/sentinel-trends/page11.pdf>

⁴ <http://www.consumer.gov/sentinel/sentinel-trends/page10.pdf>

⁵ <http://www.consumer.gov/sentinel/sentinel-trends/page3.pdf>

someone other than he or she really is or has been for his or her whole life. According to *Consumer Reports*, victims of identity theft lose an average of \$800 each but spend two years clearing their names.⁶ Reestablishing one's name is time-consuming and expensive and can precipitate lawsuits against financial institutions for honoring forged documents and general carelessness in checking out the person using the stolen identity.

Corporate Identity Theft

Corporations can be the victims of identity theft just as much as individuals, but they can also be the source of the stolen identities. Credit card companies, banks, mortgage lenders, and savings and loans are common targets of identity thieves. In fact, any company that sells a product using credit services can be a victim.

Corporations are involved in identity theft primarily as repositories of names, Social Security Numbers (SSNs), and the other information essential to the commission of identity theft. The number of databases is increasing with the proliferation of business both on and off the Internet. As has become embarrassingly clear in the last few years, corporations are outrageously slack at preserving the integrity of this vital information. The problem of identity theft for most corporations is primarily a problem of computer security.

14.1.2 Common Types of Identity Theft

1. *Credit-card fraud*: Credit card fraud is the most commonly reported type of fraud, accounting for 42 percent of all frauds reported. The stolen identity was usually used to open new accounts (24.4 percent) or steal from existing accounts (12.1 percent).
2. *Theft of wireless telephone services*: This is the next most frequent type of identity fraud (10.5 percent).
3. *Theft from existing bank accounts*: (8.1 percent).⁷

By the time the victim discovers what has been done, his or her credit rating may be impaired and large amounts of money may have been lost. Then the victim has the long, uphill struggle to reestablish a credit rating and prove the transactions were all done by someone else.

Identity theft is a type of fraud accountants are going to see more and more frequently. It is growing with the flow of information and the increasing number of business and consumer transactions being conducted through high-risk technologies. Despite the introduction of new laws to fight identity theft, the number of victims continues to rise.

14.2 LAWS TO COMBAT IDENTITY THEFT

Congress has responded to the growing problem of identity theft with three new laws:

1. The 1996 amendments to the Fair Credit Reporting Act (FCRA) of 1970.⁸

⁶ "Identity Theft: 33 Million Victims and Counting," *Consumer Reports*, October 2003, p. 12.

⁷ <http://www.consumer.gov/sentinel/sentinel-trends/page9.pdf>

⁸ <http://www.ftc.gov/os/statutes/fcra.htm>

2. The Identity Theft and Assumption Deterrence Act of 1998⁹, which amended chapter 47, title 18 of the U.S. Code to recognize identity theft itself as a crime.
3. The Gramm-Leach-Bliley Act of 1999,¹⁰ which regulates disclosure of nonpublic financial information by financial institutions.

14.2.1 Fair Credit Reporting Act

The FCRA (amended in 1996) governs the creation and use of credit reports. The three main repositories of credit information, the credit reporting agencies (CRAs), are Equifax, Experian, and Trans Union. Together they have 1.5 billion files on more than 190 million individuals and receive about two billion pieces of new or updating information each month. The FCRA makes it an offence to acquire “information on a consumer from a CRA under false pretenses” (§619).

The movement of the credit information sought by the identity thief is at the heart of the modern economy. Consumer spending accounts for more than two-thirds of U.S. gross domestic product, and consumer credit drives this spending. The credit reporting system keeps open the flow of information that facilitates the rapid assessment of credit risk and the approval of mortgages and consumer loans of all kinds. Creditors voluntarily submit (they are not required to do so by law) data on their clients and their borrowing history to the CRAs, which keep credit records on individuals only. Where there is a loan in two or more names, such as those of a married couple or business partners, a record is kept in each name with a reference to the joint loan.

The credit record contains five basic types of information:

1. Information that identifies the individual by name, SSN, and current and previous addresses.
2. The service history of each loan.
3. Information on bankruptcy, foreclosure, liens, and other events contained in public documents.
4. Collection agency reports.
5. Identities of everyone who has requested information from the record.

Some reports even include a spouse’s name, number of dependents, telephone numbers, income and employment record. The CRAs answer more than two million requests for these records *every day*.¹¹ The information arrives from banks, finance companies, credit unions, major retailers, oil and gas companies, utilities, collection agencies, court and other public records. Most accounts are revolving credit accounts followed by installment accounts.

This data is accessed and used by lenders to develop predictive statistical models that assess the likelihood of default by a loan applicant. Through the analysis of historical consumer credit data, lenders have developed generic templates of borrower behavior to which the data on the loan application are compared. The extent of congruity of the application with

⁹ <http://www.ftc.gov/os/statutes/itada/itadact.htm>

¹⁰ <http://www.ftc.gov/privacy/glbact/glbsub1.htm>

¹¹ <http://www.cdiaonline.org/about.cfm>

the historical data provides a means of “scoring” the applicant as a risk. Credit evaluators rely primarily on the level of current and past indebtedness, payment history, and credit account characteristics, such as the type of account, its age, and the frequency with which the borrower applies for other types of credit such as car loans and mortgages.¹²

The development of electronic data processing has changed the whole credit application process. The days of the personal visit to the loan officer and the wait for his or her decision are over. Consumers can now shop for the best rates on the Internet and receive almost instant approval because lenders can apply their credit scoring system to information obtained from an electronic consumer report provided by the CRAs.

The lending industry has also changed from a passive user of credit reports to an active marketer of products based on credit information provided by the CRAs. Insurers and credit card issuers supply the CRAs with a credit-risk profile by which to screen their databases to find those who could be low-risk buyers of their cards or coverage. The insurer or credit card issuer then makes a “prescreened” firm offer of services to the individuals on the list of prospects. The 1996 amendments to the FCRA sharpened the definition to the prescreening process and gave the target consumer the right to opt out of future prescreened lists.

One of the goals of the FCRA is to protect consumer privacy by limiting the distribution of credit reports to those with statutorily defined “permissible purposes” (§604). Such entities include:

- Credit grantors
- Employers
- Insurance issuers
- Government licensing agencies
- Investors, providers of services, and current insurers
- The consumer, upon a written request

A second important objective of this legislation is to achieve the greatest accuracy possible in the recording of information. The FCRA recognizes the importance of reliable information for the credit score but realizes that complete accuracy in this volume of information is not humanly possible. The Act expresses its intent by requiring the CRAs to “follow reasonable procedures to assure maximum possible accuracy” (§607 (b)). To offset the danger of errors, mechanisms are provided that allow the consumer to check his or her own report, dispute the information, and have it corrected. The consumer has the right to know all information in the file except the risk scores and to learn the identity of anyone who has received a copy of the report within the last year.

14.2.2 Identity Theft and Assumption Deterrence Act

The Identity Theft and Assumption Deterrence Act of 1998 is an extremely important piece of legislation that recognizes identity theft as a distinct crime. Up to that time, the unlawful creation, use, or transfer of identity *documents* were crimes but the actual theft of the *information* was not. A person is now considered to have committed identity theft who

¹² <http://www.federalreserve.gov/pubs/bulletin/2003/0203lead.pdf>

“knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.” The key phrase here is “means of identification,” which refers to the names, numbers, codes, and personal characteristics that identify a person and can be transferred from document to document.

The term *means of identification* includes:

- Name, SSN, date of birth, official state or government issued driver’s license or identification number, alien registration number, government passport number, or employer or taxpayer identification number
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation
- Unique electronic identification number, address, or routing code
- Telecommunication identifying information or access device, such as an access code or personal identification number.

14.2.3 Gramm-Leach-Bliley Act of 1999

The Gramm-Leach-Bliley Act of 1999 creates for every financial institution “an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.” The various authorities and agencies that regulate the different types of financial institutions will be responsible for establishing appropriate means of achieving this security and confidentiality.

Financial institutions are now required to provide customers with an annual statement of their disclosure and protection policies. This statement must cover the types of information collected and disclosed to affiliates and third parties on both current and former customers. The customer must be given the opportunity to stop the institution from disclosing information to a nonaffiliated third party. The financial institution may, however, disclose information to such a third party for the institution’s marketing purposes provided the third party contracts not to disclose the information. No account number, access code, or other identifier may be provided to any party other than a CRA.

14.3 HOW THIEVES STEAL YOUR IDENTITY

The identity theft that will affect a person or business may be committed by a friend, a stranger, or an employee, by kids rummaging in the dumpster out behind the office, by the employee of a gas station or restaurant waiter, or by some hacker on the other side of the country or even on the other side of the world. All that matters is that the fraudster obtains sufficient identification to be recognized by the accounting system as an authorized entity with which the company can do business. The initial crime is often not connected to identity theft until many months later, when irregularities start to appear on bank or credit card statements or when credit is refused on a consumer loan or mortgage application. A lost or stolen wallet or home break-in may provide the thieves with a name and Social Security, credit card, and bank account numbers, which can be sold to sophisticated rings

that use the information to commit larger, more daring thefts against banks and corporations—in the victim's name.

Employees, especially in the accounts department of retailers, at banks, insurance companies, medical offices, and government services, use personal information every day in the processing of documents or to verify the identities of customers making inquiries. This data can be copied and sold to identity thieves without leaving any incriminating evidence in the system. Credit reports obtained lawfully from the CRAs may be seen by dishonest employees at credit grantors and used or sold. These reports are particularly attractive targets for identity thieves because they contain *all* the information required to fill out the credit application forms. Although they do not show the victim's credit "score," the thief can determine whether that score is likely to be good or bad from the record; the higher the probable rating, the easier it will be for the identity thief to obtain credit. Information can also be stolen from the mails. Millions of documents with identifying personal information flow through the postal system every day. A "lost" form or bill might not even be noticed until much later. Preapproved credit card offers are a favorite target and an easy one to use quickly.

Thieves also find information carelessly discarded in garbage or in dumpsters. Residential garbage often contains foils from credit card receipts, telephone calling cards, change-of-address forms, and preapproved credit card offers thrown out as junk mail. "Dumpster diving" is especially effective for finding business information such as client lists, bank account numbers, telephone numbers, SSNs, signatures, file numbers, and tax information.

Identity thieves may have acquired some of a potential victim's personal information but need more to commit the crime. They then call a business where the victim is known to be a customer on the pretext of discussing an account and try to talk the phone clerk into giving them the missing information.

The key information the thief needs is the potential victim's name, date of birth, and SSN. Once this information has been gathered, impersonation is, sadly, relatively easy; the thief can do anything the victim could do based on the victim's credit rating.

As stated above, credit cards are the most popular target for identity thieves. Application for the preapproved credit to be sent to a different address or the use of the change-of-address form to redirect credit card bills for the existing number can give the thief plenty of time to use the card before the victim finds out anything is wrong. Delinquencies will go onto the victim's credit report.

The other types of fraud that can be committed with the right identity information are probably limitless: opening bank accounts and writing bad checks on those accounts, taking out loans and defaulting, purchasing goods and services without paying the bills are but a few examples.

14.4 PERSONAL IDENTITY THEFT

14.4.1 Who Are You, Anyway?

To a bureaucracy, you are only who your identification documents say you are. You are your birth certificate, passport, SSN, driver's license, or credit cards. Once you are separated from the identity inscribed on those documents, you cease to be that person. The

person who steals and uses your documentary identity detaches you from your identifiers and places you in a Kafkaesque limbo of frustratingly endless nonrecognition. It is your impersonator who now enjoys the privileges to which you are otherwise entitled simply by virtue of possessing your identifying information—not the documents—just the information. To an institution, you are now a nonperson, a nullity with whom no business can be done.

14.4.2 How Do You Become Separated From Your Identity?

The very act of providing information about yourself to others puts your identity at risk of being stolen. “When you provide information to a person, organization or Internet-based enterprise through a website, use a debit or credit card, use a cordless telephone, a cell phone, a personal digital assistant (PDA), use your personal computer or another computer, send or receive physical mail or email, the risk of others accessing and misusing your most sensitive information is always present.”¹³ Mail can be stolen and information is now available that allows eavesdropping on cell phone conversations. E-mail is notoriously vulnerable to interception. Your personal computer can be hacked and your passwords stolen. In addition, the organizations that gather this information often share it with others. The more the information is shared, the greater the number of employees who have an opportunity to view it and work with it.

The risk of having your information tampered with is compounded by the fact that institutions have a prejudice in favor of taking the computer entry as true over your complaint that there is an error. The institutional position is understandable since the assumption is that the entry only exists because someone saw the appropriate original documents to make the entry in the first place. As a result, there is the suspicion that *you* might be the identity thief or at least have an ulterior motive for wanting to change the data in your file. This combination of prejudice and suspicion form the block that makes it so difficult for victims of identity theft to reestablish their good name.

Finally, institutions have three competing demands on them for the use of identity data. Customers want quick service. To provide this, retailers must have ready access to the databases providing the credit information that makes the sale of a car, TV, or other big-ticket item possible. Institutions of all kinds need the personal information they have gathered to develop marketing strategies that will allow them to focus sales campaigns on those people who fit the right profile for their products. There is also a demand for this information at other organizations that do not have the resources to assemble the data themselves. This profitable use of the information by retailers and marketers then has to be balanced against the need for security to protect the privacy of the individual whose data is being used and the need to provide citizens with protection against the misuse of their identity information by these compilers and users of databases has made necessary the new laws described in Section 14.2, Laws to Combat Identity Theft.

¹³ Jim Gaston and Paul K. Wing, *Protecting Your Money, Privacy & Identity from Theft, Loss & Abuse*, (Toronto: The Canadian Institute of Chartered Accountants, 2003) p. 5.

14.4.3 Protecting Personal Information

Wallets and Purses

The key to protecting personal information is to have as little of it exposed to public view or physical loss as possible. For example, do not carry unnecessary documents in your wallet or purse. Leave at home your Social Security card, birth certificate, passport, the credit card you use only in foreign countries, membership cards, and any other item not used every day. Clear your wallet or purse of all credit card receipts and other papers carrying personal identifiers at the end of the day. Destroy or file at home all unnecessary papers once accounts have been reconciled. Carry only one credit card, your bankcard, and anything else you use regularly. Take care not to leave your wallet or purse unattended in any place such as an office, restaurant, library, or other public place. Make sure all cards carrying your signature are signed immediately upon receipt. Cut up any expired cards.

Mail

An amazing amount of material useful to the identity thief arrives through your mailbox: new unsigned credit cards, driver's licenses, new checkbooks, telephone bills, tax information from all levels of government, utility bills, and bank and investment information, as well as preapproved credit card solicitations and so forth. An identity thief could reconstruct your identity by stealing just a few of these documents.

The risk of having your identity stolen from your mailbox can be greatly reduced by having a secure mailbox with a slot through the door. Outside mailboxes hanging on a wall with a flip top can be looted easily. Keep track of what bills and other documents you should be receiving. If something seems long overdue, call the sender to see whether it has been sent. A common practice is for identity thieves to steal a bill carrying your name, address, and account number. They will then contact the bank or company concerned, send in the change of address form and create a new address in your file and have your correspondence redirected. Since utility bills are frequently asked for by financial institutions to show that you really live where you say, the redirection of these bills is a common ploy of identity thieves gathering the identifiers needed to set you up as a potential victim. The new address will become an additional authenticator of your stolen identity to be used by the thieves.

When you are absent for any length of time, have a friend pick up your mail or have it held at the post office. If you move, call the places from which you receive important mail and notify them of the address change. For these sources, do not simply rely on the post office's forwarding services. The arrival of statements from entities with which you do not do business is a sure indicator something is wrong. Follow up immediately to see why you are getting such material. There may just be a computer error at the company but this may be the first indication that you have become the victim of an identity theft.

Telephones

Landline telephones are more secure than either cordless or cellular. Of course, landlines can be tapped but that requires special equipment and an intrusive connection to your line. You are more likely to have information stolen out of the air by a scanner that can pick up signals from your portable or cell. Your identity is at risk when doing telephone banking over a cordless or cellular phone because thieves can pick up the bankcard numbers and access codes. If you do a lot of banking and must use these insecure phones, change your access codes often.

The telephone is also a tool commonly used by fraudsters to commit their various scams. In one of the most common frauds, a “bank inspector” calls saying there is a fraud going on at your branch and they need your access codes to monitor a suspected dishonest bank employee. Since banks never actually investigate internal fraud this way, any such call is by definition fraudulent. Never give any identifying information to anyone over the phone. Never give any identifying information in a fax that will be going to a general fax number at an office. Anyone can read those faxes. If you have to send confidential information by fax, call the recipient and ask them to stand by the fax machine while you send it.

Debit and Credit Cards

Thieves have been known to go to extremes to get debit and credit card information: fake automated teller machines (ATMs) that record the numbers, hidden cameras at gas stations and restaurants to capture the transaction, simply looking over a person’s shoulder as the personal identification number (PIN) is entered, observing an ATM with binoculars from across the street, posing as a security guard or window cleaner and watching people enter their numbers. The stolen information is encoded on a magnetic strip on the back of a false card that is then used as if it were yours. Debit and credit cards are a major source of information for identity thieves and should be used carefully. Change the PIN on your debit card every time you receive a replacement. Limit the number of accounts linked to your debit card. The best practice is to have it linked only to your checking account where there is likely to be less money at any given moment than in the savings account. Never let your debit card out of your sight during a transaction. On the back of credit cards issuers have added a number composed of three or more digits to the basic card number. This supplementary “card verification value” is not necessary to complete any purchase and should not be revealed at any time except to the issuing financial institution. If you are traveling, make sure you have the local emergency number to call if your card is lost or stolen. Sign the back of all replacement cards upon receipt.

Social Security Number

In the United States this is one of the key, if not *the* key, pieces of identity information needed to impersonate you. It is your unique identifier developed by the government primarily for keeping track of its dealings with the millions of American citizens. Unfortunately, as noted elsewhere in this chapter, the government has legislated its use for a wide variety of trivial purposes that puts it into a lot of different databases. Since there is no legislation preventing its use for recordkeeping in the private sector, a lot of companies use it as a cheap and ready identifier that saves the cost of creating a new file number for every client. As a result, your SSN could be not only in numerous government databases but also in an unknown number of private ones.

The best protection against misuse of your SSN is to monitor closely all transactions with entities you know use this number in their recordkeeping. Never give it out to unsolicited callers. Never send it by any of the insecure communications technologies such as e-mail or cell or portable phones. If you are disposing of papers carrying the SSN, shred them; do not put them out with the trash or into recycle bins.

Computers

The personal computer installed in your home is the primary means of processing information today and, as a result, likely contains many of your personal records most valuable to an identity thief. The first line of defense in protecting this information is to allow no one else to use your computer. More people than you might think could have access to your computer: guests, tradesmen, children, housekeepers, babysitters, friends. Hackers can now break into your software and track your keystrokes or enter your files and access passwords and PIN numbers and other personal information. Viruses, worms, and other malicious invaders can copy information and transmit it over the Internet to an identity thief.

Basic protection of your computer begins with limiting access. Other frequent users such as your teenaged children should have their own passwords and access only to what they commonly use. Only you should be able to install or remove software. Never download software from an unknown source. Get one of the well-known virus scanners and use it at least once a month. Never open e-mails from unrecognized senders. All obvious spam should be deleted immediately. Store essential private information such as tax records or medical prescriptions on CD-ROMs, USB memory sticks or some other medium—but not on your hard drive. Log off correctly from bank, utility, or other Web sites where you have transacted financial business. Only disclose credit card numbers or other financial information to a known institution or vendor when transacting over the Internet. Never send personal information by e-mail; it can be read by anyone. If you work from home and must send important information to clients, use encryption.

14.4.4 What To Do If You Become a Victim

The first thing to do when you suspect something is wrong is to define the problem. Is whatever happened really identity theft or some other kind of theft or simply an error somewhere in a company computer system? Perhaps you just lost something or made a transaction you have forgotten about or the transaction was processed under the name of the vendor's holding company which you don't recognize instead of under the name of the vendor where you made the purchase. If you cannot explain the matter satisfactorily to yourself, contact the company concerned and check to see how the transaction came to be on your bill. Write down the names of everyone you talk to in the course of your investigations and keep notes of what was said. This information will be important later in the police investigation if, indeed, there has been an identity theft.

If the company confirms your suspicions, take immediate action to close all affected accounts and cancel any cards or PINs associated with them and your online and telephone banking services. Examine the record of recent transactions in all accounts to make sure you are not under attack from another quarter. If you discover a pattern of unexplained transactions, inform the police immediately. Provide the police with the names and telephone numbers of everyone you contacted in your own inquiries.

While the police are conducting their investigation, contact the fraud departments of the CRAs and have a “fraud alert” put on your credit report. It is essential to contact the CRAs immediately since they are clearinghouses for almost all requests for credit. Send a request in writing to get a copy of your report. Check to see whether any accounts have been opened in your name or any unauthorized changes made to existing accounts. Get the names of any companies making inquiries in your name. Inform the police of all these inquiries and any fraudulent accounts opened as a result of these inquiries. Give the police the names of the companies making the inquiries. Since fraud alerts and victim statements expire, continue to monitor your credit report and renew the alerts if necessary. CRAs are under no legal obligation to provide these services; check the policy of each bureau. Red flagging your credit report with a fraud alert is, however, no guarantee that additional credit might not be granted on the fraudulent accounts. Credit grantors can override these fraud alerts if they wish. For this reason, it is imperative that you close the fraudulent accounts.

If the police report determines that an identity theft is the most likely explanation of the questionable transactions, it can be used as a first step to reestablishing your name with your creditors. The police report can be used to reinstate your name with the bank. Once the bank has accepted that you are who you say you are, get a letter from them that can be used with other credit institutions or vendors to explain any questionable transactions. Get a letter from each company that accepts the police explanation so that you can develop a file to show to each succeeding company. The greatest problem will be in explaining transactions done in your name with companies with which you normally do not do business or are located overseas.

If it is established that you have been a victim of identity theft, you should file a complaint with the Federal Trade Commission through their hotline (877) IDTHEFT (438-4338) or www.consumer.gov/idtheft. The FTC cannot bring a criminal case but they can help you with information on how to deal with the consequences of the theft. The FTC also passes your information on to law enforcement and other agencies that assist in tracking down identity thieves.

I Always Wanted To Be a Doctor Case Study

There was a late fall chill in the Maine air when a man walked into the branch of a large national bank and identified himself as a medical doctor. He said he had a successful practice in another part of the city and was considering joining a clinic in the area near the bank. He needed the line of credit to do some renovations to his home and to make some investments that he wanted to keep secret from his wife. He gave the loans officer a cell phone number saying his wife worked at his clinic and he didn't want the bank calling either his office or his residence.

The man had been referred to the loans officer by a mutual friend, a real estate agent. The loans officer was an experienced employee who had worked for the bank for 12 years and had a lending record far better than average. The real estate agent had introduced other clients to the loans officer through the years and this referral seemed no exception. The real estate agent herself, however, did not do her

banking at this branch and the loans officer actually had no real knowledge of the agent's financial affairs.

The man completed the application for a \$250,000 line of credit in the normal way and provided his date of birth, SSN, a telephone number, and various credit references, none of which indicated account numbers or outstanding balances. He would secure his loan with a mortgage on title against his principal residence, which was registered in his own name, valued at \$800,000 and mortgage free.

The application was quickly approved and within a few weeks he had drawn down the whole line of credit. In one 10-day period, \$236,650 was drawn down in a series of checks and bank drafts. A credit card application was also requested through the branch. It was approved and soon carried a liability in excess of \$4,000.

As part of the credit application, a request for insurance had also been completed. Because the line of credit exceeded \$200,000 the insurance company conducted a verification check with the client. They were surprised to find that the doctor they talked to was not the same "doctor" who had applied for insurance. The real doctor denied having a line of credit at the branch in question. The bank was notified and its investigation revealed that the line of credit and the credit card were being used in a way typical of a fraudster. One of the last purchases was airline tickets to Caracas, Venezuela. The card and the airline tickets were immediately cancelled.

The subsequent investigation showed that the real doctor in no way physically resembled the man who had sat across the desk from the loans officer and applied for a \$250,000 line of credit. The doctor said that about three months prior to discovering he had become a victim of identity fraud, he and his wife had noticed that mail had stopped coming to their residence. They finally checked at the local postal station and found that a change of address card had been made out for their residence and mail was now being redirected to a private mail box in the suburbs. They filed a complaint with the local police but nothing more was heard until the insurance company contacted him to verify the particulars of the line of credit. The doctor stated he did not know the real estate agent, knew nothing of any mortgage or transfer of title on his principal residence from his wife's name to his own, had no business in that part of the city, and was not familiar with the payees of the checks drawn on the line of credit.

Investigation of the checks and drafts drawn against the line of credit showed that large sums had been paid to the real estate agent, her company, and her husband. Substantial amounts had been paid for German luxury cars and \$100,000 to a foreign exchange broker. A lawyer had received \$8,500 for the registration of the mortgage and transfer of title. An additional \$15,000 had been paid to a third party for reasons unknown. Surveillance showed the agent driving one of the foreign cars.

The loans officer had completed the loan application using a photocopy of a driver's license and a copy of the doctor's Social Security card. Examination of the photocopy of the driver's license showed it to be a forgery because the font used to print the card was different from that used on genuine licenses. The birth date on the photocopy was also different from that written on the credit application. The Social Security card was a replacement obtained using information found in the stolen mail.

The fraudsters used an inexperienced young lawyer to prepare the mortgage and title documents required by the bank. The lawyer discovered that the property was indeed mortgage free but that title was registered not in the doctor's name but in the name of his wife. The loans officer instructed the lawyer to register the new mortgage against title in the doctor's name since he was the mortgagor. The fraudster and a woman posing as his wife duly appeared in the lawyer's office and signed the necessary mortgage and transfer documents. The loans officer authorized the line of credit once the lawyer had notified her that the transfer and mortgage documents were in order.

The bank referred the matter to the police and the real estate agent was arrested and charged with fraud. Two foreign cars were seized as the proceeds of crime. The man who impersonated the doctor was charged with fraud but avoided being taken into custody. The bank made a claim against the lawyer for negligence and against a provider of title insurance. The real doctor obtained legal counsel who assisted him in having the fraudulent mortgage and transfer removed from his residence.

Conclusion and Analysis

There is plenty of blame for everyone in this case. Red flags were there right from the beginning. The real doctor and his wife should have acted more quickly. Three months without mail should have raised more questions than it did. Once they discovered their mail was being redirected, they should have taken the actions described in Section 14.4.3, Protecting Personal Information, to see what damage might have been done to their finances. The loans officer should have become suspicious when presented with a photocopy of the applicant's driver's license instead of the real license, which is a document readily available because it is always carried on the person. The request to use the cell phone number exclusively should also have been a sign that there was something wrong with the application; the explanation that the applicant wanted to keep his investments secret from his wife should not have been accepted. The bank seems to have made no effort to check out his credit references despite the fact they contained no account numbers or amounts. The discovery that title to the property was registered in his wife's name and not in his own as he had stated should have been the biggest red flag of all. It is simply not credible that any husband could make that mistake. The lawyer and the loans officer both should have refused to proceed once that had been revealed. The bank should also have been more alert to the fact that the money was not being used for the declared purposes for which the loan had been obtained.

14.5 CORPORATE IDENTITY THEFT

14.5.1 Preventing Identity Theft From Affecting a Business

The identity theft that can affect a business can be committed both on and off site. The key to preventing both types of identity theft from causing harm is to have tighter internal controls. Tight controls at company A mean that it cannot become a source of information that can be used to damage company B. The introduction of Sarbanes-Oxley compliance requirements puts the full responsibility for maintaining internal controls squarely on the

shoulders of the chief executive officer (CEO) and chief financial officer (CFO) at companies regulated by the Securities and Exchange Commission.¹⁴ The CEO and CFO must now certify that the internal controls of their company are sufficiently stringent to guarantee that the financial statements reflect the true financial condition of the company. The external auditor must also be satisfied that the controls are adequate since they must be able to attest to the certification of the CEO and CFO. This means, so far as identity fraud is concerned, the primary responsibility lies with business to put in place tight controls for handling sensitive information. Credit granting institutions will have to introduce stricter verification methods for loan applicants. Of course, not all fraud can be prevented. Determined fraudsters will always attempt to find ways around even the most rigorous system and will sometimes be successful. Sarbanes-Oxley means, however, that the external auditors will be asking harder questions and sloppiness will no longer be tolerated since the reputations of the CEO, CFO, and the auditors are all on the line.

14.5.2 Internal Controls

Corporate Code of Ethics and Privacy Policies

The most important internal control any company can have is a code of ethics that management lives by and enforces since the ethical tone of a company always flows from the top down. This code should be written and provided to every employee in conjunction with education and training programs that emphasize honest business practices. Included in this code should be the company's privacy policies for the handling of client and employee identity information. Privacy policies should be reinforced by privacy audits under the authority of a chief privacy officer responsible for implementing and developing the standard operating procedures for privacy security.

Regulate Information and Personnel With Access

The basic principle is that the amount of information used and the number of persons handling it should be kept to a minimum. Information should be accurate, complete, timely, and relevant to the purpose for which it was collected. For example, is it really necessary to use a SSN to identify clients?¹⁵ Could a simple internal code not be used instead? A similar code should be used for employee identification on parking permits, time sheets, paychecks, and other internal documents. No part of the SSN should be used on passwords or other access codes. If an identity thief were to get hold of the company identifier, the damage would be limited to a company use.

Information should be collected directly from the individual client concerned. The client should know the purpose of the information and be assured that it will be used for that purpose alone. Every client should know that they have the right to review and correct any information kept on them.

Employees should be thoroughly trained in the management of sensitive information, especially in the handling of information requests. They should understand the meaning of

¹⁴ http://www.sarbanes-oxley.com/pcaob.php?level=1&pub_id=Sarbanes-Oxley

¹⁵ Unfortunately, the SSN is relatively easy to steal since Congress has authorized more than 40 required uses of it for identification purposes to get a job, open a bank account or even get a fishing license: <http://financialservices.house.gov/media/pdf/040303pa.pdf>

the information requested and the use of the forms by which it is transmitted. They should know how to extract the requested data from the records so that only that data is transmitted. For example, the careless faxing of a medical record that contains more information than requested could unnecessarily red flag an insurance company to an issue that is none of its concern but could be used against the insured in a claim. Data to be transmitted to an outside user should be carefully vetted by a second person before being sent. Temporary staff should be supervised closely.

Data Security

Client information is only as secure as the system that carries it. Persons should be assigned to data security under the chief privacy officer who are kept up-to-date on technical and legal issues through regular retraining. Data processing systems should be designed to leave a clear audit trail and provide penalties for browsing and unauthorized access. Employees must not leave their computers while sensitive information is on the screen. The use of password-activated screensavers is an additional protection.

Physical access to the electronic and paper files containing sensitive identity information should be restricted to those handling the files. Background checks should be made on all employees with access to sensitive information, including the cleaning staff and temporary workers. Password procedures should be strictly enforced and passwords should be changed frequently. Transmission of sensitive information over the Internet should be strictly controlled through authorizations and encryption. Penetration tests should be conducted regularly on all systems to determine their vulnerability to hackers.

Records Management Policies

There should be strict guidelines about what must be disposed of at the end of the working day and how it must be handled. Unneeded duplicates, photocopying errors, and handwritten notes can all carry information useful to the identity thief looking for just such carelessly discarded material to turn up in the dumpster parked outside the back door. Material scheduled for destruction should be kept in segregated locked containers and shredded under supervision.

Old records must be subject to a secure records management policy that establishes schedules for retention and destruction that meet the statutory, legal, and practical requirements of the industry. Records are evidence for possible use in court and must be created and retained in such a form that ensures their integrity by guaranteeing they have not been subject to tampering whether stored on or off site. Records boxed and ready for shipment to a secure offsite storage facility must be kept in a locked room while awaiting transport. At the expiry of the retention period, documents must be destroyed by a bonded recycling company that provides a certificate of destruction.

Diskettes, tapes and hard drives carrying sensitive information should be erased and then physically destroyed at the end of their retention period. Mere erasure is not enough to destroy electronic information. Sophisticated modern techniques can recover "deleted" files and e-mails and reconstitute information on burned or otherwise damaged drives.

The fax machine can easily become the means of leaking confidential information. A dedicated fax machine should be kept in a supervised area restricted to authorized persons only. Incoming faxes should be distributed to their recipients immediately and not be left lying in a bin. Senders should check the accuracy of all fax numbers with a preliminary

phone call to the recipient just before transmission. This prepares the recipient for the message and prevents unauthorized persons from reading the document at the other end where security might be loose. A cover sheet with the names, addresses, and phone numbers of both sender and recipient should be attached to every transmission. A transmission report should be filed with the original of every sent fax.

Sensitive information should never be left on answering machines or voice mail systems. A dialing error can and has led to sensitive information being left at the wrong phone number. The caller should ask to be called back and the sensitive issue discussed person to person only. There should be a clear policy on who has the right to access incoming voice mails. If management has a right to access the voice mails of an employee when he or she is ill or on vacation, this policy should be made known to all employees.

Sensitive information should never be discussed on cellular or cordless phones because conversations can be picked up by electronic eavesdropping equipment. Cellular phones should never be used for the additional reason that the calls are often taken in the presence of strangers who should not hear third-party private information.

E-mail policy should be equally clear. E-mail messaging is widely used and treated casually because of its apparent impermanence. It is quick and easy to use, can be sent from anywhere to anyone, can carry attached documents, and is used not only to communicate within the business organization but also with outsiders such as customers and suppliers. E-mail messages can be easily accessed by unauthorized persons when in transit between servers or are forwarded by the recipient without the sender's knowledge. Management should have a policy concerning who can use the system and what kinds of information can be transmitted by e-mail and to whom. There should also be a policy on the use of the system for private communication, the retention/purge schedule, copying and forwarding, password creation, and change procedures as well as encryption.¹⁶

Employees Working at Home

The company should have explicit rules for working at home and the use of laptops. Many of the same general rules covering the transmission of sensitive data would also cover the transmission of information between the office and home or a laptop. There should be strict control, however, of the type of information that can be taken home in paper files and created or kept at home in paper or electronic files. The house, apartment, condominium, or other residence must be secure and well protected against fire or other types of peril. Laptops should never be used to handle sensitive information in public places, such as aircraft or waiting rooms. The network connection between the office and remote computers must be secure.

Electronic Monitoring of Employees

Lastly comes the difficult and delicate issue of electronic monitoring of employees at work. If an employer decides it is necessary to monitor employee productivity by listening in on telephone calls or scrutinizing Internet activity, this policy should be made known to all employees and its methods explained. Credit granting institutions must take greater care in the verification of the identity of loan and credit card applicants. Records should be

¹⁶ Michael R. Overly, *e-policy: How to Develop Computer, E-mail and Internet Guidelines to Protect your Company and Its Assets*, (New York: American Management Association, 1999).

checked to see whether an account in the applicant's name already exists. Persons applying for credit cards on the basis of a preapproved credit offer solicited through the mails should be carefully vetted to make sure the applicant is indeed the person to whom the offer was made. The use of an SSN should be supplemented with the name and address on utility bills or tax records. Any request for an address change should be corroborated, especially where it differs from the one on the credit report. Account numbers should be truncated on point-of-purchase transaction slips. Implementation of an account profiling system would red-flag unusual activity and precipitate a notification to the customer.

14.6 CYBER IDENTITY THEFT

Computer security is one of the principal concerns of consumers and businesses alike because the amount of business being done through the Internet is growing so rapidly. Although most e-commerce is business-to-business, retail sales reached an estimated \$46 billion in 2002, up from \$36 billion in 2001. The use of Internet-transmitted identities makes these transactions possible. With more than 600 million computers in use around the world today, of which 180 million are in the United States and the business being done among them growing rapidly, identity theft is certain to grow too.¹⁷

Three major cases illustrate the vulnerability of electronic systems and the devastating results that occur when identity thieves attack.

Teledata Communications Inc. Case Study

Teledata Communications Inc. is a Long Island company providing so-called "credit prompter boxes" to more than 25,000 companies to facilitate quick credit checks to the three principal CRAs mentioned above. By pretending to be a credit-report user such as a bank, a TCI help-desk employee is alleged to have requested reports using the credit grantor's name and access number. About 30,000 credit reports were stolen and sold to a Nigerian fraud ring operating in the New York area. The Nigerians paid \$60 for each report, which the accused split with an intermediary. For the 30,000 reports stolen, the accused and the intermediary would each have received \$900,000.

The thefts were remarkably easy since the workers at the help desk already knew the client codes to perform their duties. Any help-desk staffer could have done what the accused is alleged to have done. This fact raises the issue of employee screening and how successful it can be. Unless an employee has a criminal record, it is almost impossible to determine who will commit fraud since criminologists remain unable to construct the risk profile of a potential workplace fraudster. Experience shows instead that much fraud is committed by trusted employees faced with need or tempted by opportunity. In the TCI case, it seems the accused was approached by the alleged intermediary with the suggestion there was money to be made selling credit reports. Some particular reports were allegedly stolen to order for the

¹⁷ <http://financialservices.house.gov/media/pdf/040303jf.pdf>

Nigerians who provided the accused with names and SSNs acquired through other identity thefts.

The suspect worked for TCI for only 10 months but the thefts went on over a three-year period and even continued after he left TCI and moved to Georgia. He is alleged to have loaded a laptop with names and access codes which he turned over to the Nigerian gang to operate on their own. He kept many override codes for himself, however, which he provided to the gang when companies they were trying to access changed their codes. About one third of the names were pulled *after* leaving TCI because the passwords the accused allegedly downloaded to his laptop remained valid. The scheme came apart when the gang got greedy and tried to request 15,000 reports from the Ford Motor Company.

The 30,000 innocent individuals whose identities were used to steal a minimum of \$2.7 million did not find that their personal information had been taken until many months later when the bills began to come in and credit applications were refused. They are now engaged in the time-consuming and expensive process of reestablishing their good names.

This case reveals a shocking lack of Internet security and supervisory vigilance at TCI as well as the CRAs. Neither TCI nor the CRAs seem to have been aware of the now obvious patterns of requests coming from the suspect and his colleagues. There seems to have been no way of noticing suspicious activity and verifying it with the bank or retailer or whoever initiated the request. There was also no way of notifying the consumer that a request had been received. The FCRA establishes consumers' right to know what is in their reports, but such a right can do nothing to detect an unauthorized request by an alleged credit grantor at the time it is made. As mentioned above, anyone can request a copy of their report and check for unrecognized inquiries. There also seems to have been no way for the CRAs to detect patterns of queries from credit grantors who have received complaints from customers.

TriWest Healthcare Alliance Corp. Case Study

TriWest Healthcare Alliance Corp. is a Phoenix-based Department of Defense contractor supplying managed healthcare services to 1.1 million active and retired U.S. military personnel and their families in a 16-state area around Arizona. During a break-in at one of its offices, computers storing sensitive personal information including SSNs of 500,000 members of military families were stolen from a secure room. Credit card information for 23 clients was also taken. The motive of the theft is unknown.

Although the stolen personal information does not seem to have been used for fraudulent purposes yet, the risk is still hanging over every beneficiary of TriWest. The use of the SSN as an account identifier meant that one of the fraudster's most coveted pieces of information is now available on half a million persons. In this case, the risk of abuse to military records was increased since nearly all such records

are kept under the SSN. The storing of highly sensitive personal medical records in unencrypted databases increased their vulnerability to hackers.

TriWest has responded to the risk of future threats by revamping its IT infrastructure, the details of which have not been made public. TriWest has now set up a fraud alert system with the CRAs that would allow beneficiaries to view their credit reports.

DPI Merchant Services Case Study

The third case is an attack by hackers on DPI Merchant Services, which specializes in the establishment of merchant credit card accounts and payment processing. More than 10 million Visa, MasterCard, and American Express card numbers and expiration dates were stolen. These numbers do not seem to have been used to commit fraud so far. Quick action on the part of the card issuers and the financial institutions seems to have prevented harm to the cardholders.

These three huge and dramatic cases illustrate the vulnerability of personal identity information to hacking and the importance of corporate security in protecting databases. There is much evidence of widespread sloppiness in corporate database security that is an invitation to hackers to steal personal information.

A final example from the manufacturing industry should illustrate the vulnerability of all industries to the effects of sensitive information falling into the wrong hands. Identity thieves do not always just impersonate individuals; sometimes they impersonate companies.

Breaking the Code Case Study

A manufacturing company had established an elaborate system of unique number codes to monitor the movement of replacement automotive parts from its warehouse to customers. A warehouse computer operator familiar with the codes sold some of them to a ring of thieves who wanted to sell the parts on the black market. The stolen codes allowed the thieves to assume the identities of parts retailers and submit orders. Extra parts were added to certain shipments. The drivers, who were in on the scheme, drove to the prearranged drop-off points where the extra parts were unloaded into the thieves' trucks. The thieves then sold them to body shops that asked no questions. The parts manufacturer was defrauded of millions before the scam was discovered by an internal audit that contacted the real clients about the unusually high levels of their orders.

14.7 CONCLUSION

The statistics presented at the beginning of this chapter show that identity theft is a serious and growing problem. New laws recognize identity theft as a distinct class of crime; other new laws attempt to control the flow and use of personal information from the databases where it is gathered. No laws, however, can prevent the occurrence of identity theft when individuals are careless with the custody of their SSNs, credit cards, and personal mail and other carriers of the personal identifiers beloved by identity thieves. Corporations, as seen in the cases described above, are also careless with the custody of the personal information entrusted to them. The belief that hackers are the greatest corporate security risk is an urban myth. Experience is showing that employees entrusted with the access codes for the databases used in the normal course of their daily work are a greater risk than any hacker. There is also all too often a failure to check the backgrounds and establish internal controls and monitoring systems to prevent and catch unauthorized behavior. The personal information provided on job applications is all too often not checked out. Information on credit applications by new customers is also frequently not verified.

It is expected that Sarbanes-Oxley will force corporations to tighten their security systems. Sarbanes-Oxley requires that the CEO be able to vouch for the accuracy and clarity of company financial statements. This, in turn, requires that the CEO ascertain that the internal controls are sufficiently rigorous to control the flow of funds and information within the company to produce reliable financials. The external auditors must review these controls and concur with the CEO before they will lend their signature to the financial statements. This dual review plus the penalties for producing unreliable statements should go a long way to strengthening internal controls, at least among the companies registered with the Securities and Exchange Commission.

Vigilance is going to be the price of avoiding personal or corporate identity theft. Watch your purse or wallet; do not accept preapproved credit-card solicitations; check your bills and mail for anything unusual; be careful when using e-mail or cell phones. Corporations will have to vet job applicants more closely; tighten access to databases; encrypt; stop using Social Security numbers as a filing system; change passwords more frequently and, in general, inconvenience themselves a lot more to ensure the security of their clients' personal information.

14.8 CHECKLIST: DETECTION OF PERSONAL IDENTITY THEFT AND CORPORATE IDENTITY FRAUD

This checklist addresses control issues, taken from the discussion in this chapter specific to personal identity theft and corporate identity fraud.

This checklist is intended for general guidance and information only. Use of the checklist does not guarantee the prevention or detection of fraud and is not intended as a substitute for audit or similar procedures. Those with vital concerns about fraud prevention or who suspect fraud should seek the advice of a competent fraud practitioner.

TABLE 14.1 IDENTITY THEFT CHECKLIST

| Identity Theft Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| A. Protecting Personal Information | | | | |
| <i>A No answer to any of the questions in this section indicates a greater likelihood of potential identity theft and fraud.</i> | | | | |
| 1. Do you carry in your purse or wallet only those documents needed to conduct daily business? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. Do you remove all credit card receipts or other papers carrying your personal identifiers from your purse or wallet at the end of the day? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Do you destroy or file all papers carrying identifiers such as credit card receipts, bank statements or documents carrying your SSN once they have been reconciled? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 4. Do you sign all new cards or replacement cards upon receipt? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 5. Do you cut up or otherwise destroy all old cards? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 6. Is your mailbox secure? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 7. Are all the bills you regularly receive by mail arriving on time? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 8. Are you receiving mail only from entities with which you do business? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 9. Do you have your mail picked up by a friend or held at the post office when you are away? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 10. Do you conduct personal financial business only on a secure land line? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 11. Do you call the intended recipient before sending a fax? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 12. Do you change the PIN on your debit card every time you receive a replacement? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 13. Do you carry the local emergency telephone number to call if your debit or credit card is stolen while traveling? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 14. Do you keep track of all the places where your SSN is on file? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 15. Are you the only person with access to your home computer? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 16. Do you know the sources of all your downloaded software? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 17. Do you have a virus scanner installed? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 18. Is important tax, health, or other information stored on your memory stick or CD-ROM instead of on your hard drive? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 19. Do you send only nonpersonal information by e-mail? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 20. If you work at home, do you use encryption to send client information? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

(continued)

TABLE 14.1 (continued)

| Identity Theft Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|-----|
| B. Corporate Identity Theft | | | | |
| <i>A No answer to any of the questions in this section indicates a need to take action to improve your internal controls.</i> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 1. Are your internal controls Sarbanes-Oxley compliant? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 2. Does your company have a written code of ethics that includes a privacy policy? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 3. Is the privacy policy reinforced by a privacy audit that reviews standard operating procedures for privacy security? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 4. Do you use an internally developed filing system instead of SSNs to identify client or employee files? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 5. Are your employees well-trained to handle information requests? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 6. Are your consultants and temporary personnel closely monitored when they must handle confidential information? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 7. Is all data to be transmitted outside the company vetted by a second person before being sent? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 8. Are your data security personnel kept up-to-date on changing technology and privacy law through regular retraining? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 9. Does your data processing system leave a clear audit trail? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 10. Does your privacy policy provide penalties for unauthorized access or browsing in the databases? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 11. Do you do background checks on employees who will be accessing personal information? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 12. Do you enforce password procedures? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 13. Do you change passwords frequently? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 14. Do you subject your systems to regular penetration tests? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 15. Do you have a strict records management policy in place regarding retention of documents onsite, destruction, and offsite storage? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 16. Do your records meet the evidentiary standards of a court of law? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 17. Can the integrity of your records be guaranteed onsite and offsite? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 18. Are your diskettes, tapes, and hard drives erased <i>and</i> destroyed at the end of their retention period? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |
| 19. Do you have a dedicated fax machine in a restricted area for receiving confidential information? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ___ |

TABLE 14.1 (continued)

| Identity Theft Checklist | Yes | No | NA | Ref |
|--|--------------------------|--------------------------|--------------------------|------------|
| 20. Is there a cover sheet and transmission report for every transmission? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 21. Does your security policy forbid employees from leaving confidential information on answering machines or voice mail systems? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 22. Do you have a policy on who has the right to access the voice mails of absent employees? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 23. Do your e-mail operating procedures include a retention/purge schedule, copying and forwarding policy, password creation, and the use of encryption? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 24. Do you have policies governing the use of company files on laptops or computers at home? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 25. Do your security policies forbid employees from using laptops in public places such as airplanes? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |
| 26. Do you have a policy permitting the monitoring of employees while they work? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | — |

GLOSSARY

Abuse of trust: See *Trust, abuse of*.

Account manipulation, direct: The alteration of computer programs to obtain direct but unauthorized access to account files for the purpose of manipulation.

See also: *Computer crime*.

Account, nominee: A bank or trust account set up under an alias, an assumed name, a company name, a corporate name, or a blind trust.

Account, posting improper credits to: Concealing a fraud involving the sales and collection cycle. In this scheme, an employee posts credit memos or other noncash items, for example, a sales return or writeoff, to the customer account from which the funds were diverted.

See also: *Sales and collection cycle*.

Accounts receivable, misappropriation of: The diversion of payments received from customers. An employee may open a personal bank account with a name similar to that of the customer (for example, Acme Inc. rather than Acme Company). Customer payments can then be taken by the employee and deposited into the employee's bank account.

See also: *Sales and collection cycle*.

Acquisition and payment cycle: The sequence of accounting procedures that address the procurement of and payment for all goods and services except payroll and capital acquisitions.

See also: *Capital acquisition and repayment cycle; Payroll and personnel cycle; Procurement fraud*.

Advance-fee fraud: A scheme in which assurances of some future benefit (for example, a loan) are given to the proposed victim in return for a payment described as an advance service fee or other advance good-faith deposit (often falsely described as a "returnable" deposit).

Typical victims of advance-fee schemes are business people who cannot obtain banking services or credit from customary sources. They pay "deposits" or "fees" to others on the promise that the perpetrator will arrange loans or credit for them.

See also: *Commercial crime; Finance fraud*.

Advertising, false and misleading: Use of untrue or deceptive promotional techniques resulting in consumer fraud.

Victims are consumers who rely on the false or misleading advertising or promotion. Noteworthy practices include the following:

1. Advertising as a "sale" item an item that is actually at the regular or higher price
2. Misrepresenting the size, weight, volume, or utility of an item

3. Making false claims about an attribute that a good or service does not in fact possess
4. Misstating the true costs of a good or service through the use of confusing payment provisions or otherwise

See also: *Bait and switch; Consumer fraud.*

Allegation: In litigation, a formal assertion, claim, declaration, or statement of a party to an action, made in a pleading, setting out what that party expects to prove. In a nonlitigious situation, a concern backed by evidence that a party has committed fraud.

Anti-trust offense: An offence consisting of one or more of the following:

1. Combinations in restraint of trade, price fixing, predatory pricing or other schemes for the purpose of unlawfully driving competitors out of business.
2. Agreements among competitors to share business according to some agreed formula, for example, bid-rigging conspiracies and discriminatory pricing agreements.
3. Domination of a business area by one or a few enterprises.

Victims of anti-trust offenses are businesses and purchasers of goods or services who pay prices higher than they would if the offenses were not committed.

See also: *Price fixing; Procurement fraud; Trade, restraint of.*

Appraisal, false: False and inflated appraisal used to support a loan for an amount larger than would be granted if the true value of the property were known.

See also: *External fraud; Land fraud; Real estate fraud.*

Arson for profit: Intentional burning of a house or property whether one's own or another's to collect the payment from the insurance company on a claim for the loss.

See also: *Commercial crime; Insurance fraud; Property-insurance fraud.*

Auto-repair fraud: A form of consumer fraud involving maintenance services to automobiles.

Auto-repair fraud falls into several categories, including the following:

1. Overcharging for labor or parts or use of shoddy or substandard parts
2. Failure to perform promised services or repairs
3. Charging for services not performed or parts not used
4. Performing services or repairs that are unnecessary or unwanted

See also: *Consumer fraud; Repair fraud.*

Backdooring: Sale of shares by "friends" of a promoter in a stock market manipulation scheme as the price rises but contrary to their agreement to sell only on his or her instructions.

See also: *Distribution network, setting up; Stock market manipulation; Warehousing.*

Bagman: The person who carries cash as a bribe to the recipient.

Bait and switch: A form of consumer fraud involving misleading advertising. A bargain (the *bait*) is advertised as an inducement to lure customers to the store where they are presented with a similar but higher priced item (the *switch*). Thus, the advertisement does not constitute a bona fide offer for sale of the merchandise in question. This scheme may be used because the advertised item is not available or is in short supply. The sales staff may try to prevent the customer from purchasing the advertised item by directing him or her to higher priced merchandise by criticizing the advertised goods.

See also: *Advertising, false and misleading; Consumer fraud.*

Banking fraud: Violations by insiders or customers of banks, trust companies or credit unions. Insider violations generally involve embezzlement or self-dealing whereby insiders lend money to themselves or to businesses in which they have an interest, take bribes to make loans or refrain from collecting loans, provide special favors to outsiders or defalcations from customer accounts. Violations by outsiders would include submitting false financial statements to induce a bank to make a loan, the use of fraudulent collateral, check kiting, and similar offenses.

Victims of banking fraud are bank depositors and shareholders, creditors, the federal government as the insurer of deposits, and surety companies that bond bank employees and officers.

See also: *Check kiting; Collateral fraud; Commercial bribery; Trust, abuse of.*

Bankruptcy fraud: Fraud against parties to a bankruptcy. Victims are usually creditors and suppliers of the failed or failing business, although managers of fraudulently operating businesses can also victimize silent partners and shareholders. The following are the two major kinds of bankruptcy fraud.

1. *Fraudulently planned bankruptcy.* The assets, credit, and viability of a business are purposely and systematically used to obtain cash, which is then hidden.
2. *Fraudulent concealment or diversion of assets in anticipation of filing for bankruptcy.* This prevents the assets from being sold for the benefit of creditors.

Planned thefts and fencing activities may be associated with either kind of bankruptcy fraud as a means of diverting assets for the purpose of converting them to cash.

See also: *Finance fraud.*

Bid rigging: A conspiracy among contractors to set the price or terms of a contract for the purpose of raising the cost to the purchaser.

See also: *Commercial crime; Procurement fraud.*

Biometrics: A method to ensure that only authorized people have access to computer systems, restricted areas, and/or equipment. It can include the checking of fingerprints, iris recognition, and hand geometry.

See also: *Computer-access control.*

Blowing off: The sale of unusually large amounts of stock during a stock market manipulation (also referred to as *blowing a position*).

See also: *Stock market manipulation.*

Boiler room: A place of business used to promote fraudulent sales of securities, charitable donations, lotteries, and so on, through telephone solicitation. Salespeople working from call lists ask victims to buy a particular product or service. They call both locally and long distance, use glibly scripted presentations and work on high commissions. Legitimate enterprises, especially charitable institutions, often mistakenly use the services of these operators and, as a result, rarely see much of the money collected in their names.

See also: *Charity and religious fraud; Securities fraud.*

Borrower misapplication of funds: Loan fraud in which a borrower, with little or no personal risk in the collateral, misapplies borrowed funds.

See also: *Loan or lending fraud.*

Bundling and unbundling claims: See *Claims, bundling and unbundling.*

Business-opportunity fraud: One of the most common but varied forms of fraud, in which the victim is offered the opportunity to make a living or to supplement his or her income by going into business, full- or part-time, or by purchasing a franchise or equipment to manufacture some item, sell merchandise, or perform some service.

Victims are generally individuals with a small pool of savings, who are enticed by the prospect of independence and/or income.

This kind of scheme ranges from being a total sham to an “opportunity” whose promised return is highly illusory. Work-at-home merchandising schemes, such as selling knitting machines or raising mink, or the sale of distributorships in cosmetics, special rug cleaning processes, and so on, are common examples of the kinds of opportunities offered in this form of fraud. The opportunity presented by the fraudster often includes the promise of “guaranteed” markets for the goods or services to be produced. This kind of fraud can turn into a pyramid scheme if victims are induced to enlist other prospective victims.

See also: *Franchise fraud; Pyramid scheme; Self-improvement scheme.*

Capital acquisition and repayment cycle: The sequence of accounting procedures whereby capital items are purchased and paid for. This process is sometimes referred to as the *financing cycle*.

See also: *Acquisition and payment cycle; Procurement fraud.*

Casualty-insurance fraud: Claims for staged accidents and false claims for real accidents submitted under a casualty-insurance policy covering personal injuries and property damage that may be sustained as the result of an accident.

See also: *Claim, accident with false; Insurance fraud; Personal-injury insurance fraud.*

Chain-referral scheme: Fraud in which the victim is induced to part with money or property on the representation that he or she will make money by persuading others to buy in.

First-tier victims usually believe that those they involve in the scheme (second-tier victims) will make money. Since second-tier victims can only make money by involving third-tier victims and so on, the scheme must eventually collapse. Generally, only the fraudster makes money; few first- or second-tier victims (especially if they are honest) have a sufficient number of participating friends and acquaintances to come out whole.

One common form of chain-referral scheme is the chain-letter. A more sophisticated version is the *pyramid scheme*. Here, the victim is sold a franchise to sell both merchandise and other franchises. Profits are promised to come from both merchandise sold and commissions or “overrides” on merchandise sold by any second- or later-tier victims who buy a franchise. The profits appear, therefore, to be in selling franchises rather than in selling merchandise. These schemes ultimately collapse under their own weight.

See also: *Merchandising fraud; Pyramid scheme*.

Charity and religious fraud: Fraud arising out of the fund-raising activities of charitable and/or religious groups.

Almost anyone can be the victim of this type of fraud often without knowing it. Even if the victim may later suspect the fraud, however, his or her individual loss may be so small that there is little desire to pursue the matter. The following two kinds of fraud are common.

1. *Fake charity.* Money is solicited for a nonexistent charitable organization or cause or for a charitable front set up to defraud donors.
2. *Misrepresentation of association with a charity or religious group.* Individuals solicited for donations to a legitimate charity or religious organization are not aware that most of the money collected is used to cover the cost of professional fund raisers and/or administrative overhead expenses, rather than the charity. (This is a gray area in law, since professional fund raisers perform a legitimate service for which they may properly and legally be compensated).

In some instances, charitable organizations themselves are the victims of con artists who use them as a front to keep the largest part of the money collected. In other instances, the solicitation falls into a gray area where otherwise legitimate charities cover up the fact that most of the money collected goes to salaries and fund raising.

See also: *Boiler room; Sham, corporate*.

Check forgery: The copying of a check or some of its components (most often the signature) onto a fraudulent check to induce a financial institution to believe it is a bona fide check.

See also: *Check fraud*.

Check fraud: A general term for the attempted or actual negotiation of a bad check at a financial institution. Kinds of fraud in this category include: a false deposit made by a new customer, forged, altered or stolen check and check kiting.

See also: *Check kiting; New-account fraud*.

Check kiting: A kind of fraud against banks that depends for success on the length of time the banking system takes to clear checks. The most common form of check kiting involves at least two bad checks used intentionally to temporarily obtain credit. In the simplest case, the fraudster must open two bank accounts, each of which contains little or no money. The accounts are often established at different banks in different cities in order to create and take advantage of a longer clearing period. A check is then written on one account for deposit in the other. This process may be repeated within the next day or so to build up the amount the fraudster needs to carry out the scheme. Money is then withdrawn

from one of the accounts before the first checks are cleared. The process can continue with multiple accounts in different cities and a constant stream of deposits and withdrawals.

Banks are victims of check kites. When first discovered, check kites often appear to have cost the bank far more than they actually have after all transactions have been analyzed, since hundreds of thousands of dollars in checks may have been circulated to steal only a few thousand dollars. In some instances, however, massive amounts have been stolen. In many cases, businesses employ check kites when they cannot get loans from banks to tide themselves over a temporary business crisis and intend to (and often do) put the money back into the accounts before the check kite is discovered. In these instances, the bank has been fraudulently induced to unwittingly grant what amounts to an interest-free loan. This form of fraud is becoming increasingly difficult to perpetrate because of the speed of electronic clearing.

See also: *Banking fraud; Check fraud.*

Churning: The buying and selling of stock for a client by a broker solely to generate commissions rather than to meet the client's investment objectives.

Claim, accident with false: An individual involved in a real accident later exaggerates the seriousness of his or her personal injuries in order to collect an excessive insurance claim.

See also: *Casualty-insurance fraud; Insurance fraud.*

Claim, false or fraudulent: Fraudulently written claim for payment for goods or services not provided as claimed. False claims may involve activities such as the following:

1. Presentation of a bogus claim or claimant; for example, ghost payrolling
2. Misrepresentation of the qualifications of an otherwise ineligible claim or claimant, for example, welfare fraud
3. Misrepresentation of the extent of payment or benefits to which a claimant is entitled, for example, overtime-pay fraud
4. Claims for reimbursement for goods and services allegedly provided to nonexistent recipients, for example, health care fraud, by service providers

The false claim will carry all the trappings of a legitimate claim and is most successfully undertaken by individuals with a thorough knowledge of the system being defrauded. The false claim will sometimes involve the cooperation of executives or officials of the entity to which the claims are submitted.

See also: *Commercial bribery; Ghost employee; Government-benefit program, fraud against; Insurance fraud; Health-care fraud; Welfare fraud.*

Claims, bundling and unbundling: The practice of physicians or clinics billing a patient's health insurance provider (government or private carrier) separately for medical services performed at the same time.

See also: *Health-insurance fraud.*

Cleaning up the market: Buying up as many shares of a company as possible when they become available. (Also referred to as *taking out the market*)

Collateral fraud: The holding, taking, or offering of defective collateral pursuant to a financial transaction. In many instances collateral fraud will be related to bank loan transactions. Beyond this, however, this kind of fraud may be encountered in connection with any transaction in which defective security is provided, such as security for private loans, non-existent accounts receivable sold or pledged to factors, and the like. In some cases, collateral used as security may not belong to the person offering it. The collateral could be stolen (for example, securities), borrowed, or already subject to an undisclosed lien or other encumbrance. Alternatively, there may be some gross misrepresentation as to the collateral's value.

Collateral frauds are typically violations of federal fraud and banking laws. There may be elements in banking or corporate violations involving self-dealing, such as when a bank officer makes a loan knowing the collateral is bad. Collateral frauds may also be involved in organized crime activities, for example, obtaining proceeds of stolen securities not by an attempted sale, which would precipitate discovery when title was transferred, but by their use as collateral for loans.

See also: *Banking fraud*.

Collusion or collusive fraud: A private agreement in which several parties plan to commit fraud against another party or organization. The group of fraudsters could be as few as two people and could include parties who are internal or external to an organization, or both. For example, collusion occurs if an internal fraudster helps an external fraudster commit a crime in return for a secret commission, kickback, or bribe.

See also: *External fraud; Internal fraud*.

Commercial bribery: A form of insider fraud or abuse of trust in which an employee or officer of a business, charitable organization, or government entity is given a bribe or some other valuable consideration to induce the employee or official to make a purchase, grant a contract, or provide some special privilege (such as a zoning variance or license).

See also: *Trust, abuse of; Procurement fraud*.

Commercial crime: A white-collar crime committed by an individual or group of individuals in a company for the benefit of that company and, indirectly, themselves.

See also: *Economic crime; External fraud; Procurement fraud; White-collar crime*.

Compartmentalization: A restriction that limits computer users' access to the specific files and programs for which they have a job-related requirement.

See also: *Computer-access control*.

Computer-access control: A series of controls used to help ensure that only authorized persons are permitted to access computer systems. Controls include passwords, compartmentalization, the use of biometrics, one-time passwords, automatic log-off, time-day controls, dialback systems, requests for random personal information, and Internet authentication.

See also: *Biometrics; Compartmentalization; Computer crime; Dialback systems; Internet authentication; Information, random personal; Controls, time-day*.

Computer crime: A crime in which a computer is used either to commit a crime or as the target of crime. Crimes committed using a computer may include embezzlement, larceny, fraud, forgery, and counterfeiting. Crimes that target computers may include sabotage, vandalism, electronic burglary, wire tapping, and gaining illegal access. The most common forms of computer crime involve the manipulation of inputs and outputs.

See also: *Computer-access control*.

Computer fraud: Fraud arising out of the increasing use of the computer to maintain business and government records, such as those relating to inventories, accounts payable and receivable, and customer and payroll records. Most computer frauds are really traditional kinds of fraud that are committed by using a computer to alter electronic records rather than manually altering paper records. True computer frauds do exist, such as those involving unauthorized changes to a computer's programming, but these are relatively less common and are most often committed by technical computer people.

See also: *Computer crime*.

Computer intrusion: Unauthorized access to another organization's computers.

See also: *Computer-access control; Computer crime*.

Consumer fraud: A deception in the marketplace involving sellers' misrepresentations to buyers. Victims are consumers of all kinds, individual and institutional, public and private. Common forms of consumer fraud include the following:

1. Sale of useless goods or services, represented as beneficial, for example, "miracle face creams"
2. Misrepresentation of product performance, benefits, or safety
3. False and misleading advertising
4. Failure to service items after sale, including reneging on warranties
5. Repair fraud
6. Hidden charges with respect to financing, necessary follow-up services, and so on
7. Weights and measures violations

See also: *Advertising, false and misleading; Auto-repair fraud; Bait and switch; Chain-referral scheme; Merchandising fraud; Repair fraud; Weights and measures fraud*.

Controls, time-day: Controls that restrict access to computer systems to those times when employees are supposed to be on duty. An extension of this concept uses automated time-clock systems to deny access; the system reports a violation if access is attempted when an employee is shown as not being authorized to be present.

See also: *Computer-access control*.

Copyright piracy: The use of another's copyright or other business rights for profit without the legal right to manufacture or copy the product.

See also: *Commercial crime*.

Corruption, public or official: An abuse of trust violation involving commercial bribery, collusion with bid-rigging, avoidance of the competitive process in connection with the purchase of goods and services by government entities, self-dealing in connection with government purchases, or grants of franchise to use public property and real estate.

Most public corruption has its parallel in the private sector. Thus conflict of interest is the public equivalent of insider trading.

See also: *Commercial bribery; Procurement fraud; Government-benefit program, fraud against; Trust, abuse of.*

COSO framework: A framework for internal control created by the Committee of Sponsoring Organizations of the Treadway Commission published in 1992 as *Internal Control—Integrated Framework*. The SEC final rules for internal control over financial reporting accept the COSO framework as compliant with Sarbanes-Oxley. The framework defines internal control as: “a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.”

Coupon-redemption fraud: Cheating manufacturers or merchandisers who promote sales of their products by offering coupons that return part of the purchase price when the products are purchased.

Many manufacturers, primarily in the food business, place coupons in newspaper and magazine ads offering, for example, “15 CENTS OFF” if the product is purchased. The grocery store is supposed to redeem the coupon, and will customarily receive a service charge of about 5 cents for handling the transaction. Frauds are committed against the manufacturers by amassing large numbers of coupons and submitting them to manufacturers without any bona fide purchases of the products.

This kind of fraud involves two basic steps, as follows.

1. Collect coupons.
2. Process the coupons for redemption.

Coupons can be collected by going through large numbers of old newspapers and magazines; sometimes this is done by trash collection or waste disposal companies as a side venture. Processing for collection requires the collaboration of retail merchants and is most efficiently done with the cooperation of officials of food retail chains.

See also: *Commercial crime.*

Credit-card fraud: Fraudulent application for, extension, and use of credit cards. Victims are the issuers of the credit cards. Common credit card abuses include the following:

1. Use of stolen credit cards
2. False statements in the application for a credit card, including application under a false name

3. Making a purchase using a legitimate credit card with no intention of paying
4. Manufacture and use of fake credit cards
5. Electronic swiping of a card to capture card data later used to make unauthorized purchases

See also: *Banking fraud*.

Credit-card receipt, altered: A fraudulent increase in the amount recorded on a credit-card receipt.

See also: *Sales and collection cycle*.

Credit, false application for: False information on a credit application including overstated assets, nonexistent assets, understated or omitted liabilities, inflated revenue, and understated expenses.

See also: *External fraud; Loan or lending fraud*.

Credit rating fraud: Fraudulent application for, extension, and use of credit. Victims are generally the providers of credit. Common credit-related schemes include the following:

1. Sale of good credit ratings to high-risk applicants
2. False statements in credit applications
3. Creation of false credit accounts for the purpose of theft

The *modus operandi* of these schemes varies widely. Recently, employees of credit rating organizations have altered credit ratings for payment, sometimes using computer techniques. The creation of false financial statements is another common method. On a smaller scale is a fraud that operates like shoplifting—opening a charge account with false information in order to purchase and immediately take away goods.

See also: *Loan or lending fraud*.

Customs duty fraud: The false understatement by an importer of the value of goods to be imported to reduce the amount of customs duty paid to the government of the country into which the goods are imported.

See also: *Commercial crime; Tax and revenue violation*.

Debt-consolidation or adjustment swindle: The purported bundling of a debtor's assets and income to repay all creditors over a period of time in order to keep creditors from pressing for the immediate payment of all sums due.

There are legitimate private agencies that provide these services and they have similar workout procedures available after filing for bankruptcy.

The usual *modus operandi* is to use heavy television and newspaper advertising to lure debtors into signing up. Sometimes the perpetrators will talk creditors into waiting for their money; in other instances, they falsely tell the debtors they have been able to call the creditors off. They then take the debtors' assets and a portion of their weekly or monthly earnings, paying themselves first and (usually only after they have their entire "fee") dole out the remainder to creditors. Frequently, creditors receive little or nothing and the debtors are left minus their fees and still in debt.

See also: *Finance fraud*.

Dialback systems: A computer security system that accepts a user identification (ID) and password then hangs up and dials a predetermined number. The system is only accessible by dialing in from a set location.

See also: *Computer-access control*.

Differential association: A theory established by Edwin H. Sutherland that explains why crime is committed. There are ten principles to his theory which, in summary, asserts that a person becomes a criminal because of an excess of definitions favorable to violation of the law over definitions unfavorable to violation of the law.

Diploma mill: An outlet that grants diplomas to all people who apply for them in exchange for a hefty fee. Because the diploma mill is not accredited, the diplomas are worthless.

See also: *External fraud; Self-improvement scheme*.

Directory-advertising fraud: Fraud arising from the selling of printed mass advertising services. The following are the two basic kinds.

1. Impersonation schemes involve con artists who send bills to business enterprises resembling those customarily received; for example, purported bills from the phone company for yellow page advertising, with directions to make checks payable to entities whose names are similar to legitimate payees of the bills.
2. Another kind of scheme involves promising that advertising will appear in a publication distributed to potential customers even though distribution will actually be limited to the advertisers themselves, if the directory is printed at all.

See also: *External fraud*.

Disclosure Controls and Procedures: Defined under SEC Rules 13(a)-15 (e) as procedures:

“designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits under the Act is

- Recorded
- Processed
- Summarized, and
- Reported

within the time periods specified in the Commission’s rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by an issuer in the reports that it files or submits under the Act is accumulated and communicated to the issuer’s management, including its principal executive and principal financial officers, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure.”

Distribution network, setting up: A term used in stock market manipulation. The network is set up with the promoter as its head and several distributors located in cities with facilities for trading the stock in question. Each distributor has access to a brokerage house’s sales force which in turn has access to the floor traders who will actually be

executing the trades. Via this network, the promoter has control over trading in the subject stock.

Double-indemnity fraud: The report by a beneficiary of a life insurance policy of a natural death as having been accidental in order to obtain more than the face value of the policy.

See also: *Insurance fraud; Life-insurance fraud.*

Double-pledging collateral: Fraudulently pledging the same collateral to different lenders before the related liens are recorded and registered.

See also: *External fraud; Land fraud; Real estate fraud.*

Down payments and retainers, absconding with: A fraud in which the fraudster absconds with money obtained from the victim in advance by the false promise to provide goods or services.

Economic crime: A crime that is similar to white-collar crime but broader in its scope in that it includes violent crimes committed by people without any particular occupational status.

See also: *White-collar crime.*

Economic espionage: An act in which business secrets are stolen for the benefit of another organization.

Economic extortion: A crime in which a financial benefit is sought or obtained through intimidation or persistent demands.

See also: *Commercial crime.*

Embezzlement and fiduciary fraud: The conversion to one's own use or benefit of the money or property of another, over which one has custody with which one has been entrusted or over which one exerts a fiduciary's control. Victims include institutions, businesses in general, pension funds, and beneficiaries of estates managed by fiduciaries.

See also: *Banking fraud; Insider trading; Loan or lending fraud; Trust, abuse of.*

Employment-agency fraud: Fraudulent solicitations of money or fees in order to find employment for, to guarantee the employment of, or to improve the employability of another. Victims are generally individuals seeking jobs or hoping to improve their skills in order to obtain better paying jobs. Variations of employment-related fraud include the following.

1. *Phony job agencies.* An agency solicits advance fees in order to find employment for the victim, when in fact, the service is neither provided nor is it intended to be.
2. *Job training fraud.* Money is received from victims to train them for specific employment. The training is not supplied; "guaranteed" job opportunities on completion of training do not materialize; the training is misrepresented as being "certified" or "recognized" by employers when it is not.

Energy-crisis fraud: Fraud arising out of the sale of goods or services related to energy or fuel use, saving, and production.

Victims are generally consumers interested in saving on energy costs. Energy schemes include the following.

1. *Merchandise schemes.* Sale of worthless or bogus items that do not deliver the specific benefits promised or the degree of benefit promised; for example, carburetor gadgets to save gasoline or phony solar heating systems. Often, these kinds of fraud occur because of the novelty of the items involved combined with the naiveté of the victims.
2. *Weights and measures violations.* Short weighing or measuring fuels to customers; for example, the manipulation of gas pump measuring devices or the misrepresentation of fuel types by changing octane ratings on fuel pumps.
3. *Distributors' discriminatory allocation of fuel.* Distribution to subdistributors and retailers, in consideration of commercial bribes to distributors' executives or special payments to companies with the power to make distribution, in the form of under-the-table payments or required purchases of other items, in violation of antitrust or other laws.

See also: *Antitrust offense; Commercial bribery; Merchandising fraud; Weights and measures fraud.*

Environmental abuse: Business behavior that can harm the environment. The legal system considers these acts to be crimes. The two major practices are pollution and the misuse of natural resources. Businesses commit these crimes to avoid the costs associated with compliance.

See also: *Commercial crime; Pollution and environmental protection violation.*

Ethics: Principles or standards of human conduct.

Evidence: Oral, written, or physical material presented as proof in a trial or other hearing for the purpose of convincing the trier of fact (that is, judge, jury, mediator, arbitrator, and so on) of the truth of the facts and allegations.

Expense report, false: Expense report containing any combination of overstated, fictitious, or duplicated items prepared and submitted for reimbursement to an employee.

See also: *Acquisition and payment cycle; Claim, false or fraudulent.*

Expert witness: A person possessing specialized knowledge acquired through experience, education, or training. Expert witnesses can provide opinions in court, whereas lay witnesses can only provide evidence regarding their physical experiences—what they saw, smelled, heard, tasted, or touched.

External fraud: Fraud committed against an organization by arm's-length parties.

See also: *Commercial crime; Internal fraud.*

Fictitious company, payment of invoices to: The embezzler establishes a fake entity (often with a post-office box for an address, and a name similar to that of a legitimate company) and gets the fake entity entered into company records as a legitimate vendor. The embezzler then produces invoices for the fake vendor, has them processed in the accounts payable system, and pockets the payments made to satisfy the fake invoices.

See also: *Acquisition and payment cycle; Procurement fraud; Sham, corporate.*

File-maintenance instructions, failure to enter: Failure to input information into the computer system because of an intention to deceive. For example, deliberately not

updating computer files when an employee has left the firm and not removing that employee from the payroll records. This kind of "omission" might be for the purpose of creating a ghost employee.

See also: *Payroll and personnel cycle*.

File-maintenance transactions, phony: Performing file-maintenance transactions such as changing a customer's address or adding a new employee to the payroll. These transactions can lay the groundwork for any number of frauds, for example, the use of ghost employees to embezzle funds.

See also: *Computer crime; Payroll and personnel cycle; Sales and collection cycle*.

Final Rules: See *Securities and Exchange Commission Final Rules*

Finance fraud: One of several kinds of fraud, including the following:

1. *False mortgage security.* The mortgage loan is larger than the underlying value of the property secured by the mortgage.
2. *Advance fee fraud.* The victim pays an up-front finder's fee in exchange for a promise to receive an advance on a loan.
3. *Debt consolidation scheme.* A fraudulent debt consolidation agency makes money by organizing the debtors' affairs and collecting and retaining most, if not all, the money handled on the debtor's behalf.
4. *Bankruptcy fraud.* This includes fraudulent conveyances, concealed assets, asset stripping, or fraudulently planned bankruptcy.

The victims of financial fraud are generally financial institutions.

See also: *Advance-fee fraud; Bankruptcy fraud; Commercial crime; Mortgage security, false*.

Financial-statement auditing: A methodology used by auditors to evaluate the accuracy, timeliness, and completeness of recorded business transactions through sampling, confirmation, and analytical techniques.

Financial statement, false: False information created by upper-level managers with intent to manipulate data to enhance reported profitability and thereby earn higher bonuses, impress supervisors or executives, impress stockholders or lenders, or simply to comply with the goals set by senior management. The methods of creating a false financial statement include overstating revenue, overstating assets, understating expenses, understating liabilities, and misrepresenting information in the notes to the financial statements.

See also: *Commercial crime; Securities fraud; Statement, false*.

Forensic: Material that is used in, or suitable to courts of law.

See also: *Forensic accounting; Forensic standard*.

Forensic accounting: An accounting subdiscipline that investigates alleged financial wrongdoing or damage for the purpose of providing evidence to meet the evidentiary standards of the courts. The forensic accountant also supplies expert testimony for arbitration hearings, mediation, and other business dispute resolution processes.

See also: *Forensic; Forensic standard*.

Forensic standard: The evidentiary test of the courts. Evidence must meet the standards of court admissibility and be able to withstand cross examination.

See also: *Forensic; Forensic accounting.*

Franchise fraud: Fraud in the sale or service of a franchise.

Franchise fraud generally occurs in one or more of the following ways.

1. The franchisor has no intention of honoring any of its obligations; that is, the “franchise” is a complete ruse to acquire the victim-franchisee’s initial investment money.
2. The franchisor fails to provide promised goods or services essential to the success of the franchise.
3. The franchisor makes success for the franchisee either difficult or impossible by allowing too many franchises in a given market area.
4. The franchisor has misrepresented the market or demand for goods or services central to the franchise, or has misrepresented the level of skill needed to realize franchise profitability.

Item 1 is outright fraud, while items 2 to 4 represent variations that range from fraud to shady dealing and the failure to fulfill contractual obligations.

See also: *Business-opportunity fraud; Chain-referral scheme.*

Fraud: Criminal deception intended to financially benefit the deceiver. The deception must be criminal in nature and involve financial benefit.

See also: *Commercial crime; External fraud; Internal fraud.*

Fraud auditing: A methodology used by fraud auditors to find transactions that differ from the normal series of transactions and suggest irregularities that could be fraudulent.

See also: *Financial-statement auditing.*

Fraudulent disbursement: The theft (embezzlement) of a company’s cash by an employee, for example, by using company checks either to withdraw cash directly or to pay personal expenses.

See also: *Acquisition and payment cycle.*

Front-end fraud: The improper direction given to a company’s customers to take their business elsewhere thereby depriving the company of profits it would otherwise have earned.

See also: *Sales and collection cycle.*

Funeral fraud: A class of guilt-inducement fraud that relies on the emotional stress of victims who have lost or are about to lose loved ones through death. Victims are the relatives or friends of the deceased or terminally ill.

Funeral-related fraud often takes the form of consumer and merchandising fraud and generally involves one or more of the following practices.

1. *Relying on the guilt or anxiety of bereaved relatives.* Victims are persuaded to contract for unnecessary or unduly elaborate funeral services or merchandise.
2. *Billing for funeral expenses to include charges for services not performed.* The fraudster relies on the victim's grief to cloud his or her memory as to whether or not a particular service was performed and/or to preempt the victim's challenge of the bill for payment.
3. *Misrepresentation.* Victims are told that certain goods or services are required by law when they are not.
4. *Fraudulent contracts.* The victim is sold and pays for the future provision of goods or services the fraudster has neither the intention nor the capacity to provide; for example, the sale of nonexistent cemetery plots.

See also: *Consumer fraud; Guilt-inducement fraud; Merchandising fraud.*

Generic risk factors: Risk factors within the control of the entity protecting itself but outside the control of potential perpetrators.

Ghost employee: A payroll fraud in which the embezzler enters the name of a fictitious employee into the payroll system and receives the resulting payroll check. Fictitious employees are commonly referred to as "ghosts."

In one variation of this scheme, the names of individuals whose employment has terminated are kept on the payroll for several pay periods after they leave their jobs. The embezzler then receives the paychecks for the former employees. In another variation of the ghost payroll, the fraudster develops an overtime-pay scheme in which false claims are made for overtime work performed by bona fide employees.

Victims are generally public and private entities responsible for honoring payroll claims. Often, the ghost payroll is a device used to defraud government programs designed to provide employment for the unemployed or disadvantaged. This is closely related to welfare and unemployment insurance fraud. This device is used in cost-plus contracts to cheat government entities or by managers of sub-units in private enterprises to steal from their parent organizations.

See also: *Claim, false or fraudulent; Government-benefit program, fraud against; Payroll and personnel cycle.*

Government-benefit program, fraud against: Unlawful application for and receipt of money, property, or benefit from a public program designed to confer money, property, or benefit under specific guidelines.

Victims are federal, state, county, and municipal governments; their taxpayers; and qualified, intended beneficiaries of the programs. Typical kinds of fraud suffered by government programs include the following:

1. The misrepresentation of applicants' qualifications concerning program eligibility; for example, welfare received by ineligible people
2. False billing or vouchering for services not rendered or for nonexistent beneficiaries; for example, physician's claims under provincial health programs for patients not treated or for specific treatments not provided

3. Inflated billing, vouchering, or claiming that charges public programs more than the allowable costs; for example, housing fraud in which the cost of construction is inflated so that the builder or owner receives more than the total cost of land and buildings and avoids making the investment required by law and administrative guidelines
4. Embezzlement by employees or officials misusing their custodial or fiduciary positions to convert public funds, property, or benefits to their own use; for example, licensed dispensers of food stamps converting them to their own use
5. Use of properly obtained funds in which money, property, or benefit are used for purposes other than those for which they were intended; for example, the use of student loans for purposes other than education

See also: *Claim, false or fraudulent; Embezzlement and fiduciary fraud; Health-care fraud; Statement, false; Welfare fraud.*

Guilt-inducement fraud: Fraud perpetrated by inducing guilt or anxiety in the victim concerning a child, parent, spouse, or friend. Victims are persuaded to part with money or property in the belief that they are atoning for any “shortcomings” or fulfilling “obligations” toward another.

Guilt inducement is used in many kinds of fraud. A few examples are the following.

1. Encyclopedia salespeople induce victims to sign purchase contracts by suggesting that their children will fail at school unless the books are bought.
2. Children of deceased parents are persuaded to purchase elaborate and unnecessary funeral arrangements for fear of not giving a “decent” burial. Victims are urged to believe that their failure to make these purchases implies a lack of affection or respect for the deceased.
3. Unnecessary and imprudent expenditure for life insurance is induced by the suggestion that failure to do so implies a lack of care for spouse and children.
4. Self-improvement merchandise and facilities are marketed to victims on the basis of guilt inducements such as, “You owe it to your spouse to be as [lovely, manly, successful, or whatever] as you can be” or “You can only be a failure if you fail to take advantage of opportunities to improve your [looks, job, speaking ability, or whatever].”

See also: *Funeral fraud; Self-improvement scheme.*

Health-care fraud: This term covers numerous types of fraud in the health care industry, for example; marketing drugs without adequate testing or for which the test results have been falsified.

See also: *Commercial crime; Health-insurance fraud; Medical fraud.*

Health-insurance fraud: There are several forms of health insurance fraud, for example, mobile labs, bundling or unbundling claims, or collusion between an insured and a provider to claim health insurance for his or her own benefit.

See also: *Claims, bundling and unbundling; health-care fraud; insurance fraud.*

Home-repair or home-improvement fraud: Fraud arising from the provision of goods and services in connection with the repair, maintenance, or renovation of housing units.

Victims are generally homeowners but may also include public agencies or programs that subsidize or underwrite home purchase and ownership. Home repair or improvement fraud includes the following practices:

1. Intentionally shoddy or incompetent workmanship
2. Sale of overpriced or unfit materials or services
3. Failure to provide services or goods paid for by the customer
4. Submission of false claims for materials or work not provided
5. Misrepresentation of the need for particular materials or services to be performed
6. Misrepresentations or concealment of the costs of credit or of the nature of liens securing the payment obligations

The victim may be told that the home is in violation of building codes or in a condition substandard to the rest of the neighborhood thus lowering the value of the home or compromising the safety of the victim's family.

See also: *Consumer fraud; Merchandising fraud; Repair fraud.*

Homicide for profit: A homicide in which a victim is murdered for financial gain by the murderer or the person hiring the murderer.

See also: *Homicide fraud; Insurance fraud; Life-insurance fraud.*

Homicide fraud: A fraud in which a beneficiary of a life insurance policy murders the policy holder to collect benefits.

Income tax fraud: The evasion of a tax by any means including filing false or fraudulent returns.

See also: *External fraud.*

Inflated costs: Expenses that have been artificially inflated and invoiced when a contractor is paid on a cost-plus basis.

See also: *Commercial fraud; Procurement fraud.*

Information, random personal: Information, known only to an authorized individual, that is used as a means of identifying unauthorized log-in attempts to a computer system. The computer randomly transmits a question using this information and denies access to the user unless it receives the right answer. If several dozen questions are on file, it can be a very useful technique for stopping unauthorized computer use.

Input tampering: A computer scheme that can be accomplished by altering, forging, or fabricating computer input documents. In an entity, especially a small business with inadequate logical access control, input tampering is quite easy to accomplish.

See also: *Computer crime.*

Insider trading: Benefiting oneself or others in whom one has an interest by trading on privileged information or position. Typical situations include those in which a corporate officer or director trades in the stock of his or her company on the basis of inside information as to prospective profits or losses; bank officers lending money to themselves

or businesses in which they have an interest; corporate executives or purchasing officials setting up suppliers of goods and services to contract with their companies.

See also: *Banking fraud; Commercial bribery; Securities fraud; Trust, abuse of.*

Instructions, unauthorized: Commands placed by a computer programmer into a computer program to perform unauthorized functions, for example, making payments to a vendor not on an approved list.

See also: *Computer crime.*

Insurance fraud: Fraud perpetrated by or against insurance companies. Victims may be the clients or stockholders of insurance companies or the insurer itself.

Insurance fraud breaks down into the following categories and subclasses.

1. Fraud perpetrated by insurers against clients or stockholders includes the following:
 - a. Failure to provide coverage promised and paid for when claim is made
 - b. Failure to compensate or reimburse fully on claims
 - c. Manipulation of risk classes and high-risk policy holder categories
 - d. Embezzlement or abuse of trust in management of premium funds and other assets of insurance companies
 - e. Twisting, that is, illegal sales practices in which the insurer persuades customers to cancel current policies and purchase new replacement ones
2. Fraud perpetrated by policy holders against insurance providers includes the following: Filing of bogus claims for compensation or reimbursement, or of multiple claims for the same loss from different insurers, and so on
 - a. Inflating reimbursable costs on claim statements
 - b. Paying bribes or kickbacks to local agents to retain coverage or to obtain coverage in an improper risk category
 - c. Failing to disclose information or making false statements in an application for insurance

See also: *Casualty-insurance fraud; Claim, accident with false; Claim, false or fraudulent; Double-indemnity fraud; Homicide fraud; Life-insurance fraud; Mortgage-insurance fraud; Personal-injury insurance fraud; Trust, abuse of.*

Intellectual-property theft: The theft of intellectual assets such as business plans or trade secrets.

Internal Control Over Financial Reporting: The form of internal control required for compliance with the Sarbanes-Oxley Act. Defined in the SEC final rules as: “A process designed by, or under the supervision of, the registrant’s principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant’s board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

- Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and the dispositions of the assets of the registrant;
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant; and
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition use or disposition of the registrant's assets that could have a material effect on the financial statements.”

Internal fraud: Fraud committed against an organization by its employees, officers, or directors.

See also: *External fraud*.

Internet authentication: A computerized security measure used to identify a specific Internet user and to send information across the Internet safely.

See also: *Computer-access control*.

Inventory balances, understating beginning: Fraudulent financial reporting to conceal inventory shortages or theft. A common method for understating beginning inventory is to overstate the allowance for inventory obsolescence. For example, understating may be perpetrated if there has been a change in management and current management wishes to report improved profitability.

See also: *Financial statement, false; Inventory and warehousing cycle*.

Inventory and warehousing cycle: The accounting process that deals with the purchase and warehousing of merchandise for manufacture or resale or both.

See also: *Acquisition and payment cycle*.

Investment fraud: The use of imprudent, illusory, or bogus projects or businesses to attract investors through the prospect of high rates of return.

Investment fraud generally victimizes those with a pool of liquid or convertible assets, ranging from retirees or near-retirement age people, widows and widowers, to high-income professionals and businessmen. Hallmarks of this kind of fraud may include the following.

1. The investment promises a higher-than-average rate of return.
2. The investment project is still in development, that is, the project or business is not a mature entity.
3. The buyer purchases the investment from a stranger.
4. The investment has a generalized definition of its nature and scope and lacks detailed plans for measuring any progress.
5. The object or site of the investment is geographically remote or distant from investors.
6. The seller fails to fully disclose facts that are material to the investor prior to his commitment of money.

7. The seller is not registered with the appropriate regulatory agencies, such as the Securities and Exchange Commission or a state's securities commission.
8. The seller promises special advantages such as tax benefits.

See also: *Land fraud; Ponzi scheme; Pyramid scheme; Securities fraud.*

Invoice, false: An invoice submitted by a contractor for goods not delivered or for service not performed.

See also: *Commercial crime; Procurement fraud.*

Invoice, false sales: An altered company copy of the sales invoice showing a lower sales amount than the original invoice sent to the client. The difference between the real sale amount and the adjusted lower amount is then misappropriated when payment is received.

See also: *Sales and collection cycle.*

Invoice, false supplier: A supplier's invoice is prepared and submitted for payment to the company even though no goods have been delivered, no services rendered, or the invoice shows inflated quantity, inflated value, or both.

See also: *Acquisition and payment cycle; Procurement fraud.*

Jitney: The buy/sell broker disclosed on the exchange printout is acting on behalf of another broker.

Kickback: A form of off-book fraud in which the funds used for illegal payments or transfers are not drawn from the payer's regular company bank account and the payments do not appear on the payer's books and records. In collusion with suppliers, a purchasing agent may get paid a kickback for any number of activities, including allowing the supplier to submit fraudulent billing and approving the payment, excess purchasing of property or services, or bid-rigging.

See also: *Commercial crime; Procurement fraud; Off-book fraud; Secret commission.*

Land fraud: The sale of land, based on extensive misrepresentations as to value, quality, facilities, and/or state of development.

Victims are usually individuals buying land for retirement and/or investment. Land fraud usually consists of the direct sale of land or the sale of an interest in land—

1. To which the seller has no present title or claim of right; that is, the seller cannot properly transfer title or interest to the buyer as represented at the time of the sale.
2. About which there has been a misrepresentation or failure to disclose a material fact.
3. At inflated or unjustified prices based on misrepresentations made to the purchaser.
4. On the promise of future performance or development, which the seller neither intends to provide nor can reasonably expect to occur. Misrepresentations usually claim the presence of utilities, water, roads, recreational facilities, credit terms, and so on.

See also: *Investment fraud.*

Landlord-tenant fraud: Unlawful leasing or renting of property. Common fraud practices by landlords include the following:

1. Keeping two sets of books, in support of tax fraud
2. Schemes to avoid the return of security deposits
3. Rental of property to which one has no title claim or right
4. Deliberate and persistent violations of safety and health regulations; failure to provide heat, services, and so on.

Lapping: A customer's payment is embezzled and then recorded as paid sometime after the receipt of a subsequent payment from another customer. To keep customer *A* from complaining, the payment from customer *B* is applied to customer *A*'s account. Customer *C*'s payment is applied to customer *B*'s account, and so on.

See also: *Sales and collection cycle*.

Legitimate front: A form of money laundering in which a legitimate front business operating with large cash receipts is opened so that illegally earned money can be mingled with the bank deposits of the legitimate income of the business to disguise the source of the illegal money.

See also: *Money laundering*.

Life-insurance fraud: Any form of fraud making a life insurance company the victim.

See also: *Double-indemnity fraud; Homicide fraud*.

Loan fraud, single-family housing: Misapplication of funds by a borrower who purchases single-family housing units, ostensibly for personal use, but in reality is purchasing rental properties for resale.

See also: *Loan or lending fraud*.

Loan or lending fraud: The use of false information or the omission of material information for the purpose of granting or extending a loan.

When perpetrated by borrowers, loan fraud may take on any of the following forms:

1. Obtaining a loan through false statements
2. Using the loan for a purpose other than that for which the loan was granted
3. Larceny by false pretenses by which a loan is obtained with no intention of repayment

When perpetrated by the lending officer, loan fraud may take on any of the following forms:

1. Lending to oneself through ghost accounts
2. Lending to friends or entities in which one has an interest
3. Commercial bribery, meaning, approving loans to those who would not otherwise qualify as borrowers in exchange for kickbacks or other considerations
4. Advance fee schemes by which would-be borrowers remit money to secure a loan that is not forthcoming or for which no payment was necessary

A separate and important dimension of loan fraud involves the misuse or misrepresentation of items of collateral and collateral accounts.

See also: *Banking fraud; Collateral fraud; Statement, false; Trust, abuse of*.

Loan, nominee: A loan made in the name of a straw borrower or agent while the identity of the real borrower is undisclosed to the lender.

Loan to non-existent borrower fraud: Use of a false identity to obtain a loan. This scheme can be carried out individually by the borrower or with the assistance of an insider such as a loan officer.

See also: *External fraud; Loan or lending fraud.*

Long the stock: Buying stock. Your long position represents the number of shares owned (also referred to as going long).

Market manipulation: The intentional inflation of a stock price accomplished by stock purchases, usually in a small-cap market, with a sudden sale to third parties who are left with stock that is worth substantially less than they paid for it.

Medicaid-Medicare fraud: Fraudulent practices involving the receipt or provision of health-care services under government-financed Medicare or Medicaid programs. This kind of fraud is usually perpetrated by health-care providers (both professional and facility operators) against the government financing the programs or the intended beneficiaries of the programs, or both. Specific Medicaid-Medicare fraud practices include the following.

1. *Ping-ponging.* Referring patients to other doctors in a clinic to claim reimbursement for the “consultation” rather than for bona fide patient treatment or observation.
2. *Upgrading.* Billing for services not provided.
3. *Steering.* Sending patients to a particular pharmacy, medical lab, and so on, for required prescriptions or services and receiving improper payments in return.
4. *Shorting.* Delivering less medication (for example, pills) than prescribed while charging for full amount.
5. *Procurement abuses.* Establishing supply-purchase arrangements with firms that pay kickbacks to health care facilities or providers with firms that are owned by those controlling the facility itself.
6. *False claims.* Submitting claims for payment by the government for patients who do not exist, or who were never seen or treated.

See also: *Claim, false or fraudulent; Government-benefit program, fraud against; Kickback; Procurement fraud.*

Medical fraud: Provision and sale of bogus, highly questionable or dangerous medical services, cures, or medications.

Victims are often terminally or incurably ill patients seeking miracles. Also victimized are the poorly informed, who are vulnerable to false claims for beauty treatments and cosmetics.

Medical fraud generally includes one or more of the following.

1. *Quackery.* False representation of oneself as a legally trained and licensed health care professional
2. *Fake cures.* Sale of bogus or highly questionable “cures” for specific illnesses or diseases

3. *Misrepresentation.* In addition to misrepresenting the therapeutic value of medication, the intentional omission of the known side effects of medication.
4. *Misrepresentation of treatment.* False statement about the therapeutic value of a particular treatment and the degree of its "acceptance" in bona fide medical practice; omission of material information concerning known side effects of a treatment that would affect the patient's choice of treatment program.

See also: *Health-care fraud.*

Merchandising fraud: An umbrella term for a broad variety of consumer fraud involving false inducements to purchase merchandise, which either is not as represented or will never be delivered.

These kinds of fraud usually involve one or more of the following:

1. Representation that the item is sold at a lower than usual price, even though it is actually sold at the usual retail price or higher
2. Misrepresentation of the quality or utility of the merchandise
3. Misrepresentation of the ultimate price or credit terms
4. Misleading information on warranties, the return policy or the validity of "money back guarantees"
5. Solicitation of money with no intention to deliver the merchandise promised
6. "Bait and switch" fraud

Victims customarily buy from door-to-door salespeople or are entrapped when they respond to newspaper, magazine, telephone, radio, or television advertisements.

See also: *Consumer fraud.*

Mixing of funds: Commingling client funds with the funds of the brokerage firm, which then enables the broker to post the winning trades to the brokerage firm or the losing trades to their clients.

See also: *Commercial crime; Securities fraud.*

Mobile lab: A scheme in which a group of people posing as medical professionals set up a lab in a storefront located in a blue-collar, low-income area to offer free physicals to people who have medical insurance. The insured is subjected to extensive, expensive tests that are billed to his or her insurance company. The mobile labs are gone when the insured returns for the test results.

See also: *Health-insurance fraud; Insurance fraud.*

Modeling-school fraud: Fraudulent schools tell students they must have a portfolio of portraits to send to potential customers in order to get modeling assignments. The victim is then charged greatly inflated prices by a photographer who is often a participant in the scam.

See also: *External fraud; Self-improvement scheme.*

Money laundering: The process of turning “dirty” money, that is, illegally obtained money, into “clean” money to conceal its existence, source or use, or to obstruct investigative efforts, to preserve assets from forfeiture or to evade taxes.

See also: *Legitimate front; Offshore banks and tax havens; Reporting guidelines, breach of; Smurfing.*

Money-transfer fraud: Funds are stolen by an outsider or bank employee with access to the correct identification numbers needed to transfer funds by wire.

See also: *External fraud.*

Mortgage-insurance fraud: A scheme in which a healthy individual, who has a mortgage insurance policy that guarantees mortgage payments to the lender if the purchaser of the property defaults because of death or disability, falsely claims that he or she is disabled in order to have the insurance company pay the mortgage.

See also: *Casualty-insurance fraud; Insurance fraud.*

Mortgage security, false: Security offered for mortgage financing purposes that is nonexistent or has a value far lower than represented.

See also: *Commercial crime; Finance fraud.*

New-account fraud: The use of false identification to open new accounts and steal money before the bank collects the funds from fresh deposits.

See also: *Check fraud.*

Nominee account: See *Account, nominee.*

Nursing-home fraud: Various kinds of fraud perpetrated by individuals providing institutional nursing and convalescent care to patients, particularly the aged.

Victims are the patients of the facilities, their families, and/or governmental entities that subsidize the cost of care.

Forms of nursing home fraud abuses include the following:

1. Unlawful conversion or attachment of patients' assets
2. False claims to patient, family, or government entity regarding services delivered
3. False statements in license applications or renewals
4. Maintenance of fraudulent records as to general or overhead costs of operation of facilities as a basis for false claims to governmental entities
5. Receipt of kickbacks from facility suppliers
6. Employment of inadequate or unqualified staff in violation of licensing guidelines

See also: *Claim, false or fraudulent; Embezzlement and fiduciary fraud; Government-benefit program, fraud against; Health-care fraud; Procurement fraud.*

Off-book fraud: Fraud that occurs outside the accounting environment where no audit trail is likely to exist.

See also: *On-book fraud.*

Offshore banks and tax havens: Banks or financial institutions located in tax havens that conduct local and international business transactions in which money and other securities can be held or transferred from one jurisdiction to another in secrecy under the protection of banking privileges. The owners of the assets direct the transactions—personally or through an intermediary, such as a trust to minimize taxes, evade taxes, or avoid creditors.

See also: *Money laundering*.

On-book fraud: Fraud occurring in a business in which an audit trail (sometimes obscure) exists that could aid in its detection.

See also: *Off-book fraud*.

Overhead charge, false: Fraudulently inflating costs through the addition of bogus labor charges or overbilling of materials to increase profits in a cost-plus contract to allow the contractor to keep the difference between actual and inflated costs.

See also: *Property-improvement fraud*.

Patent fraud: A variation of the advance fee fraud. The fraudster solicits “patentable” ideas or gadgets through newspaper advertisements, and so on, for “evaluation by experts.” The “evaluation” usually involves a fee, or at least “further processing” of the submission may involve a fee. The fraudster usually has neither the intention nor the capacity to evaluate or process a patentable item.

See also: *Advance-fee fraud; Self-improvement scheme; Vanity-publishing scheme*.

Payroll and personnel cycle: The accounting process that handles the hiring, firing, and payment of employees along with timekeeping, expense accounts, and travel reimbursement and insurance matters.

See also: *Acquisition and payment cycle*.

Pension-fund fraud: Theft and fraudulent conversion of pension fund assets either by trustees, employers, or employees.

Fraud perpetrated by trustees in violation of their fiduciary duty in the management of pension funds through the following:

1. Poor investments tied to self-dealing or commercial bribery
2. Embezzlement

This fraud victimizes both the individuals who have contributed to the fund and those intending to benefit from it. Victims are employees whose potential benefits are reduced either by fraud or bankruptcy, as well as the employer whose contributions to the pension plan could be inflated or lost.

See also: *Embezzlement and fiduciary fraud; Claim, false or fraudulent; Commercial bribery; Trust, abuse of*.

Personal checks, substituting for cash: An employee takes money from the cash register and substitutes a personal check. In that way, the cash drawer is always in balance, but the employee never submits the personal check for deposit to the company’s bank account. Consequently, the employee receives free use of the cash.

Personal-injury insurance fraud: Report of a real but overstated physical injury or a false injury to an insurance company to recover unentitled benefits such as for a tort claim or reimbursement of fake medical expenses.

See also: *Casualty-insurance fraud; Insurance fraud.*

Personal property pawned: The perpetrator inflates the value of his or her personal belongings, insures them, and then pawns them for a lesser amount of cash. He or she then reports them stolen and files a claim. If the insurance payment is received, he or she then recovers the items from the pawnshop with a portion of the insurance payment and pockets the difference.

See also: *Insurance fraud; Property-insurance fraud.*

Pigeon drop or pocketbook drop: One of a large variety of street con games. The victim is persuaded to withdraw a large sum of cash from a bank account to show good faith or financial responsibility regarding the sharing of a “discovered” cache of money with two other persons (who are con artists). In the course of the con, both the “discovered” money and the victim’s “good faith” money disappear as do the con artists.

Victims may be anyone, since perpetrators of this fraud have a remarkable ability through words to disarm their victims. Keys to the pigeon drop con are the following:

1. The con artists do not appear to be associated or know each other in any way.
2. A pocketbook, envelop, and so on, containing a sizable amount of money and no owner identification is “found” by one of the perpetrators who suggests the money is illicitly generated, for example, a gambler’s proceeds.
3. The fraudsters agree to share the money with the victim who shows “good faith” to those involved by putting up money. Alternately, all may agree to put money into a pool to be held by a conspirator, meaning, the one who did not find the money.
4. A switch is made while the victim is distracted, and his or her money is stolen by one of the perpetrators.

Pollution and environmental protection violation: One of many abuses that violates specific environmental- and pollution-control statutes and orders. White-collar crime abuses in this area consist primarily of the making or submitting of false statements concerning the degree of compliance with regulations for pollution control in order to cover up violations or lack of compliance with environmental standards. Falsification of test or sample data designed to measure compliance with standards represent another form of this violation.

See also: *Commercial crime; Environmental abuse; Statement, false.*

Ponzi scheme: This is a general class of fraud (a variation of the pyramid scheme) in which the fraudster uses money invested by later victims to pay a high rate of return to the first group of investors instead of making promised investments. These schemes must inevitably collapse because it is mathematically impossible to continue them indefinitely. The length of time they can continue will depend upon the promised rate of return to investors, the amount of money the fraudster takes out for him- or herself and the costs of inducing victims to part with their money (for example, sales commissions). Many of these

frauds have cheated their victims of millions of dollars; some frauds have operated over a period of years.

Ponzi elements exist in many varieties of investment fraud under different guises and in different variations; for example, long-term investments and short-term business financing.

See also: *Investment fraud*.

Possession of property obtained by crime: An offense that refers either to the actual possession of property obtained by a crime or to the possession of proceeds from the disposal of property obtained by a crime.

See also: *Fraud*.

Price fixing: Illegal combinations by sellers to administer the price of a good or service, thus depriving customers of a competitive marketplace, restraining competition, and maintaining an artificial price structure.

Victims are customers who are deprived of freely determined prices for the goods and services they purchase. Secondary victims may be competitors of the firms participating in the price fixing agreement.

See also: *Anti-trust offense; Trade, restraint of*.

Procurement fraud: Unlawful manipulation of the public or private contracting process to obtain an advantage.

Victims are competitors, the public or private entity soliciting bids it believes to be competitive as well as customers or constituents of those entities who do not realize the benefits that would be derived from a truly competitive procurement process.

Three main forms of competitive procurement fraud are the following.

1. *Bid rigging.* A form of illegal anticompetitive activity in which bidders in a competitive procurement collusively set their bids in such a way as to deprive the bid solicitor of a competitive process. The effect is an administered bidding process in which the winner and the terms and prices of the goods and services involved are set by the conspirators rather than by the competitive process. Parties to the conspiracy are thus able to divide among themselves a set of procurement contracts and to fix prices for goods and services at the same time.
2. *Bid fixing.* A form of illegal manipulation of the procurement process whereby one bidding party is provided with inside information by the bid solicitor or an agent, which enables the said bidder to gain an unfair advantage over other bidders.
3. *Bribery and kickbacks.* The awarding of procurement contracts on the basis of the payment of bribes and kickbacks to procurement officials rather than on the basis of competitive procurement guidelines.

See also: *Claim, false or fraudulent; Commercial bribery; Kickback; Corruption, public or official*.

Product substitution: The substitution, without the knowledge of the purchaser, of a less expensive product or service. The purchaser is charged for the more expensive product or service and the fraudster pockets the difference.

See also: *Commercial crime; External fraud; Procurement fraud; Property-improvement fraud*.

Property-improvement fraud: The fraudster goes door-to-door promising repairs to property at bargain rates, collecting up-front money and then absconding with the proceeds. The victims are usually senior citizens.

See also: *External fraud*.

Property-insurance fraud: An insured reports a false theft, inflates the value of his or her personal belongings and pawns them or purposely destroys them to collect a benefit from the insurer.

See also: *Arson for profit; Insurance fraud; Personal property pawned; Repossessed household goods*.

Public Company Accounting Oversight Board (PCAOB): “A private-sector nonprofit organization created by the Sarbanes-Oxley Act of 2002 to oversee the auditors of public companies and protect the interest of investors and further the public interest in the preparation of informative, fair and independent audit reports”. The PCAOB replaces the Audit Standards Board (ASB) of the AICPA as the body responsible for creating auditing standards for public companies. The ASB will continue to set generally accepted audit standards for non-public companies.

Public or official corruption: See *Corruption, public or official*.

Purchases, unnecessary: Inventory ordered specifically for personal use, theft, or scrap proceeds. The embezzlements are then charged to inventory.

See also: *Acquisition and payment cycle; Inventory and warehousing cycle; Procurement fraud*.

Pyramid scheme: The commercial version of the chain letter scheme used by fraudsters to sell phony investments (Ponzi scheme), distributorships, franchises, and business opportunity plans.

See also: *Chain-referral scheme; Franchise fraud; Investment fraud*.

Real estate fraud: A form of loan fraud involving the purchase of under- or over-valued real estate.

See also: *External fraud; Loan or lending fraud; Mortgage security, false*.

Referral sales fraud: See *Chain-referral scheme; Merchandising fraud*.

Repair fraud: Consumer fraud involving repair or maintenance service performed on consumer goods.

These white-collar crime schemes generally involve the following:

1. Overcharging for services performed
2. Charging for services and parts not used
3. Performing services or repairs not wanted or needed
4. Failing to perform services or repairs promised

See also: *Consumer fraud*.

Reporting guidelines, breach of: A breach in defiance of a government requirement that banks assist in the prevention of money laundering by reporting details of large cash

deposits. For example, a bank employee who conspires with a money launderer to make deposits without reporting the required details is breaching the reporting guidelines.

See also: *Money laundering.*

Repossessed household goods: Household items are repossessed and the insured submits a false claim to the insurer reporting the property was stolen.

See also: *Insurance fraud; Property-insurance fraud.*

Repurchasing: A stock market manipulation in which the promoter buys back control of the company when the stock price reaches rock bottom.

See also: *Stock market manipulation.*

Risk factors, generic: Risk factors within the control of the entity protecting itself but outside the control of potential perpetrators.

Revenue recognition in the improper period: Preparation of false financial statements through the improper accruals of revenue on future, anticipated sales. Techniques include altering dates on shipping documents or holding the books open until after shipments have occurred. This technique is often used to inflate reported profits.

See also: *Financial statement, false; Revenue recognition on transactions that do not meet revenue recognition criteria.*

Revenue recognition on transactions that do not meet revenue recognition criteria: Preparation of false financial statements by improperly recognizing revenue on transactions for which the earning process is incomplete—for example, when the right of return exists, or on bill-and-hold transactions. The items involved are often concealed through the use of written side agreements or oral agreements that are not included with the company's books of account.

See also: *Financial statement, false; Revenue recognition in the improper period.*

Running a box: One or more persons control the movement of a stock to manipulate its price. They are called "the box."

See also: *Stock market manipulation.*

Sales and collection cycle: The billing of goods or services to customers, the setting up of accounts receivable for customers who purchase goods or services on credit and the collection of funds relating to those receivables.

Sarbanes-Oxley Act: Act of Congress passed in July 2002 to give greater reliability to financial statements of public companies.

Scrap, theft of: This kind of theft can be significant, especially if the thief has the authority to designate saleable inventory as scrap. In most companies, inventory scrap is easy to steal because it is not recorded or well controlled.

See also: *Procurement fraud.*

Secret commission: The most common form of procurement fraud. A secret payment is given, usually by a supplier to a purchasing agent, to buy the purchasing agent's influence on his or her employer's decision-making.

See also: *Commercial crime; Kickback; Procurement fraud.*

Securities and Exchange Commission Final Rules: Regulations published by the SEC after discussion. As used in this *Handbook*, the final rules are the means of implementing the intent of the Sarbanes-Oxley Act of 2002.

Securities fraud: Fraudulent activities involving the sale, transfer, or purchase of securities or money interests in the business activities of others.

Victims are generally investors who are not aware of the full facts regarding transactions into which they enter. Abuses cover a broad range and can include, for example, the following situations.

1. Businesses or promoters seek to raise capital unlawfully or without proper registration and monitoring.
2. Securities of no value are sold or are misrepresented as being worth far more than their actual value.
3. Purchasers are not advised of all facts regarding securities and/or of the failure to file appropriate disclosures with federal and provincial regulatory agencies.
4. Insiders use special knowledge to trade in securities to the disadvantage of the general public.
5. Broker-dealers and investment advisers act for their own benefit rather than for the benefit of their clients.
6. False information is provided to security holders and the investing public in financial statements published or filed with securities regulatory agencies or in the media as a result of payments to financial writers or publications.
7. Manipulation of the price of securities by purchases and sales on the stock exchanges or over-the-counter markets.

Securities violations potentially exist wherever investors rely on others to manage and conduct the business in which an investment is made. It is not necessary that there be any formal certificates such as stocks and bonds. Any form of investment agreement is potentially a “security.”

See also: *Advance-fee fraud; Boiler room; Insider trading; Investment fraud; Statement, false.*

Self-improvement scheme: This kind of fraud appeals to the victims’ desire to improve him- or herself personally or financially by the acquisition of social, employment, or physical skills or attributes.

Schemes in this category tend to run on a continuum from improving purely personal or social skills and attributes to those tied to an individual’s employment opportunities. On the personal end of the scale are the dance studio or charm school schemes; on the employment end of the scale are fraudulent job training schemes and advance fee employment agencies.

Somewhere in the middle are modeling agencies which purport to both improve the “person” and his or her employment prospects. Also included are courses on improving one’s image or ability to communicate with others. Some business opportunity schemes, which hold out the prospect of financial improvement plus “being a respected community

businessperson,” also fall into this category by appealing to the victim’s desire to improve his or her finances and life style.

See also: *Business-opportunity fraud; Employment-agency fraud; Vanity-publishing scheme.*

“Sewer” service: A term used to describe the kinds of activity noted below.

Many merchandising, home repair, and other kinds of fraud rely on the use of litigation for ultimate collection of the proceeds of the fraud. Likewise, many enterprises that are not strictly speaking fraudulent, for example, those that sell much overpriced merchandise on credit, also depend on litigation or the threat of litigation to squeeze money from victims.

In both these situations, devices are often adopted to fraudulently deprive victims of the opportunity to defend against litigation—usually by not informing them that litigation has been initiated against them (that is, dropping the summons or subpoena “down the sewer”). This is accomplished, usually, by false affidavits, filed in court, that a summons and complaint were served on the victim.

See also: *Stock market manipulation.*

Sham, corporate: The use of a corporate entity to provide a veil of respectability and substance for fraudulent activity.

See also: *Commercial crime.*

Sham transaction: A fraudulent transaction giving the impression of a legitimate transaction at a higher price. These transactions are particularly difficult to detect because they involve collusion with a co-conspirator outside the entity.

See also: *Sham, corporate.*

Shell company: An inactive company whose shares have been repurchased.

Short weighting or loading: Deliberate shorting of the volume or quantity of a cargo or other purchase. The short load is accompanied by a false invoice demanding payment for the full amount. This kind of fraud is easiest to perpetrate where the goods involved are of a nature or bulk that it is difficult for the receiver to detect shortages.

The reverse of the short weighting or loading fraud is often used as a modus operandi for theft of cargo. In this situation, a transport vehicle is intentionally overloaded; the overage is not recorded and the overloaded amount forms the basis of kickbacks to the scheme operators from the recipient of the shipment, who is often the fence for the stolen goods. Manipulation of the size or volume of loads must always be accompanied by false documentation.

This violation involves either a false claim to a customer or a plain and simple theft from the shipper. Because insiders are frequently involved, it will often involve commercial bribery, kickbacks, and so on.

See also: *Weights and measures fraud.*

Short selling: A technique whereby the trader is gambling that the price of a stock will fall. Thus, he or she anticipates a profit on the transaction by selling a number of shares first, for later delivery at a specified price. The trader then buys those shares at a later date,

when, if his or her gamble were correct, the share price has fallen and he or she delivers them. Thus, the trader makes a profit during a period of declining prices of the stock.

Siphoning funds: Illegal withdrawal of money in small amounts from a large number of accounts. For example, pennies and portions of pennies (resulting from rounding off) can be shaved from thousands of savings accounts. The money is then accumulated in a single account that is accessed by the embezzler.

Skimming: A scheme in which cash is skimmed before it enters the accounting system. For example, an employee accepts cash but never prepares a receipt or prepares a receipt for less than the amount received.

See also: *Sales and collection cycle*.

Smurfing: The use of couriers (also known as *smurfs*) to deposit and withdraw cash or cash equivalents at financial institutions in amounts less than the reporting limit to avoid reporting requirements.

See also: *Money laundering*.

Statement, false: The concealment or misrepresentation of a fact material to the decision-making process of an entity. The false statement is often the means by which a fraudulent scheme to obtain money or benefit is effected for either of the following, among other, reasons.

1. The false statement constitutes the underlying documentation for a false claim.
2. The false statement impedes discovery of the fraudulent scheme, that is, covers up the fraud. These statements often provide the opportunity for conditioning the victim to unquestioningly accept and approve a false claim.

See also: *Claim, false or fraudulent; Ghost employee; Government-benefit program, fraud against*.

Stock market manipulation: A crime perpetrated by a stock promoter who artificially influences the market price of shares in a company for personal gain at the expense of the investing public.

See also: *Commercial crime; Securities fraud*.

Street certificate: A stock certificate that has been issued in the name of a brokerage firm and then endorsed by it. It is now like a bearer certificate and can change hands several times in many trades without being returned to a trust company for transfer.

Taking out the market: See *Cleaning up the market*.

Talent-agency scheme: See *Self-improvement scheme; Vanity-publishing scheme*.

Tax and revenue violation: Fraud perpetrated with the intent to deprive a taxing authority of revenue to which it is entitled or of information it needs to make a judgment regarding revenues to which it is entitled or to avoid admission of involvement in illicit, though profitable, business activities.

Tax fraud may be perpetrated through the filing of a false return, as in personal income tax fraud; through the bribery of a public official, as may occur in property tax assessment fraud; or in the failure to file appropriately, as with an organized crime-figure who may not be concerned with avoiding tax liability but rather with revealing the sources of his or her

taxable income. Many white-collar crimes obligate the offender to commit tax fraud because of illicitly obtained money he or she does not wish to report, for example, assets due to bribe, larceny, kickback, or embezzlement proceeds. Common crimes, especially of a business nature, also result in tax violations, for example, bookmaking and fencing stolen goods, which could be income and sales tax abuses.

Tax avoidance through false statements may be a component of otherwise legitimate business enterprises, especially in the areas of business and occupation taxes, inventory taxes, and sales taxes. Individuals and businesses will also seek to avoid or evade excise taxes, for example, on cigarettes or in the case of tanker trucks by the substitution of low-taxed home heating oil for higher-taxed diesel fuel.

See also: *Income tax fraud.*

Trade, restraint of: Actions, combinations, or schemes that interfere with unfettered marketplace transactions. Examples are price fixing, bribery and kickbacks for commercial advantage, interference with competitive bidding processes, dictation of price structure to customers or dealers, and exclusive buying arrangements.

See also: *Commercial bribery; Price fixing; Procurement fraud.*

Transactions, entering false: Entering invoices for fake vendors into the accounts payable system or recording false credit memos to reduce legitimate accounts receivable.

See also: *Acquisition and payment cycle; Sales and collection cycle.*

Trust, abuse of: Misuse of one's position and/or privileged information gained by virtue of that position to acquire money, property, or some privilege to which one is not entitled. Abuse of trust also often involves a violation of fiduciary duty.

Abuse of trust can occur in many areas but arises most frequently in the following four white-collar crime areas.

1. *Banking.* Self-dealing in connection with loans or credit to oneself, one's friends, or business associates.
2. *Securities.* Insider information used for personal benefit at the expense of clients, stockholders, and others.
3. *Commercial bribery.* Manipulation of procurement and competitive bidding processes.
4. *Embezzlement.* Misuse of property or funds in the custody of a trustee.

See also: *Banking fraud; Commercial bribery; Embezzlement and fiduciary fraud; Insider trading; Procurement fraud; Securities fraud.*

Trust fund, misappropriation of: The diversion of client funds held in trust and use of the money for purposes other than those intended by the client.

See also: *External fraud.*

Vanity-publishing scheme: Any scheme that involves eliciting fees from individuals on the promise of promoting their creative "talents" (real or imaginary) or assisting them in the development of said "talent."

The success of these kinds of fraud relies on the victim's vanity about his or her hitherto unrecognized talent. These schemes work best in areas such as literary publishing or song writing, where taste is more important than performance standards.

The fraudster will imply a promise of national advertising, book reviews, distribution, and special marketing services but not so concretely that he or she will be held to any obligation. The victims usually invest heavily and lose both their money and their hopes. They are left with a few copies of a printed and scored song arrangement or a number of copies of books that established book review publications have not troubled to look at because of their publishing source.

See also: *Self-improvement scheme*.

Warehousing: Part of a stock market manipulation that places shares into the hands of people who are friendly to the promoter—warehousing or parking—to allow the promoter to maintain control of the shares and continue to restrict and regulate their availability.

Wash-trading: A flurry of trading activity falsely created by the promoter's group to give the appearance of great interest in the stock to increase demand for the stock among the public to whom the promoter plans to eventually sell his holdings when the price reaches a certain level.

See also: *Stock market manipulation*.

Weights and measures fraud: Cheating customers by failure to deliver prescribed weights or volumes of desired goods. The victim is defrauded by relying on the false documents provided by the fraudster testifying to the delivered quantities.

Examples of white-collar crimes include the following:

1. Gas pump meter manipulation to show more gas pumped than received by the customer
2. Odometer rollbacks in auto sales

These kinds of fraud are most successful if the victim cannot easily verify the accuracy of the measuring devices or if the victim has no reason to question the seller's claim or statement, for example, when the products sold are bottled or packaged.

See also: *Short weighting or loading*.

Welfare fraud: Abuses of government income and family subsidy programs.

Government welfare programs are often exploited by applicants who apply for benefits to which they are not entitled or continue to claim eligibility even though they no longer meet the eligibility criteria.

Receipt of money from claimants by officials processing welfare claims represents another dimension of this fraud. These monies may be solicited as kickbacks in exchange for the filing of inflated claims; as bribes to certify claimants who are ineligible or to avoid reporting claimants' ineligibility or as extortion for processing claims to which a recipient is fully eligible. In some cases, nonexistent recipients (*ghosts*) may be created to fraudulently siphon money out of the programs.

See also: *Government-benefit program, fraud against*.

White-collar crime: Nonviolent crime for financial gain committed through deception by entrepreneurs, professionals, or semiprofessionals using their special occupational skills and opportunities. This category also includes similar crimes committed by anyone having special technical and professional knowledge of business and government, irrespective of the person's occupation.

See also: *Commercial crime; Economic crime.*

Work-at-home schemes: See *Business-opportunity fraud; Franchise fraud.*

Written-off account, diversion of payments from: Diversion of payments received from a customer whose account has been written off. Because most companies do not monitor defunct accounts, this activity is rarely detected. For example, an employee will work with a customer to collect an overdue receivable. Before the customer pays, the employee writes off the account, removes it from the books, and pockets the funds received.

See also: *Internal fraud; Sales and collection cycle.*

BIBLIOGRAPHY (SUGGESTED REFERENCES)

The following is a list of suggested references (books, publications, reports, etc.) and Web sites for further reading on the subject of fraud, commercial crime, and related topics.

BOOKS, PUBLICATIONS, AND REPORTS

2005 Fraud Examiners Manual, Austin, TX: Association of Certified Fraud Examiners, 2004.

Albanese, Jay S. *White-Collar Crime in America*. Englewood Cliffs, NJ: Prentice Hall, 1995.

American Institute of Certified Public Accountants. *Internal Control Reporting: Implementing Sarbanes-Oxley Act Section 404*. Financial Reporting Series. New York, NY: American Institute of Certified Public Accountants, 2004.

Beasley, Mark S., Joseph V. Carcello, and Dana R. Hermanson. *Fraudulent Financial Reporting: 1987–1997. An Analysis of U.S. Public Companies*. New York, NY: Committee of Sponsoring Organizations of the Treadway Commission, 1999.

Beaven, Guy W. *Hello Suckers!: Inside the Brutal World of Stock Market Scams and How to Prevent Falling Victim*. Washington Grove, MD: Gordon-Richardson Press, 1995.

Bequai, August. *White Collar Crime: A Twentieth Century Crisis*. Lexington, MA: D.C. Heath, 1978.

Bertrand, Marsha. *Fraud!: How to Protect Yourself from Schemes, Scams, and Swindles*. New York, NY: American Management, 1999.

Binstein, Michael, and Charles Bowden. *Trust Me: Charles Keating and The Missing Billions*. New York, NY: Random House, 1993.

Bintliff, Russell L. *Complete Manual of White Collar Crime Detection and Prevention*. Englewood Cliffs, NJ: Prentice Hall, 1993.

Black, Henry C. *Black's Law Dictionary: Eighth Edition*. St. Paul, MN: West Publishing, 2004.

Blue Ribbon Committee Report on Improving the Effectiveness of Corporate Audit Committees, 1999. See www.nyse.com and www.nasdaqnews.com.

Bologna, Jack, and Paul Shaw. *Avoiding Cyber Fraud in Small Businesses*. New York, NY: John Wiley & Sons, 2000.

Bologna, Jack. *Handbook on Corporate Fraud: Prevention, Detection, and Investigation*. Boston, MA: Butterworth-Heinemann, 1993.

Brickey, Kathleen F. *Corporate and White Collar Crime: Selected Cases and Statutes*. New York, NY: Aspen Law & Business, 1997.

- Bucy, Pamela H. *White Collar Crime: Cases and Materials*. St. Paul, MN: West Group, 1998.
- Calavita, Kitty, Henry N. Pontell, and Robert H. Tillman. *Big Money Crime: Fraud and Politics in the Savings and Loan Crisis*. Berkley, CA: University of California Press, 1997.
- Camerer, L. *Costly Crimes, Commercial Crime and Corruption in South Africa*. Johannesburg: Institute for Security Studies, 1997.
- Cole, Richard B. *Management of Internal Business Investigations: A Survival Guide*. Springfield, IL: Charles C. Thomas, 1996.
- Coleman, James William. *The Criminal Elite: Understanding White-Collar Crime*. New York, NY: St. Martin's Press, 1998.
- Comer, Michael J. *Corporate Fraud*, Second Edition. New York, NY: McGraw-Hill, 1998.
- Comer, Michael J., Patrick M. Ardis, and David H. Price. *Bad Lies in Business: The Commonsense Guide to Detecting Deceit in Negotiations, Interviews, and Investigations*. New York, NY: McGraw-Hill, 1992.
- Committee of Sponsoring Organizations of the Treadway Commission. *Integrated Control—Integrated Framework*. Two Volumes. Jersey City, NJ: American Institute of Certified Public Accountants, 1994.
- Croft, Roger. *Swindle!: A Decade of Canadian Stock Frauds*. Toronto, ON: Gage Pub., 1975.
- Dailey, Edward J. *Health Care Fraud: A New White Collar Crime: Strategies for Compliance, Audit, Litigation, and Prosecution*. Boston, MA: MCLE, 1997.
- Durkin, Ronald L., and Everett P. Harry III. *Fraud Investigations in Litigation and Dispute Resolution Services: A Nonauthoritative Guide*. New York, NY: American Institute of Certified Public Accountants, Inc., 1997.
- Dykeman, Francis C. *Forensic Accounting: The Accountant as Expert Witness*. New York, NY: John Wiley & Sons, 1982.
- Silverstone, Howard, and Michael Sheetz. *Forensic Accounting and Fraud Investigation for Non-Experts*. Hoboken, NJ: John Wiley & Sons Inc., 2004.
- Frank, Peter B., and Michael J. Wagner. *Providing Litigation Services*. New York, NY: American Institute of Certified Public Accountants, 1993.
- Garman, Thomas E. *Ripoffs and Frauds, How to Avoid and How to Get Away*. Houston, TX: Dame Publications, 1996.
- Geis, Gilbert, Robert F. Meier, and Lawrence M. Salinger. *White-Collar Crime: Classic and Contemporary Views*. New York, NY: Free Press: Distributed by Simon & Schuster, 1995.
- Ghosh, Anup K. *E-Commerce Security: Weak Links, Best Defenses*. New York, NY: John Wiley and Sons, 1998.
- Grau, J.J., and B. Jacobson. *Criminal and Civil Investigation Handbook*. New York, NY: McGraw-Hill, 1993.
- Green, Gary. *Occupational Crime*. Chicago, IL: Nelson-Hall, 1997.

- Green, Scott. *Manager's Guide to the Sarbanes-Oxley Act: Improving Internal Controls to Prevent Fraud*. Hoboken, NJ: John Wiley & Sons, Inc., 2004.
- Hoyt, Douglas et al. *Computer Security Handbook, Second Edition*. New York, NY: MacMillan Publishing Company, 1995.
- Janal, Daniel S. *Risky Business: Protect Your Business from Being Stalked, Conned, or Blackmailed on the Web*. New York, NY: Wiley, 1998.
- Judson, Karen. *Computer Crime: Phreaks, Spies and Salami Slicers*. Berkley Heights, NJ: Enslow Publishers, 1999.
- Katz, Leo. *Ill-Gotten Gains: Evasion, Blackmail, Fraud, and Kindred Puzzles of the Law*. Chicago, IL: University of Chicago Press, 1996.
- Lam, James. *Enterprise Risk Management: From Incentives to Controls*. Hoboken, NJ: John Wiley & Sons, Inc., 2003.
- Lander, Guy P. *What is Sarbanes-Oxley?* New York, NY: McGraw-Hill, 2004.
- Leonard, Orland. *Corporate and White Collar Crime: An Anthology*. Cincinnati, OH: Anderson Publishing, 1995.
- Levi, Michael. *Fraud: Organization, Motivation, and Control*. Aldershot, England; Brookfield, VT: Ashgate, 1999.
- Lundelius, Charles R. *Financial Reporting Fraud: A Practical Guide to Detection and Internal Control*. New York, NY: American Institute of Certified Public Accountants, 2003.
- Magnuson, Roger J. *The White Collar Crime Explosion: How to Protect Yourself and Your Company from Prosecution*. Minneapolis, MN: Dorsey & Whitney, 1992.
- Manning, George A. *Financial Investigation and Forensic Accounting*. Boca Raton, FL: CRC Press, 1999.
- McMahon, David. *Cyber Threat*. Toronto, ON: Warwick Publishing, 2000.
- Moeller, Robert R. *Sarbanes-Oxley and the New Internal Auditing Rules*. Hoboken, NJ: John Wiley & Sons, Inc., 2004.
- Moscarino, George J., and Charles M. Kennedy. *Corporate Investigations: A Practical Primer*. Washington, DC: Washington Legal Foundation, 1996.
- Neilson, R. Todd, et al. *Providing Bankruptcy and Reorganization Services: A Nonauthoritative Guide*. New York, NY: American Institute of Certified Public Accountants, 1998.
- Nossen, Richard A. *The Detection, Investigation, and Prosecution of Financial Crimes*. Richmond, VA: Thoth Books, 1993.
- Pipkin, Donald L. *Information Security: Protecting the Global Enterprise*. Upper Saddle River, NJ: Prentice Hall PTR, 2000.
- Podgor, Ellen S., and Jerold H. Israel. *White Collar Crime in A Nutshell*. St. Paul, MN: West Publishing, 1997.
- Poveda, Tony G. *Rethinking White-Collar Crime*. Westport, CT: Praeger, 1994.

- Ramachandran, K.S. (Kattalai Sivasubramanya). *Scanning the Scam: How and Why of the Securities Scandal*. New Delhi: Neo Publishing, 1993.
- Ramos, Michael. *How to Comply with Sarbanes-Oxley Section 404: Assessing the Effectiveness of Internal Control*. Hoboken, NJ: John Wiley & Sons, Inc., 2004.
- Ramos, Michael J., and Anita M. Lyons. *Considering Fraud in a Financial Statement Audit: Practical Guidance for Applying SAS No. 82*. New York, NY: American Institute of Certified Public Accountants, 1997.
- Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*. New York, NY: John Wiley and Sons, 2000.
- Siegel, Larry J. *Criminology: Theories, Patterns and Typologies (with InfoTrac)*, Eighth Edition. Belmont, CA: Wadsworth Publishing, 2003.
- Soble, Ronald L., and Robert E. Dallos. *The Impossible Dream: The Equity Funding Story, the Fraud of the Century*. New York, NY: New American Library, 1975.
- Stephenson, Peter. *Investigating Computer-Related Crime: Handbook for Corporate Investigators*. Boca Raton, FL: CRC Press, 1999.
- Tomes, Jonathan P. *Fraud, Waste, Abuse and Safe Harbors: A Guide for the Healthcare Professional*. Chicago, IL: Probus Publishing, 1993.
- Tomes, Jonathan P. *Healthcare Fraud, Waste, Abuse, and Safe Harbors: The Complete Legal Guide*. Chicago, IL: Probus Publishing, 1993.
- United States Congress. *Federal Efforts to Combat Fraud, Abuse, and Misconduct in the Nation's S & L's and Banks*. Washington, DC: U.S. G.P.O., 1990.
- Wadlow, Thomas A. *The Process of Network Security: Designing and Managing a Safe Network*. Reading MA: Addison Wesley Longman, 2000.
- Wellman, Francis L. *The Art of Cross-Examination*. New York, NY: Dorset Press, 1997.
- Wells, Joseph T. *Occupational Fraud and Abuse*. Austin, TX: Association of Certified Fraud Examiners, 1997.
- White-Collar Crime: Loss Prevention Through Internal Control*. Report prepared for Chubb Group of Insurance Companies by Ernst & Young. See www.chubb.com.
- Williams, Howard E. *Investigating White-Collar Crime: Embezzlement and Financial Fraud*. Springfield, IL: C.C. Thomas, 1997.

WEB SITES WITH FRAUD RELATED TOPICS

Approximately 1,200 new Web sites are created every day and an untold number become derelict. It is important, therefore, to understand that no list can ever be up-to-date or guarantee accuracy.

The AFU and Urban Legends Archive. www.urbanlegends.com

This site separates the myriad hoaxes on the Internet (and in society) from those with a grain or more of truth.

American College of Forensic Examiners. www.acfe.com

The American College of Forensic Examiners has more than 15,000 members and is a networking opportunity for forensic science experts of all disciplines. It is the largest association established for forensic experts of all disciplines to promote continuing education, networking and seminars, conferences, workshops, Internet, continuing education courses, and home study courses.

Asiaweek.com. www.asiaweek.com

This newsmagazine Web site also includes a list of the region's 1,000 largest companies and 500 largest banks.

Association of Certified Forensic Investigators of Canada (The).

www.homewoodave.com

This nonprofit Canadian organization's objective is to promote and foster a national forum and governing body for the affiliation of professionals who provide to the public, governments, and employers their expertise and services in the areas of fraud prevention, detection, and investigation.

Association of Certified Fraud Examiners (The). www.cfenet.com

This is the Web site for The Association of Certified Fraud Examiners, an international, 25,000-member professional organization dedicated to fighting fraud and white-collar crime. With offices in North America and chapters around the globe, the Association is networked to respond to the needs of antifraud professionals anywhere in the world.

Billy's Money Laundering Information Website. www.laundryman.u-net.com

This site provides information about UK Government money laundering laws. This is not a government authorized site, however, some of the interesting and valuable material includes an overview of the business areas prone to money laundering activities, UK legislation, money laundering offenses, and international initiatives in place to prevent this crime.

Business Credit USA. www.businesscreditusa.com/index.asp

Offers free and inexpensive credit ratings, credit reports, and customer opinions on 12 million businesses.

Business Roundtable (BRT). www.brtable.org

The Business Roundtable is an association of chief executive officers of leading U.S. corporations. The BRT is committed to advocating public policies that foster vigorous economic growth, a dynamic global economy, and a well-trained and productive U.S. workforce essential for future competitiveness. The BRT's *Corporate Governance Task Force* focuses on issues related to corporate governance and responsibilities, including accounting standards

California Business Search Program. www.ss.ca.gov/automate.htm

Allows you to search California corporations, limited partnerships, and limited liability company databases. Provides access to more than two million records with frequently requested business entity information, such as status, Secretary of State file number, date of filing, and agent for service of process. The information is not a complete file and is currently updated weekly rather than daily.

ChinaOnline. www.chinaonline.com

This daily online paper provides real-time, in-depth news and information about the rapidly growing Chinese marketplace, including industry updates, analyses and in-depth reports, and company and media profiles, including fraud-newsworthy events.

Committee of Sponsoring Organizations of the Treadway Commission.

www.coso.org

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. Originally formed in 1985 to sponsor the National Commission of Fraudulent Financial Reporting, COSO has released numerous influential publications including *Internal Control—Integrated Framework*.

Note: See “Struggling to incorporate the COSO recommendations into your audit process? Here’s one audit shop’s winning strategy” by Dennis Applegate and Ted Wills (from the December 1999 issue of *Internal Auditor*) at www.coso.org/Articles/audit_shop.htm.

Conference Board. www.conference-board.com

The Conference Board is a global, independent membership organization that creates and disseminates knowledge about management and the marketplace to help businesses strengthen their performance and better serve society. They conduct research, convene conferences, make forecasts, assess trends, publish information and analysis, and bring executives together to learn from one another. The Conference Board’s *Blue-Ribbon Commission on Public Trust and Private Enterprise* has proposed reforms to strengthen corporate compensation practices and help restore trust in America’s corporations and capital markets.

Consumer Scams in Canada. www.canadaonline.about.com/cs/scams/

This Web site provides warnings, alerts, and safety precautions to protect you from Canadian scams and fraud, online and offline. It includes consumer information and assistance, invention company scams, and job scams, Net hoaxes, 1-900 phone scams, cheque fraud, counterfeit bank notes, online auction fraud, phone fraud, telemarketing fraud, and the latest RCMP fraud cases.

Corporate Board Member. www.boardmember.com

Corporate Board Member magazine’s website, Boardmember.com, serves as a central resource for officers and directors of publicly traded corporations, top private companies, and Global 1000 firms. Their Resource Center offers the full-text of *Corporate Board Member* magazine, as well as additional articles, webcasts, and interviews. Topics include corporate governance, strategic board trends and issues, executive and director compensation, audit committees, risk management, international and technology trends, investor relations, board education, and other critical topics facing today’s directors and officers of publicly traded companies. They also offer conferences, director training programs, roundtables, an extensive database, and timely research.

The Corporate Library. www.thecorporatelibrary.com

The Corporate Library serves as a central repository for research, study and critical thinking about the nature of the modern global corporation, with a special focus on corporate governance and the relationship between company management, their boards and shareholders. Most general content on the site is open to visitors at no cost; advanced research relating to specific companies and certain other advanced features are restricted to subscribers only.

Cybercrime.gov. www.cybercrime.gov

The Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division U.S. Department of Justice is responsible for implementing a comprehensive program designed to address the growing threat of computer and intellectual property crime. Their Web site contains links, information, and other resources for consumers, parents, and law enforcement personnel about cybercrime and other computer-aided scams and schemes.

Escrow.com. www.escrow.com

Escrow.com, founded in 1999 by Fidelity National Financial, is a privately held company providing secure business and consumer transaction management on the Internet. Its Web site provides an overview of the escrow process, and information and resources related to fraudulent use of the escrow process in the online environment.

Ethics Officers Association (EOA). www.eoa.org

The EOA is the professional association exclusively for managers of ethics, compliance and business conduct programs. The EOA provides ethics officers with training and a variety of conferences and meetings for exchanging best practices in a frank, candid manner.

Ethics Resources Center (ERC). www.ethics.org

The ERC is a nonprofit, nonpartisan educational organization whose vision is a world where individuals and organizations act with integrity. Their mission is to strengthen ethical leadership worldwide by providing leading-edge expertise and services through research, education and partnerships. Especially useful are their resources on business and organizational ethics.

Experts.com. www.experts.com

This is an extensive directory of qualified and professional experts from all over the world in many areas of expertise. Experts.com promotes and matches high-level expert professionals with individual business or legal needs.

Federal Deposit Insurance Corporation. www.fdic.gov

The Federal Deposit Insurance Corporation (FDIC), created in 1933, is an independent agency of the federal government whose stated mission is to preserve and promote public confidence in the U.S. financial system by insuring deposits in banks and thrift institutions for up to \$100,000; by identifying, monitoring and addressing risks to the deposit insurance funds; and by limiting the effect on the economy and the financial system when a bank or thrift institution fails. More on the FDIC can be found at its Web site which also contains information on deposit

insurance, consumer protection, industry analysis, regulation and examination, asset sales, and other topics.

Fighting Fraud and Corruption.

<http://www.ex.ac.uk/~RDavies/arian/scandals/fight.html>

This site provides links to a host of other fraud-related Web sites that include professional bodies, investigative services, forensic accounting firms, pressure groups, and so on.

Financial Executives International (FEI). www.fei.org

FEI is the preeminent professional association for senior level financial executives including Chief Financial Officers, VPs of Finance, Controllers, Treasurers, and Tax Executives. They provide peer networking opportunities, emerging issues alerts, personal and professional development and advocacy services.

Financial Services Regulation. www.fsa.gov.uk

The Financial Services Authority is an independent body that regulates the financial services industry in the UK. The FSA has four objectives under the Financial Services and Markets Act 2000, which are to maintain market confidence; promote public understanding of the financial system; protect consumers; and fight financial crime.

Firstgov.gov. www.firstgov.gov

Firstgov.gov is the official U.S. gateway to all government information with a comprehensive search engine allowing the user to search through millions of pages (many not available elsewhere) from federal and state governments, the District of Columbia and U.S. territories.

Fraudnet. www.auditnet.org/fraudnet.htm

Fraudnet is a specialized section of AuditNet® that provides an opportunity for auditors and financial professionals around the world to share (via submissions) fraud policies, procedures, code of ethics, and other resources.

Fraud Watch International (FWI). www.fraudwatchinternational.com

Fraud Watch International is a web portal, based in Australia, that contains links and other resources directed at combating Internet fraud scams such as “phishing” and protecting consumers from identity theft and other concerns.

Harvard Business School's Corporate Governance, Leadership & Values.

www.cglv.hbs.edu

Harvard Business School's Corporate Governance, Leadership & Values website is a comprehensive overview of research, educational programs, and other activities at Harvard Business School aimed at providing new frameworks for thought and practice in the interrelated areas of corporate governance, leadership, and values. It includes links to the on-going workshop series; background papers; research programs, such the Corporate Governance Initiative; executive education programs; viewpoints on key issues published in the national press; faculty comments in the media; and an on-line forum for exchanging views on emerging issues.

Information Systems Audit and Control Association (ISACA). www.isaca.org

Founded in 1969, the Information Systems Audit and Control Association® (ISACA®) is an organization devoted to issues related to IT governance, control, security and assurance. ISACA sponsors international conferences, publishes the Information Systems Control Journal,[™] develops international information systems auditing and control standards, and administers the Certified Information Systems Auditor[™] (CISA®) designation and the Certified Information Security Manager[™] (CISM[™]) designation.

Institute of Chartered Accountants in England and Wales. www.icaew.co.uk

This is the Web site of the largest professional accountancy body in Europe, with more than 120,000 members. Information contained includes professional standards, library and information services, policy, education and training and an online directory of over 25,000 CA firms worldwide.

The Institute of Internal Auditors (IIA). www.theiaa.org

The Institute of Internal Auditors is a dynamic international organization that meets the needs of a worldwide body of internal auditors. IIA focuses on issues in internal auditing, governance and internal control, IT audit, education, and security worldwide. The Institute provides internal audit practitioners, executive management, boards of directors and audit committees with standards, guidance, best practices, training, research, and technological guidance for the profession.

Institute of Management Accountants (IMA). www.imanet.org

The IMA is a leading professional organization devoted to management accounting and financial management. Its goals are to help members develop both personally and professionally, by means of education, certification, and association with other business professionals. A respected leader within the global financial community, the IMA influences the concepts and ethical practices in management accounting and financial management. Its ethical standards provide guidance to practitioners for maintaining the highest levels of ethical conduct.

IT Governance Institute (ITGI). www.itgi.org

Established by the Information Systems Audit and Control Association and Foundation (ISACA) in 1998, the IT Governance Institute (ITGI) exists to assist enterprise leaders in understanding and guiding the role of IT in their organizations. ITGI helps senior executives to ensure that IT goals align with those of the business, deliver value, and perform efficiently, while IT resources are properly allocated and its risks mitigated. Through original research, symposia and electronic resources, ITGI helps ensure that boards and executive management have the tools and information they effectively manage the IT function.

InsuranceFraud.com. www.insurancefraud.com

This Web site links organizations and professionals in the anti-insurance fraud community. It provides a unique forum for the anti-fraud executives and independent professionals who do not normally have the resources on hand to identify insurance fraud and abuse in the industry, to quickly investigate and subsequently recover from the fraudster's activities, and/or to identify ways to

prevent the occurrence or recurrence of fraud in the insurance industry. It includes a data base listing of anti-fraud professionals, vendors, and regulators.

International Association of Financial Crimes Investigators. www.iafci.org

This organization was formed by a small group of law enforcement officers and special agents of the credit card industry to represent the professional fraud investigator. The Association, a nonprofit international organization, provides services and facilitates the collection and exchange of information about financial fraud, fraud investigation and fraud prevention methods.

Internet Fraud Complaint Center (IFCC). www.ifccfbi.gov

The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).

Its mission is to address fraud committed over the Internet. For victims of Internet fraud, IFCC provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation. For law enforcement and regulatory agencies at all levels, IFCC offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides timely statistical data of current fraud trends.

Internet Scambusters. www.scambusters.org

This Web site provides information about the latest Internet frauds and scams as well as virus updates.

National Association of Corporate Directors (NACD). www.nacdonline.org

Founded in 1977, the NACD is the premier educational, publishing and consulting organization in board leadership and the only membership association for boards, directors, director-candidates and board advisors. The NACD promotes high professional board standards, creates forums for peer interaction, enhances director effectiveness, asserts the policy interests of directors, conducts research, and educates boards and directors concerning traditional and cutting-edge issues.

National Bureau of Asian Research. www.nbr.org

The National Bureau of Asian Research (NBR) is a nonprofit, nonpartisan institution that conducts advanced research on policy-relevant issues in Asia. It also serves as the global clearinghouse for Asia research conducted by specialists and institutions worldwide.

National Check Fraud Center. www.ckfraud.org

This private organization provides nationwide, updated multisource intelligence to support local law enforcement, federal agencies and the financial and retail communities in the detection, investigation, and prosecution of known check fraud and other white collar crimes.

National Fraud Information Center (The). www.fraud.org

The NFIC offers consumers advice about promotions in cyberspace and route reports of suspected online and Internet fraud to the appropriate government agencies. The NFIC was originally established in 1992 by the National Consumers

League, the oldest nonprofit consumer organization in the United States, to fight the growing menace of telemarketing fraud by improving prevention and enforcement. The NFIC provides the only nationwide toll-free hotline for consumers to get advice about telephone solicitations and report possible telemarketing fraud to law enforcement agencies.

New York Stock Exchange (NYSE). www.nyse.com

The New York Stock Exchange is a not-for-profit corporation that provides a self-regulated marketplace for the trading of financial instruments. Its goal is to add value to the capital-raising and asset-management process by providing the highest-quality and most cost-effective trading environment. They work to promote confidence in and understanding of the financial trading process and serve as a forum for discussion of relevant national and international policy issues. They have taken the lead in corporate governance issues through their participation in the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees and more recently in their formation of the NYSE Corporate Responsibility and Listing Standards Committee.

Nigeria–The 419 Coalition. <http://home.rica.net/alphae/419coal/>

This Web site is operated by “The 419 Coalition” and provides an overview and tips for combating the prevalence worldwide of an e-mail scam which has been reportedly run out of Nigeria (under successive governments) since the early 1980s. The financial damage caused by the scam is estimated at five billion dollars (in US\$) by the coalition. The scam has also been referred to as “advance fee fraud”, “419 fraud” (four-one-nine) after the relevant section of the criminal code of Nigeria, and “the Nigerian connection” (mostly in Europe).

Privacy Rights Clearinghouse (PRC). www.privacyrights.org

Founded in 1992, and mostly grant-supported, the Privacy Rights Clearinghouse (PRC) is a nonprofit consumer organization that provides consumer information and consumer advocacy. Its stated goals involve consumer privacy issues: raising consumer awareness of how their personal information is used and how to protect it; responding and documenting specific privacy related complaints, such as identity theft; and advocating for consumers’ privacy rights with policy makers (local, state, and federal), as well as industry representatives, consumer advocates, and the media.

Public Company Accounting Oversight Board (PCAOB). www.pcaobus.org

The Public Company Accounting Oversight Board (PCAOB) is a private-sector, non-profit corporation, created by the Sarbanes-Oxley Act of 2002, to oversee the auditors of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports.

Sinosource. www.sinosource.com

This is a private, Internet-based business info provider in China to help foreign business, particularly small- and middle-sized companies, communicate directly with businesses in China. Includes a business directory of China.

Statistics Singapore. www.singstat.gov.sg

This is the national statistical authority responsible for disseminating official statistics on Singapore.

U.S. Federal Trade Commission (FTC). <http://www.ftc.gov/index.html>

The Federal Trade Commission (FTC), founded in 1914, stated mission is to ensure that U.S. markets are vigorous, efficient and free of restrictions that harm consumers. The FTC enforces federal consumer protection laws that prevent fraud, deception and unfair business practices. The Commission also enforces federal antitrust laws that prohibit anticompetitive mergers and other business practices that restrict competition and harm consumers. Its site contains tips on combating telemarketing fraud, Internet scams, price-fixing schemes, identity theft, and other resources to protect consumers.

U.S. Securities and Exchange Commission. <http://www.sec.gov/consumer/cyberfr.htm>

This site provides valuable information about Internet fraud and how to avoid Internet investment scams. This alert tells you how to spot different types of Internet fraud, what the SEC is doing to fight Internet investment scams, and how to use the Internet to invest wisely.

Note. The following two articles may be of particular background interest to fraud practitioners:

“Internet Fraud: How to Avoid Internet Investment Scams” found at <http://www.sec.gov/investor/pubs/cyberfraud.htm>, and

“The Numbers Game”, a speech presented to the New York University Center for Law and Business by then SEC Chairman Arthur Levitt on Sept. 28, 1998, found at <http://www.sec.gov/news/speech/speecharchive/1998/spch220.txt>

Vodatel Networks Holdings Limited. www.irasia.com

This is an investor relations site that includes profiles of publicly listed South Asian companies. It has annual reports, press releases, stock quotes, and so on.

Yahoo Internet Business-Fraud section. See the following link:

http://dir.yahoo.com/Computers_and_Internet/Internet/Business_and_Economics/Fraud/

This section on Yahoo has links to sites dealing with specific Internet scams and other fraudulent schemes found on the World Wide Web.

AICPA SOFTWARE LICENSE AGREEMENT

Fraud Prevention Checklists CD-ROM (2006-2007)

Copyright © 2006 AICPA

All rights reserved.

LICENSE AGREEMENT

The *Fraud Prevention Checklists CD-ROM* provided with *The CPA's Handbook of Fraud and Commercial Crime Prevention* contains electronic versions of the checklists and other materials found in the book. Subject to the conditions in this License Agreement and the Limited Warranty herein, you may duplicate the files on this disk and/or modify them as necessary for your internal use only.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the AICPA. Reproduction prohibitions do not apply to the checklists, forms, worksheets, sample correspondence, and any other sample documents contained in this product, when reproduced for personal use only. This material may NOT be reproduced for commercial exploitation, unless prior permission is obtained from the AICPA's Copyright Permission Office.

Limited Warranty

AICPA warrants that the program will substantially conform to the published specifications and to the documentation, provided that it is used on the computer hardware and with the operating system for which it was designed. AICPA also warrants that the magnetic media on which the program is distributed and the documentation are free from defects in materials and workmanship. AICPA will replace defective media at no charge, provided you return the item with the original packaging with the book to AICPA within 90 days of the date of delivery.

Except as specifically provided above, AICPA makes no warranty or representation, either express or implied, with respect to this program or documentation.

In no event will AICPA be liable for direct, indirect, special incidental, or consequential damages arising out of the use of or inability to use the program or documentation, even if advised of the possibility of such damages. Specifically, AICPA is not responsible for any costs including, but not limited to, those incurred as result of lost profits or revenue, loss of use of the computer program, loss of data, the costs of recovering such programs or data, the cost of any substitute program, claims by third parties, or for other similar costs. In no case shall AICPA's liability exceed the amount of the license fee (ie: cost of product).

The warranty and remedies set forth above are exclusive and in lieu of all others, oral or written, express or implied. No AICPA dealer, distributor, agent, or employee is authorized to make any modification or addition to this warranty.

Some states do not allow the exclusion or limitation of implied warranties or limitation for incidental or consequential damages, so the above limitation or exclusion may not apply to you. In the U.K., this warranty does not affect the statutory rights of a consumer.

General

The material on this CD-ROM is designed to provide information in regard to the subject matter covered and does not represent an official position of the American Institute of Certified Public Accountants, and is distributed with the understanding that the publisher, authors, and editors are not rendering legal, accounting, or other professional services on this CD-ROM. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

AICPA retains all rights not expressly granted. Nothing in this License Agreement constitutes a waiver of AICPA's rights under the copyright laws or any other Federal or State law.

INSTALLATION OF THE FRAUD PREVENTION CHECKLISTS CD-ROM

Installation: Open *Word for Windows* on your screen and insert the *Fraud Prevention Checklists CD-ROM* into your computer's CD-ROM drive (d or e). Go to the file button and select *open* (with disk drive d or e selected). A list of files and folders will appear. *All Files* or *Word Documents* should be selected in the dialog box. Select the file you want to open from one of the folders included in the CD-ROM. You can now work on the file you have selected.

There are 14 folders of material found on the CD-ROM:

1. Chapter 1, Risk Management Checklist,
2. Chapter 2, Ethical Environment Checklist,
3. Chapter 3, Fraud Insurance Checklist,
4. Chapter 4, Computer Security Checklists,
5. Chapter 8, Computer Crime Checklists,
6. Chapter 9, Dealing with a Known or Suspected Fraud Checklist,
7. Chapter 10, Detection of Financial Statement Fraud Checklist, Sarbanes-Oxley Checklist,
8. Chapter 11, Corporate Security Checklists,
9. Chapter 12, Bankruptcy Fraud Checklist,
10. Chapter 13, Procurement Fraud Checklist,
11. Chapter 14, Detection of Personal Identity Theft and Corporate Identity Fraud Checklist,
12. Appendix A, Industry Sector by Sector Checklists,
13. Appendix B, Statement on Auditing Standards No. 99,
14. Additional Fraud Resources.

Note on Fonts: The exhibits on the CD-ROM (with the exception of Exhibit A from Chapter 12, Appendix B: SAS 99, and Resource 3: AICPA/CICA Privacy Framework) were produced in *Word for Windows 2000* using True Type fonts. If you do not have this version of *Word* or this font library available, the exhibits may not convert correctly. You will have to substitute a different font and may have to replace/correct formatting that does not convert correctly.

PDF Documents: In order to view/use the Chapter 12 Exhibit A, Appendix B SAS 99, and the AICPA/CICA Privacy Framework material, you must have Adobe Acrobat Reader to view the portable document format (pdf) files. Go to www.adobe.com and download the Adobe Acrobat Reader following the Web site's instructions. Once the Adobe Acrobat Reader is installed on your computer you can access the pdf files on the *Fraud Prevention Checklists CD-ROM*.

Saving Files: You cannot overwrite the *Fraud Prevention Checklists CD-ROM*. If you plan to continually use and update the checklist files with client or other information, use the *Save As* feature when saving a file with new information for the first time. Go to the *File* button and select *Save As*. Save the file selected under a new name that you will remember for later use. Direct the saved file to your hard drive or other location as appropriate for your needs.

As a general rule, remember to save your data frequently. If you use the *Save* function the first time you save your work, you will overwrite the template. This means that you will have to clean up your saved file to return it to its original format or reload the file from the CD-ROM again.

The CPA's Handbook of Fraud and Commercial Crime Prevention
Updating Letter—Supplement 6—2006

| Page Description | Discard These Handbook Pages (Chapter/Page) | Insert These 2006 Supplement Pages (Chapter/Page) |
|--|---|---|
| Title Page | Title Page | Title Page |
| Table of Contents | iii-viii | iii-viii |
| Preface | ix to xiv | ix to xiv |
| Acknowledgments | xv | xv |
| About the Authors | xvii to xxi | xvii to xxi |
| Chapter 1: "Managing the Risk of Fraud" | 1 to 32 | 1 to 38 |
| Chapter 8: "Computer Crime, Computer Criminals, and Computer Evidence" | 1 to 49 | 1 to 58 |
| Chapter 10: "Reducing the Risk of Financial Statement Fraud" | 1 to 115 | 1 to 121 |

NOTE: The 2006–2007 *Fraud Prevention Checklists CD-ROM*, included with Supplement 6, replaces the 2005–2006 edition. The 2006–2007 edition updates and reorganizes files for quicker access and easier search, adds new "Resources," including links to SAS 99 and related materials, and adds an overview of the AICPA Anitfraud & Corporate Responsibility Center and AICPA's Audit Committee Effectiveness Center, including links to numerous additional resources on the Centers.

This completes the filing of Fraud Supplement Six.

Upon completion, insert this Update Letter behind the "Filing Instructions" tab card.

AICPA SOFTWARE LICENSE AGREEMENT

Fraud Prevention Checklists CD-ROM (2005-2006)
Copyright © 2005 AICPA
All rights reserved.

LICENSE AGREEMENT

The *Fraud Prevention Checklists CD-ROM* provided with *The CPA's Handbook of Fraud and Commercial Crime Prevention* contains electronic versions of the checklists and other materials found in the book. Subject to the conditions in this License Agreement and the Limited Warranty herein, you may duplicate the files on this disk and/or modify them as necessary for your internal use only.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission the AICPA. Reproduction prohibitions do not apply to the checklists, forms, worksheets, sample correspondence, and any other sample documents contained in this product, when reproduced for personal use only. This material may NOT be reproduced for commercial exploitation, unless prior permission is obtained from the AICPA's Copyright Permission Office.

Limited Warranty

AICPA warrants that the program will substantially conform to the published specifications and to the documentation, provided that it used on the computer hardware and with the operating system for which it was designed. AICPA also warrants that the magnetic media on which the program is distributed and the documentation are free from defects in materials and workmanship. AICPA will replace defective media at no charge, provided you return the item with the original packaging with the book to AICPA within 90 days of the date of delivery.

Except as specifically provided above, AICPA makes no warranty or representation, either express or implied, with respect to this program or documentation.

In no event will AICPA be liable for direct, indirect, special incidental, or consequential damages arising out of the use of or inability to use the program or documentation, even if advised of the possibility of such damages. Specifically, AICPA is not responsible for any costs including, but not limited to, those incurred as result of lost profits or revenue, loss of use of the computer program, loss of data, the costs of recovering such programs or data, the cost of any substitute program, claims by third parties, or for other similar costs. In no case shall AICPA's liability exceed the amount of the license fee (ie: cost of product).

The warranty and remedies set forth above are exclusive and in lieu of all others, oral or written, express or implied. No AICPA dealer, distributor, agent, or employee is authorized to make any modification or addition to this warranty.

Some states do not allow the exclusion or limitation of implied warranties or limitation for incidental or consequential damages, so the above limitation or exclusion may not apply to you. In the U.K., this warranty does not affect the statutory rights of a consumer.

General

The material on this CD-ROM is designed to provide information in regard to the subject matter covered and does not represent an official position of the American Institute of Certified Public Accountants, and is distributed with the understanding that the publisher, authors, and editors are not rendering legal, accounting, or other professional services on this CD-ROM. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

AICPA retains all rights not expressly granted. Nothing in this License Agreement constitutes a waiver of AICPA's rights under the copyright laws or any other Federal or State law.

INSTALLATION OF THE FRAUD PREVENTION CHECKLISTS CD-ROM

Installation: Open *Word for Windows* on your screen and insert the *Fraud Prevention Checklists CD-ROM* into your computer's CD-ROM drive (d or e). Go to the file button and select *open* (with disk drive d or e selected). A list of files and folders will appear. *All Files* or *Word Documents* should be selected in the dialog box. Select the file you want to open from one of the folders included in the CD-ROM. You can now work on the file you have selected.

There are 5 folders of material found on the CD-ROM:

1. Fraud Chapter checklists folder,
2. Appendix A complete folder (text and checklists),
3. Sector-by-Sector checklists folder,
4. Other Handbook materials folder (includes Appendix B, SAS 99, Chapter 12 Exhibit A material, and other sample documents)
5. Additional Fraud Resources folder [includes "Ethics and Fraud In Business: Cases and Commentary," Resource 1: "Implementing An Ethics Strategy," Resource 2: "Designing An Ethics Training Program," Resource 3: "the AICPA/CICA Privacy Framework (Including the AICPA/CICA Trust Services Privacy Principle and Criteria)," and Resource 4: "Evaluating the Independent Auditor: Questions to Consider"].

Note on Fonts: The exhibits on the CD-ROM (with the exception of Exhibit A from Chapter 12, Appendix B: SAS 99, and Resource 3: AICPA/CICA Privacy Framework) were produced in *Word for Windows 2000* using True Type fonts. If you do not have this version of *Word* or this font library available, the exhibits may not convert correctly. You will have to substitute a different font and may have to replace/correct formatting that does not convert correctly.

PDF Documents: In order to view/use the Chapter 12 Exhibit A, Appendix B SAS 99, and the AICPA/CICA Privacy Framework material, you must have Adobe Acrobat Reader to view the portable document format (pdf) files. Go to www.adobe.com and download the Adobe Acrobat Reader following the Web site's instructions. Once the Adobe Acrobat Reader is installed on your computer you can access the pdf files on the *Fraud Prevention Checklists CD-ROM*.

Saving Files: You cannot overwrite the *Fraud Prevention Checklists CD-ROM*. If you plan to continually use and update the checklist files with client or other information, use the *Save As* feature when saving a file with new information for the first time. Go to the *File* button and select *Save As*. Save the file selected under a new name that you will remember for later use. Direct the saved file to your hard drive or other location as appropriate for your needs.

As a general rule, remember to save your data frequently. If you use the *Save* function the first time you save your work, you will overwrite the template. This means that you will have to clean up your saved file to return it to its original format or reload the file from the CD-ROM again.

The CPA's Handbook of Fraud and Commercial Crime Prevention
Updating Letter—Supplement 5—2005

| Page Description | Discard These Handbook Pages (Chapter/Page) | Insert These 2005 Supplement Pages (Chapter/Page) |
|--|---|---|
| Title Page | Title Page | Title Page |
| Table of Contents | iii-ix | iii-viii |
| Preface | xi to xvi | ix to xiv |
| Acknowledgments | xvii | xv |
| About the Authors | xix to xxiii | xvii to xxi |
| Chapter 2: "Promoting an Ethical Environment" | 3 to 4 | 3 to 4 |
| Chapter 8: "Computer Crime, Computer Criminals, and Computer Evidence" | TOC | TOC |
| | 25 to 28 | 25 to 28.4 49 |
| Chapter 9: "Dealing with a Known or Suspected Fraud" | 9 to 10.1 | 9 to 10.18 |
| Chapter 10: "Reducing the Risk of Financial Statement Fraud" | TOC | TOC |
| | 67 to 86 | 67 to 115 |
| Chapter 13: "Detecting Procurement Fraud" | TOC | TOC |
| | 3 to 47 | 3 to 60 |
| Appendix A: "Fraud Sector-By-Sector" | Delete Tab card, TOC, and pages 3 to 87 | Entire chapter has moved to the Fraud Prevention Checklists CD-ROM. |
| Glossary | 1 to 35 | 1 to 36 |
| Bibliography (Suggested References) | 1 to 10 | 1 to 12 |

NOTE: The 2005-2006 *Fraud Prevention Checklists CD-ROM*, included with Supplement 5, replaces the 2004-2005 edition. The 2005-2006 edition contains new checklists for chapters 8, 10, and 13, as well as the entire Appendix A Sector-by-Sector chapter and additional fraud checklists and resources.

This completes the filing of Fraud Supplement Five.

Upon completion, insert this Update Letter behind the "Filing Instructions" tab card.