2000

CPA WebTrust practitioners' guide

Christopher J. Leach

WebTrust Practitioners' Guide

AICPA

American Institute of Certified Public Accountants

AICPA Practice Aid Series

CPA WebTrust℠

Practitioners' Guide

AICPA

AICPA Practice Aid Series

CPA WebTrust℠ Practitioners' Guide

Written by
Christopher J. Leach, CPA

Edited by
Accounting and Auditing Publications Staff

American Institute of Certified Public Accountants

AICPA

AICPA Practice Aid Series

CPA WebTrust Practitioners' Guide

Written by
Christopher J. Leach, CPA

Edited by
Accounting and Auditing
Publications Staff

American Institute of Certified Public Accountants

AICPA

NOTICE TO READERS

WebTrust Practitioners' Guide presents the views of the author and others who helped in its development. This publication has not been approved, disapproved, or otherwise acted upon by any senior technical committees of the American Institute of Certified Public Accountants. Therefore, the contents of this publication, including recommendations and suggestions, have no official or authoritative status.

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

ACKNOWLEDGMENTS

The author wishes to thank those who have been so supportive in the creation of this guide. First to Casey Bennett, former director of the WebTrust program, who always had a way of getting me to think outside the box. To Sheryl Weiner, WebTrust team leader, who pushed this work forward while keeping up with the demands of WebTrust, and to Anthony Pugliese, director of Assurance Services at the AICPA, who continues to provide needed leadership for the continued support of WebTrust. Special mention needs also to be given to Everett Johnson who has always been a role model and to the task force members who continue to donate time and energy to the success of the program. Also to all of the WebTrust licensees, who are putting this program in action, for their vision and dedication when others say it can't be done. And finally to my wife Lynette who has always been the wind beneath my wings, without whose support I could not accomplish the tasks placed before me.

Table of Contents

Preface[1]

For the CPA/CA practitioner who seeks additional guidance in planning and executing a *WebTrust*^{SM} engagement, there is assistance available. This book will provide you with insightful data about actual WebTrust engagements by presenting information based on practical WebTrust engagement experience.

A word here about WebTrust terms and definitions is in order. The rate of development of new terms relating to this rapidly expanding field is explosive. Therefore, we've included an Internet Dictionary in Appendix A. However, because of the rapidly developing field with its related new technology and terms, it might be a good idea to visit the website http://www.dictionary.com for additional assistance with required terms.

A note about the field of eCommerce before we begin. The area of eCommerce, by its nature, is an ever-changing and exciting practice area that provides new practice opportunities for the proactive accountant. Because of the rapid and constant transformation of technology and eCommerce, we can expect information about WebTrust Principles and Criteria to change often. Therefore, we plan to update this manual as needed to reflect the important changes in the technology industry as they relate to WebTrust and eCommerce issues for the practitioner.

We know that the wave of technology and all the related changes it brings is upon us and is unavoidable. We can choose to either act and ride this wave, or we can choose to do nothing and let it bury us. The outcome is up to us, the practitioners, to find a way to move along with the wave and become aware. Becoming knowledgeable about technology and involved in eCommerce and WebTrust will go a long way toward providing us with the tools and information we need to service clients better in this electronic age.

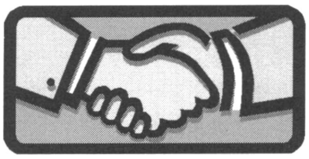
It is my hope that as we explore this new vista we will learn together how to better serve our clients and the public in general. Should you have comments or suggestions for updates to this material, I hope you will let me know. I look forward to hearing from you. As always—good computing and good luck!

[1] The procedures and opinions expressed in this book are not intended to be authoritative. Rather, they are the opinions of this author, and are to be relied upon in the context of providing guidance in the WebTrust area. We encourage each of you to modify the procedures provided to meet the practices followed by the firm in which you practice.

The WebTrust Engagement — Getting Started

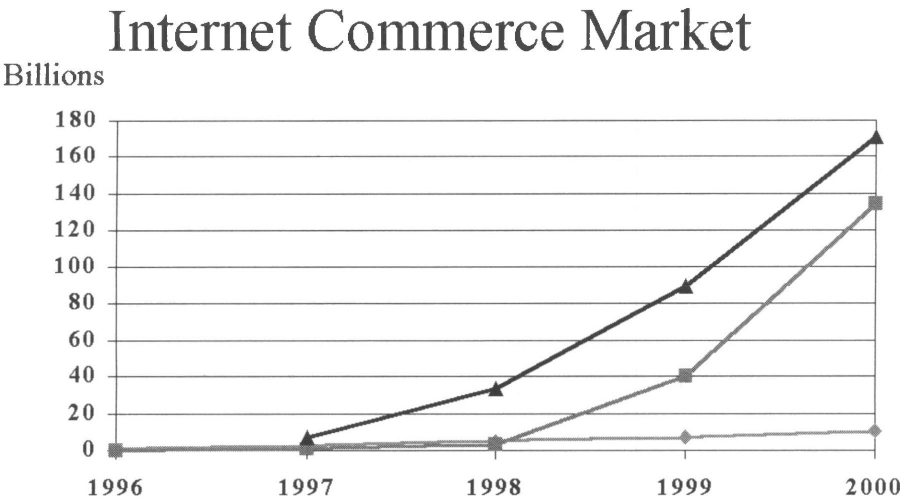
CHAPTER ONE

The WebTrust Engagement—Getting Started



WEBTRUST: A BRIEF OVERVIEW

The following exhibit, Internet Commerce Market, illustrates the rapid growth predicted for the Internet commerce market. Although various information sources debate the size of the market, most experts tend to agree that the years 1997 to 1998 marked the beginning of tremendous Internet commerce growth and related market opportunity for accountants and their clients. This opportunity still exists today!



Source: The Yankee Group, 1996 and 1997

"The total value of goods and services traded between companies over the Internet will reach $8 billion this year and $327 billion in the year 2002," according to Forrester Research. Service and responsiveness to consumer concerns will replace price and brand name as the major components in the consumer decision-making process. As accountants, we should take the lead in empowering clients in this global eCommerce market place.

Our profession is becoming more responsive to both the business consumer and the individual consumer. In response to consumer concerns regarding transacting business on-line, the WebTrust program was developed and continues to evolve for the ever-changing eCommerce marketplace.

Never before in the history of the accounting profession have we had the type of opportunity this WebTrust program offers: to make a direct impact on the bottom line of our clients' financial statements as well as tame the market channel known as the World Wide Web. Let's turn now to a discussion of the WebTrust family of products to better understand the WebTrust framework.

WebTrust: Its Family

The WebTrust "family" of products includes WebTrust for Business-to-Consumer electronic commerce and WebTrust-ISP for Internet Service Providers in electronic commerce. Practitioners may wish to refer to the "Guide to Auditors and Users of a Third-Party Service Provider Audit Report in a WebTrust Engagement." You can download this document from the AICPA's website at http://ftp.aicpa.org/public/download/webtrust/tpsp625.doc. This guidance is similar to the type of report described in SAS No. 70, "Reports on the Processing of Transactions by Service Organizations," (AICPA, *Professional Standards*, vol. 1, sec. 324). Under current development by the Electronic Commerce Assurance Task Force is WebTrust for Certification Authorities and WebTrust for the Business-to-Business marketplace.

For an Internet site to be considered for a WebTrust engagement, it must have embodied all WebTrust principles and criteria for a **minimum** of two months. If, during the two-month period, there have only been a minimal number of transactions, practitioners should consider a longer period of time as a requirement. This time-related requirement is in place to provide ample opportunity for the site to test and evaluate its own policies and procedures.

The constant state of change of the Internet and its corresponding technologies will require changes and updates to WebTrust whose principles and criteria are the core of this program.

WebTrust Principles and Criteria: Business-to-Consumer

WebTrust for Business-to-Consumer electronic commerce covers three broad areas that we refer to as principles: (1) Business Practices and Information Privacy Practices, (2) Transaction Integrity Controls, and (3) Information Protection Controls. These three principles and the corresponding criteria that support these principles are the basis of the examination for WebTrust for Business-to-Consumer electronic commerce. The most current version of the principles and criteria can be found at http://www.aicpa.org/webtrust/princrit.htm.

WebTrust Priniciples and Criteria: ISP

WebTrust-ISP for Internet Service Providers in electronic commerce, although similar to the WebTrust for consumers, focuses on the business-to-business transaction between an ISP and its customer. This program concentrates on four broad principles: (1) Business Practice and Information Privacy Practices, (2) Availability, (3) Security and Privacy, and (4) Service Integrity. Again, there are corresponding criteria related to these principles that are the basis for the WebTrust examination. The most current version of the principles and criteria for WebTrust-ISP can be found at http://www.aicpa.org/webtrust/ispfin.htm.

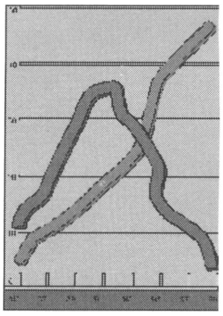
We describe WebTrust principles and criteria in more detail throughout the rest of this book and also include a table summarizing WebTrust principles in the next chapter.

New Client Acceptance

One cannot emphasize enough the importance of choosing your clients carefully and wisely. All too often, we are so excited about having a new client that we forget to take prudent care in determining whether the client is suitable for our practice.

Consider for a moment the importance of client selection in terms of the risk and exposure that a major SEC client poses to an accounting firm. If the practitioner performs financial statement work for this SEC client, he or she must consider who the intended third-party user of the financial reports will be. Stockholders, portfolio managers, banks, and other financial institutions, as well as potential investors, are all possibilities. Now consider the much wider spectrum of the WebTrust engagement. Here, the intended third-party user of the accountant's report will be **anyone** who visits the website and sees the WebTrust seal, whether or not they even read the report. Therefore, in reality, the entire world is a potential user of your WebTrust report! Such exposure is worthy of serious consideration.

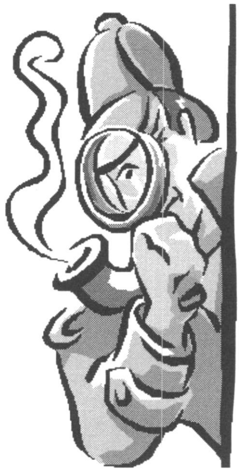
Many firms currently use a form or checklist to help identify factors related to accepting a new client. If your firm has such a document and uses it—bravo! If your firm does not have such a document or if you are looking for other ideas about how to sort through the issues that relate to client selection, we have included an acceptable checklist for your use. See the form "Engagement Acceptance" in Appendix C. Now we examine some of the major factors to consider regarding new client acceptance.



Is Going Concern an Issue for Engagements?

There has been much discussion regarding the need to verify the financial fitness of the business before issuing a WebTrust seal. It is important to understand that a WebTrust engagement is **not** intended to provide any assurance on the financial viability of a company. Rather, WebTrust is intended to provide assurance in specific consumer-oriented areas as outlined by the WebTrust principles regarding a company's electronic commerce disclosures, controls, policies, and procedures.

That being said, it is important for the practitioner to assess the risk in accepting a client that may have difficulty in meeting its current obligations. Also, there is an implied understanding that a customer order will be fulfilled according to the site's disclosed business practices. Therefore, the fact that a client site is able to meet its obligations according to its disclosed business practices, even though there has been a going concern opinion issued, would not preclude the practitioner from issuing a WebTrust seal. However, the practitioner is urged to apply due professional care in accepting the engagement and in monitoring this situation in an on-going WebTrust engagement.



Background Information

This section of the checklist would cover information such as the client name, address, telephone number, in addition to information about the key shareholders, officers, and management. Make sure you include the client's e-mail address and URL for the client website.

How the Client Was Acquired

A good understanding of your referral sources can alleviate a lot of worry about your new client. Was the referral from another client who knows and understands your firm's practices? Or was the referral from another business relationship such as an attorney, banker, or professional association? Your new client checklist is a good place to accumulate this type of information. It's also a good idea to find out why the new potential client is changing affiliations with its current accounting firm. Is there a dispute with the prior accountant that could impair the service you will be performing? Or is there no prior accountant at all—is this a new, start-up company?

Many practitioners may be a little hesitant in accepting a new client without some type of retainer until they have established a comfortable working relationship with the potential client. However, it is important to understand that this traditional approach may result in the loss of some premier clients. Clients involved in eCommerce and the Internet tend to be younger, more entrepreneurial, and eager to try new approaches to business on the net. Your next client could be the next Amazon Book or Dell Computer. How would you feel if you did not accept them as a new client simply because they had no prior accountant? This is not to say that you should exercise no caution with new clients. We are simply trying to get you to look at new client acquisitions in a different light, especially when working on the Internet.

Fees

Accountants can be terrible bill collectors, either because the tradition of our profession allows us to believe that our clients are willing to pay our invoices, or because we are too timid to ask for our fees after rendering our services. Some clients know this and are willing to use you as a bank. Consider this recommendation based on the policy we have for dealing with new clients in our firm. When we meet with a new client, we explain that we have two rules in dealing with our clients:

- We expect to do an outstanding job for our clients
- We expect to be paid in a timely manner for our services

You need to determine what a timely manner is for your firm, communicate it to your client, and then stick to your agreement. In the long run, your client will respect and value the service you render. This is not to say, however, that there will not be exceptions.

Independence

Because WebTrust is an attestation service, independence will be of paramount importance. A lack of independence will preclude you from performing the engagement. As such, it should be addressed in your new client checklist. Rule 101 of the AICPA Code of Professional Conduct (AICPA, *Professional Standards*, vol. 2, ET sec. 101) is the authoritative guide in this area. For those of you who have not reviewed these rules for some time, you may be surprised by your understanding (or lack of understanding) in this area.

Take this short quiz and then consult Rule 101 to see how you did.

1. CPA has been engaged to provide assistance in selecting and installing a computerized accounting package. Eight months later CPA is requested to do an audit for this client. Independent or not? (Hint: Does CPA have decision-making authority?)

   Answer: The CPA may still be independent if the CPA has NOT made management decisions during the installation process.

2. You just got off the telephone with Microsoft who has asked you to conduct their WebTrust engagement. Your partner has one share of Microsoft stock. Independent or not? (Hint: tell your partner to sell or give away his stock)

   Answer: Even with one share of stock, independence has been impaired, albeit the appearance of independence.

3. Your firm has a nominal ($10,000) line of credit with Bank A, which was negotiated at an arm's length and is similar to other lines of credit that Bank A has. Bank A has just requested you perform their WebTrust engagement. Independent or not? (Hint: How important is your $10,000 line of credit?)

   Answer: The firm's independence is impaired.

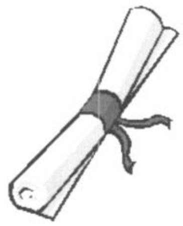
4. Same facts as number 3 except that you have your mortgage rather than a line of credit at Bank A. Independent or not? (Hint: When did you take out your mortgage with Bank A?)

   Answer: The firm's independence MAY be impaired. It depends on when the mortgage was taken out.

It is important that independence be protected and documented. Many of our clients will look to us when setting up eCommerce systems, in the same way that they looked to us to set up their computer systems and networks a few years ago. As we become involved in this process, we need to make sure we differentiate between firm-wide independence and team-wide objectivity. What do the terms, "independence" and "objectivity" mean? Independence is the ability to form an unbiased conclusion about the reliability of an assertion, no matter what that assertion may be. Objectivity is the ability to make a fair, impartial, and detached assessment of work product or process.

With these terms in mind, team objectivity occurs when a **different** group of professionals performs a WebTrust examination than the team that implements the eCommerce system for a particular client. Objectivity is an attribute that can be regained after being compromised much easier than regaining lost independence.

Required Skills for Engagements



The last area we will discuss concerning new client acceptance is whether the firm acquiring the new client has people with the required skills to perform the proposed engagement in a competent professional manner. It is important to look at our firm's resources to ascertain whether we can offer our potential clients the appropriate level of expertise that their jobs require.

Success in the next century will depend greatly on the strategic alliances we are able to form with various partners. These partners will not only serve as a resource to our firms and clients, but will also be a valuable referral source as well. For example, consider the option of becoming a partner with telecommunication, networking, and other technology companies to broaden the resources you are able to offer to your clients.

In a WebTrust engagement, practitioners will need to use skills from the audit and accounting environment, in addition to technology skills. A strong foundation in the traditional accounting professional standards is a must. A practitioner should understand "attestation standards" (AICPA, *Professional Standards*, vol. 1, AT sec. 100), ethics guidelines, as described in "Principles of Professional Conduct" (AICPA, *Professional Standards*, vol. 2, ET secs. 51–57), and quality control guidelines, as described in, "Quality Control" (AICPA, *Professional Standards*, vol. 2, QC secs. 20 & 30) for a WebTrust engagement.

Because WebTrust engagements take advantage of the opportunities of the World Wide Web, technology skills will play a major role in the engagement. As much as 30–60% of a typical engagement may have a technology component. Factor in the rapid change of technology and the accounting professional is faced with a formidable task. So how does an accountant keep up with firewalls, data scopes, cryptography protocols, and other technology-related issues in addition to tax and accounting changes?

If your firm does not have the skills on staff, you need to make a commitment to acquire those technology skills. We suggest three ways to acquire the necessary skills, outlined in order of personal preference:

1. Hire an individual who has the skills you need
2. Contract with an individual who has the skills you need, until the demand for these skills is full-time
3. Train an individual on staff with the skills you need

Although there will be some disagreement with the ordering suggested, it has been our firm's experience that the least effective way to acquire new skills is training from within the firm. Within-firm training is often more costly than the alternatives and can be very time-consuming. Therefore, we recommend that you look outside your firm for specialists. So where do we get qualified specialists?

The first place to look for another specialist is within our profession. Many state societies have created or are in the process of creating a data base of other accounting professionals and their associated skills. This data base is normally available at the state society website. The AICPA also has an Information Technology Membership section that provides additional opportunities to network with other technology professionals. If your state society does not have these resources available to you, ask how you can get involved to make them available.

Other resources to consider in your search for technology professionals are local colleges and universities as well as user groups. All of these organizations should be able to point you in the right direction.

One final word of caution when using an outside specialist—make sure you obtain reasonable assurance of the specialists' qualifications and skills. Review AICPA, *Professional Standards*, vol. 1, AT sec. 100, particularly para. .12–.13, for further guidance in this area.

Practicing Across State Lines or International Boundaries

Electronic commerce provides ample opportunities for the practitioner to practice across state lines. The AICPA is currently working with the National Association of State Boards of Accountancy (NASBA) to work out a uniform licensing agreement with the United States and its territories. This agreement has not been reached; therefore, accountants practicing across state lines should contact the licensing agency for the state in which they desire to practice and obtain the required license.

Because WebTrust is a global service, it is conceivable that an engagement may be obtained outside the country in which the accountant normally practices. If this is the situation, the practitioner should exercise due professional care in contacting the country where the report will be issued and complying with any licensing requirements of that jurisdiction.

Included in Appendix B is a summary of the state-by-state temporary practice rules. This information has been obtained from the AICPA/NASBA *Digest of State Laws and State Board Regulations—1998* (Product No. 064041). Contact AICPA's Member Satisfaction Team at 1-800-777-7077 for ordering information.

If a portion of the engagement takes place in another state—for example, if the server is physically in New York, but the client offices are in California, a New York license would not be required, because the report would be issued for the client in California. This situation would be analogous to an inventory observation where the client offices are in Colorado, but the inventory is stored in New Mexico. The Colorado CPA would not be required to obtain a license from the state of New Mexico. A simple rule to keep in mind—you should be licensed in the state where the accountant's report will be issued.

Third-Party Arbitration

Because of the unique nature of electronic commerce, customers who visit a website are concerned about how their complaints are addressed. If the company with the website is unwilling or unable to address the concerns of a consumer, what recourse does the consumer have? If the consumer is in one country and the business is in another, how will the rights of the consumer be protected?

As you know, traditional dispute resolution through the court system can be both time-consuming and expensive (in addition to frustrating!). Some governments, for example, France, England, and Germany, already require consumer recourse procedures to ensure consumer protection. The consumer recourse provision in WebTrust meets the requirements mandated by the European Union (EU) and other regulatory bodies around the globe.

What Can the NAF Do for Dispute Resolution?

To facilitate dispute resolution matters for both the consumer and the online business, the National Arbitration Forum (NAF) has assisted in the design of a program for eCommerce and, specifically, for WebTrust. The program allows users to file forms and complaints electronically, over the telephone, or through the postal service. Through NAF affiliations around the world, global consumers now have access to low cost expedient arbitration.

Companies that already have a dispute resolution mechanism would continue to use their current resolution process but would apply the consumer recourse rules that relate specifically to WebTrust. A complete version of the Code of Procedure can be found at the NAF website, www.arb-forum.com. The consumer recourse provisions of WebTrust cover not only privacy issues but also address any aspect of the consumer purchase at the website.

Supreme Court Justice Oliver Wendell Holmes said justice is found in "known rules, consistently applied." The NAF believes arbitration must be based on the rules of law, applied consistently. The NAF "Code of Procedures"[2] must also be applied fairly and without prejudice to either of the parties involved in a dispute. To that end, the NAF has developed twelve principles that form the basis of the arbitration process. These principles will be applied to all WebTrust engagements, whether the NAF is retained for the arbitration process or an alternate organization is selected. The principles are as follows:

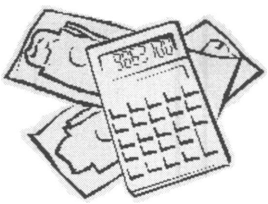
1. FUNDAMENTALLY FAIR PROCESS—All parties in an arbitration process are entitled to fundamental fairness.
2. ACCESS TO INFORMATION—Information about arbitration should be reasonably accessible before the parties commit to an arbitration contract.
3. COMPETENT AND IMPARTIAL ARBITRATORS—The arbitrators should be both skilled and neutral.
4. INDEPENDENT ADMINISTRATION—An arbitration should be administered by someone other than the arbitrator or the parties themselves.
5. CONTRACTS FOR DISPUTE RESOLUTION—An agreement to arbitration is a contract and should conform to the legal principles of contract.
6. REASONABLE COST—The cost of an arbitration should be in proportion to the claim.
7. REASONABLE TIME LIMITS—A dispute should be resolved with reasonable promptness.
8. RIGHT TO REPRESENTATION—All parties have the right to be represented in an arbitration if they wish, for example, by an attorney or other representative.
9. SETTLEMENT & MEDIATION—The preferable process is for the parties themselves to resolve the dispute.
10. HEARINGS—Hearings should be convenient, efficient, and fair for all.
11. REASONABLE DISCOVERY—The parties should have access to the information they need to make a reasonable presentation of their case to the arbitrator.
12. AWARDS AND REMEDIES—The remedies resulting from an arbitration must conform to the law.

[2] National Arbitration Forum, "Code of Procedure" (June 1, 1999).

The WebTrust Engagement — Planning Tools

CHAPTER TWO

The WebTrust Engagement—Planning Tools



In this chapter, we briefly discuss website development and then look at the various tools a practitioner may wish to use in planning a WebTrust engagement. We will discuss the self-assessment document prepared by the AICPA as well as the WebTrust engagement letter. Then, we will describe how to put together a strategy for performing the actual engagement.

WEBSITE DEVELOPMENT

Business websites typically have been developed by a marketing department. The marketing orientation of site developers often results in sites with few accounting controls, because the marketing focus is on the message more than accounting controls. If websites were developed by accounting personnel, there's a good chance that those professionals would want to place too many controls at the website. Too many controls could restrict and even curtail the success of a site. What can organizations do to achieve a better balance of functional views on their websites?

An organization that forms a group made up of the controller (or accounting personnel), members of the marketing department, and the company owner can help create a dynamic website development team. You, as the technology professional, can play an invaluable role for your client, because you offer the balance between the freedom the marketing department needs, and the control the accounting department requires.

SELF-ASSESSMENT DOCUMENT

The self-assessment document was developed by the AICPA Electronic Commerce Task Force to assist both practitioners and their clients in ascertaining WebTrust readiness. You can obtain a copy of the self-assessment document in Appendix B of "WebTrust Principles and Criteria for Business-to-Consumer Electronic Commerce" (AICPA/CICA, 15 October 1999) online at http://www.aicpa.org/webtrust/princrit.htm as well as in Appendix C of this guide.

The self-assessment document is divided into several parts. The first part of the document is intended to provide additional background information to the practitioner. The next sections are devoted to the WebTrust principles mentioned in Chapter One.

The next section of the self-assessment form addresses the issues of site management and providing notification of any changes to the practitioner. These requirements of

WebTrust are a real hurdle for both practitioners and clients due to practitioners' prior business practices, which we discuss in the following paragraph.

Historically, auditors have gone to their clients, including many review and compilation clients, at the end of the client's fiscal year to prepare for the scheduled engagements. At that time, auditors asked their clients to determine whether there have been any changes made to the internal control environment and whether there are any other significant policy changes that are important for auditors to know. Then, auditors would update the permanent files and audit procedures and perform the audit.

Guidelines for WebTrust require that our clients inform us of any change in the manner in which the client complies with the WebTrust Principles and Criteria **before** implementing such change! This revision in approach requires that both the client and the practitioner make a change in their habits. Although the criteria place the burden on the client to inform the practitioner of any changes, it would be a good idea for practitioners to be more pro-active with clients regarding changes made at the website that affect how the site qualifies for the WebTrust seal. As a matter of good practice, this management of change could be beneficial if adapted to other areas of practice.

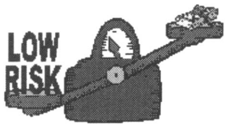
One helpful practice tip is that involving staff with this change process works well. The staff of most firms understands how to use the Internet and sometimes uses the Internet with company hardware—and on non-billable time. Requiring the engagement team staff members to visit a WebTrust site each day looking for any indication of change to the site helps turn surfing the Internet into productive time. Requiring that the staff regularly visit websites keeps the staff alert to possible changes that may affect the manner in which a company achieves the WebTrust Principles and Criteria. However, we are not so naïve as to believe that all changes to the site will be reflected in the specific pages of a website. Therefore, the manager of the engagement should review the site at least monthly and report any findings to the engagement partner.

The final section of the self-assessment documents, called "other matters," includes all other matters not previously discussed. Items in this section may include anticipated change in the organizational structure, soon-to-be-released technology that may impact the business, or specific laws governing the industry in which the client operates. By no means are these items to be considered all-inclusive.

In fact, the entire self-assessment documents should not be considered all-encompassing in its scope. The practitioner should feel free to modify the document to meet the particular needs of the firm and client. As the WebTrust Principles and Criteria continue to go through development and refinement, the self-assessment document will change as well.

Each practitioner should become familiar with the AICPA website and the specific URL for the WebTrust principles, criteria, and the self-assessment document. At the AICPA website, you can obtain an electronic copy of these documents and thereby avoid out-of-date documentation. The address for the WebTrust Principles and Criteria is http://www.aicpa.org/webtrust/princrit.htm. While you are at the AICPA site, look at the information regarding the Yankolovich study on consumer attitudes and trends to eCommerce.

Assessing Risk and Materiality



In any attest engagement, there are three types of risk: (1) **inherent** risk that is beyond the control of both the practitioner and the client; (2) **control** risk that is within the control of management; and (3) **detection** risk that is within the control of the accountant.

Professional standards require the practitioner to reduce the overall engagement risk to an acceptable level. This comment begs for a definition of what is an "acceptable level." Most practitioners would agree that an acceptable level is one that the firm is willing to take on under normal circumstances. Section 37 of AT100 (AICPA, *Professional Standards*, vol. 1) requires "careful exercise of professional judgment."

In a WebTrust engagement, the practitioner should consider gathering evidence from independent sources outside the entity as the highest source of information needed to support the reduction of risk. Next, consideration should be given to evidence obtained by first-hand experience with or knowledge of the client. This may include observations and inspection of the transactions. Last, the practitioner should consider the internal controls of the client, because these controls relate to the client's eCommerce model and website.

It could be argued that if an audit client has no internal controls, an audit is still possible. In this situation, testing of transactions would have to be greatly expanded—possibly to 100%. In a WebTrust engagement if no internal controls exist, a WebTrust seal is NOT possible because WebTrust is all about controls, procedures, and policies.

In addition to consideration of the sources of evidence the practitioner gathers in assessing risk, we should revisit new client acceptance for just a moment. Give careful consideration to this step because it has a direct impact on the overall risk of an engagement. Clients should understand their responsibility in complying with the WebTrust Principles and Criteria.

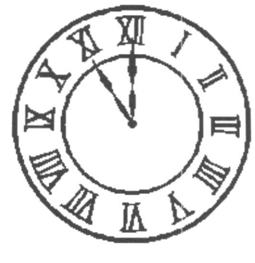
Materiality is a concept that many practitioners in the audit environment have struggled with for some time. In a WebTrust engagement, materiality is more difficult to determine due to the complexity and scope of the Internet. To illustrate this point, take a site that sells books on-line. Assume that the annual sales for this company exceed $5,000,000. Now further assume that this site decides to add a line of rare out-of-print books to its product mix.

To the overall engagement, the rare book line will probably be immaterial to the engagement. However, consider the consumer who buys only rare books and has purchased a book from this site at a cost of $2,000. To the individual consumer, the purchase of a single book is material.

The practitioner should review the guidelines for materiality that are found in AT sections 400 and 500 of AICPA, *Professional Standards*, vol. 1 for additional guidance. As with any engagement, the practitioner should exercise due professional care and judgment at all times.

Another practice note here—the question constantly comes up regarding any prohibitions on sites that are pornographic in nature. The AICPA does not issue any statements or prohibitions in this area. Similarly, the AICPA has not issued any audit guidelines with regard to this type of industry. The practitioner should exercise care and forethought, however, as to whether the practitioner's firm desires to display this association. Remember the accountants' report will be displayed at the client website for the entire world to see.

Periodic Updates



"How much?" and "how often?" are the two questions most often posed regarding the WebTrust program, from both the practitioner and client. Let's address the "how often" part of this question first.

For sites that have little change, a three-month examination period should be sufficient. Change should NOT be equated with changes to the hypertext markup language (html) documents. A mere change in form does not necessarily mean there are changes to the underlying manner in which a client meets the WebTrust Principles and Criteria. A change in an html document is equivalent to a store on Main Street changing its window display.

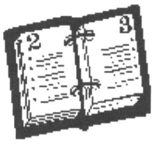
Consider change by evaluating the changes made to a website that has met the criteria for a WebTrust engagement. For example, a new firewall added to the system, moving to another Internet Service Provider (ISP), or adding a new product line are all situations that would require some additional work before issuing a new accountant's report. If these types of changes occur during a three-month cycle, the practitioner will need to consider the effect they have on the engagement and the materiality of such changes. Then, he or she should consider performing an examination before the end of a normal three-month period.

If the change is not material, for example, adding a new product line that uses the same systems and procedures as other products, the practitioner may not need to accelerate the examination of the website.

For sites that are constantly changing, a shortened examination period may be desirable. Because these sites undergo change rapidly, the practitioner's risk may be greater. The practitioner may also wish to have a shortened engagement period for clients that are new to electronic commerce or for sites that are undergoing rapid growth. After obtaining experience with new or changing sites, a three-month period may be appropriate.

Having considered the "how often" part of periodic updates, let's consider the other part of the equation—the "how much." Although no standards have been developed in this area, we have found that a good rule of thumb to follow is to perform some work in each of the criteria. For example, if a specific criteria has several points, the practitioner may choose to test one or more of those points. Certainly, the practitioner should test any criteria that have been affected by a change the client has made.

The practitioner should devise a plan of testing specific criteria so that all criteria will be tested in a calendar year on a rotating or rolling basis. Controls deemed to be material or critical to the overall client system or client business practices should always be tested on every update. For example, in a WebTrust engagement for an on-line bank where encryption is critical, the practitioner should consider testing all of the controls for encryption for each examination period.

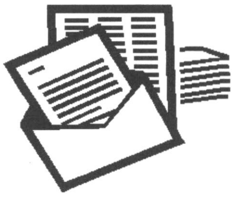


Once again, the practitioner should use professional judgment in determining how much is enough. Factors to consider are risk, materiality, and internal controls the client has in place.

Consider the following suggestion of a schedule of how to monitor a site in between your fieldwork:

- Weekly—staff assigned to the engagement should visit the site and note any changes. Note—a visual change at a website does not necessarily indicate a change in which a company meets the WebTrust Principles and Criteria but can be a good indicator of "behind-the-scene" changes taking place.
- Monthly—a manager or partner in the engagement should contact the site by telephone to ascertain whether the client has made any changes to the site.
- Other—consider the practice of placing an email address, specific to the site, on the accountants' report. By having a separate mailbox for each engagement, it is possible to monitor those sites that may be having problems quickly.

Engagement Letter



The engagement letter is one of the most valuable tools for the practitioner to use. It helps the client understand the services to be performed and the client's responsibilities to the engagement, improves overall engagement management, and is required by the WebTrust license. Take time to put the engagement letter together carefully because of the potential exposure it can cause. See a sample Engagement Letter in Appendix C.

In a WebTrust engagement, the engagement letter is mandated by the WebTrust license agreement and communicates specific requirements to the client. Among these are:

1. Need for hypertext within the WebTrust seal and the independent accountant's report.
2. Duration of the seal—this is not to exceed three months in any circumstance.
3. Requirement of the client to inform the practitioner regarding changes to the website that affect the manner in which the client meets the WebTrust Principles and Criteria.
4. Information regarding use of the WebTrust seal and other related service marks in advertising and other print or electronic media.
5. Acceptance of the subscriber agreement and related expiration date of the certificate of authority. (Currently VeriSign is acting in this role.)
6. Understanding control over the WebTrust seal and corresponding digital certificate.
7. Need for the client's consent to a review of the work papers and other documents for quality control.
8. Need for management to provide a representation letter at the end of the engagement.
9. Need for a third-party arbitration mechanism, for example, the National Arbitration Forum (NAF—refer back to Chapter One for related information) to cover transactions at the website.

A common question addresses the issue of whether the engagement letter should be an annual letter or should be prepared for the initial engagement and then for each subsequent update. Because the digital certificate awarded by the practitioner expires one year after it has been issued, an annual engagement letter covering the initial engagement and all updates would be appropriate. However, no professional guidelines have been issued; therefore, the practitioner should feel free to adapt the engagement letter to his or her practice.

Three points that need to be made regarding engagement letters:

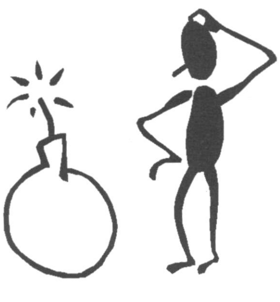
1. Use an engagement letter as a matter of practice.
2. Review engagement letters periodically for needed updates.
3. Explain the engagement letter to the client and the staff.

One final comment—the importance of an engagement letter cannot be overemphasized.

Year 2000 Issues

Hanging over our heads is the year 2000, or Y2K, problem. Experts are at odds about placing a dollar amount on this problem; the SEC is requiring little disclosure related to year 2000 matters, and attorneys are gearing up for full employment.

Because of the nature of the year 2000 issue, a WebTrust engagement is not intended to reveal problems in this area, nor is the engagement expected to give any assurance regarding the Y2K readiness of a company.



Many individuals have said that the Y2K issue would not be a challenge for a WebTrust engagement until the quarter before and after the year 2000. However, the practitioner should consider Y2K effects of some product and sales cycles that may go beyond a quarter or year; e.g., sale of annuities and purchase of mortgages.

Practitioners should add the following wording to both the engagement letter and the accountant's report regarding the Y2K issue. Any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time [such as to accommodate dates in the year 2000] may alter the validity of such conclusions.

Sample Accountant's Report

The accountant's report would then read as follows:

To The Management of ABC Company, Inc.:

We have examined the assertion [hot link to management's assertion] by the management of ABC Company, Inc. (ABC) regarding the disclosure of its electronic commerce business and information privacy practices on its website and the effectiveness of its controls over transaction integrity and information protection for electronic commerce (at WWW.ABC.COM) during the period August 1, 2000 through October 31, 2000.

These electronic commerce disclosures and controls are the responsibility of the management of ABC Company. Our responsibility is to express an opinion on management's assertions with regard to the AICPA/CICA *WebTrust* Criteria [hot link] based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included: (1) obtaining an understanding of ABC Company's electronic commerce business practices, its controls over the processing of electronic commerce transactions, and the protection of related private customer information; (2) selectively testing transactions executed in accordance with disclosed business practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time, such as to accommodate dates in the year 2000, may alter the validity of such conclusions.

In our opinion, during the period August 1, 2000 through October 31, 2000, ABC Company, in all material respects:

- disclosed its business and information privacy practices for electronic commerce transactions and executed transactions in accordance with its disclosed business practices;
- maintained effective controls to provide reasonable assurance that customers' orders placed using electronic commerce were completed and billed as agreed; and
- maintained effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce was protected from uses not related to ABC's business based on the AICPA/CICA *WebTrust* Criteria.

The CPA *WebTrust* seal of assurance on ABC's website for electronic commerce constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

This report does not include any representation as to the quality of ABC's goods or services nor their suitability for any customer's intended purpose.

X, Y & Z (name of CPA firm)
Certified Public Accountants
City, State
November 4, 2000 (date of report)

Going Concern Issues Revisited

We discussed the *Going Concern* issue in Chapter One and need to reconsider this topic as we plan the initial WebTrust engagement and subsequent updates to the seal.

The question of the financial stability of a company often comes into question before and during a WebTrust engagement. It is important for practitioners to understand that the WebTrust service does not address the going concern opinion, which is a financial condition.

The criteria for *Transaction Integrity* (introduced in Chapter One) state that the company "maintains effective controls to provide reasonable assurance that customers' orders placed using electronic commerce are completed and billed as agreed." A strict interpretation of this principle should lead the practitioner to question the financial ability of an organization to purchase the goods that customers are ordering.

Should a company in Chapter 11 bankruptcy be denied the opportunity to earn the WebTrust seal? Our first reaction may be to say yes. How can a business in bankruptcy (and with a going concern opinion) be eligible for the WebTrust seal? Although no definitive answer can be provided, note that Macy's Department Stores were in Chapter 11 for several months and still were able to carry on business. In any event, the practitioner should give special consideration to the financial stability of a company and assess the risk this adds to the engagement.

Engagement Forms, Procedures, and Considerations

The next section of this document covers examples of workpapers and the associated procedures the accountant would perform in a routine WebTrust engagement. Information presented here is not intended to be all-inclusive or authoritative. The recommendations presented here are for the practitioner's guidance; therefore, due professional care is recommended in applying this information to a specific engagement.

Self-Assessment Document Revisited

Because of the importance of the self-assessment document discussed in Chapter One, we revisit this topic here. (The document is included in Appendix C of this guide.) We include information about how you might consider using this document based on our experience.

Consider proceeding as follows when interacting with your client about the self-assessment document. Provide the self-assessment document to the client and ask him/her to complete as much of the document as possible. Explain that some of the information will not be relevant, and other information may not be known. It might be a good idea to stress that the process of completing the document is important for the client's own assessment as to readiness for the WebTrust seal. Also mention that the document should be filled out as completely as possible and not to worry if there are some areas left blank. You might consider encouraging the client to involve other individuals from their company in completing this assignment and, perhaps, recommend the sales/marketing manager (many times this is the company president), the controller or accounting manager, and the webmaster. Each of these individuals has a unique perspective concerning the company's website.

At the end of one week, meet again and review the document. Prepare for the meeting by visiting the client's website and copying pages that have any type of disclosure relating to the WebTrust Principles and Criteria. At the meeting, discuss the client's readiness for the engagement and also make some specific recommendations to the client regarding any weaknesses noted based on information in the document.

In one specific engagement situation, it was our experience that the client requested a two-week extension on preparing the document. When we met three weeks later, this client had redesigned its website to meet (and, in some cases, exceed) the requirements set forth in the WebTrust Principles and Criteria. In another engagement, the client realized that the ISP they were using provided no security for their transactions. The lack of security prompted the client to change to another ISP that provided the protection the client wanted.

When the self-assessment document is complete, the practitioner would have a basis for putting together a work program. Without the self-assessment document, both the practitioner and the client lack important information.

Analytical Procedures

Analytical procedures involve comparing actual results with industry statistics or anticipated results. Because the area of eCommerce is relatively new, the accountant may find it impossible to find any meaningful industry numbers for analytical comparison. In this case, the practitioner will need to rely on experience with the client to interpret the results.

Because a WebTrust engagement is not an examination of the financial statements of a company, traditional ratio analysis will be of little benefit. However, trend analysis and reasonableness tests should provide some help in ascertaining information regarding the electronic activities of a client.

Trend analysis compares the actual dollar amounts or percentage change in specific accounts over time. For example, the practitioner may wish to analyze the change in warranty service for goods purchased electronically over a period of time. Then, the practitioner could compare the results to the warranty service account for goods purchased in a traditional manner. Major fluctuations would require additional inquiry from the accountant.

Reasonableness tests can involve ratios or estimating account balances. For example, certain expenses are estimated with ratios:

- Commission expense ÷ electronic commerce sales
- Shipping expense ÷ electronic commerce sales

- Estimating electronic commerce sales based on the number of sales on the Internet
- Estimating warranty expense based on total sales × Internet sales

The purpose of reasonableness tests is to provide a means for the practitioner to determine where more inquiry or analysis may be required. Experience with the client and the industry will assist the practitioner in drawing meaningful conclusions from the results. Keep in mind the following factors when evaluating the results of any analytical test:

- Expected fluctuation. Some fluctuation should be expected and may be affected by outside and predictable influences.
- Materiality. Any fluctuation should be analyzed from the standpoint of overall materiality to the engagement.
- Experience with electronic commerce. If the client has little history with electronic commerce, or is in a strong growth period, analytical procedures may not be beneficial.

WebTrust Principles Summary

Because there have been two additional principles introduced as a result of the recent issuance of WebTrust ISP and Version 2.0 of the principles and criteria, the following grid shows which principles the accountant should use for the engagement being performed.

Principle	WebTrust for Business-to-Consumer eCommerce	WebTrust–ISP
Business and Information Privacy Practices Disclosure	✓	✓
Transaction Integrity	✓	
Information Protection/ Security and Privacy	✓	✓
Availability		✓
Service Integrity		✓

Business and Information Privacy Practices Disclosures

eCommerce often involves transactions between strangers. Appearances can be deceiving. How can a consumer know whether an entity that presents a well-constructed Web page will really fill its orders for goods and services as it claims? How can a consumer know whether the entity will allow the return of goods, or whether there are product warranties?

The anonymity of eCommerce and the ease with which the unscrupulous can establish—and abandon—electronic identities make it crucial that people know that those entities with which they are doing business disclose and follow certain business practices. Without such useful information and the assurance that the entity has a history of following such practices, consumers could face an increased risk of loss, fraud, inconvenience, or unmet expectations.

Information privacy can be a two-edged sword. One the one hand, merchants need certain information to process a customer order. On the other hand, the customer does not want this information provided to others without their permission. In addition, errors can occur in a company database that the consumer should be able to correct or amend as needed. Without a process for error correction in place, decisions can be made that could negatively impact the consumer.

Global Impact of Privacy Criteria

eCommerce by its nature is global. As companies cross international boundaries, they are faced with the challenges of meeting standards and complying with laws regarding privacy. Merchants who wish to tap into the global market place may find that, without adequate privacy standards at their site, they may be prohibited or restricted in the manner in which they are able to do business.

Consumers from other areas in the world are also concerned about how their information will be used, how it is protected, what process is in place that will allow them to correct erroneous information, and who will have access to this information. Without proper criteria, procedures, and controls in place and without properly related disclosure, these consumers may choose to do business at another site where there are adequate controls.

Countries around the globe are setting policies in place to assure their citizens that their information is kept private. The European Union (EU) directives for the European community took the lead in this area with the Online Privacy Alliance (OPA) with the United States close behind. WebTrust meets or exceeds all critical requirements regarding privacy and consumer recourse as imposed by these two organizations and will continue to monitor changes in this area to make sure WebTrust remains compliant.

The disclosure criteria are, perhaps, one of the easiest for the practitioner to document—either the disclosure is present or it is not. It is important to remember that a site must have been compliant to this (and all) principles to receive the seal. One may ask—how will I know whether a specific disclosure has been at a website for two or more months?

Simply put, you won't know how long a particular disclosure has been on a website if you do not have first-hand knowledge as to when the disclosure was made. This knowledge may come from information gathered at the time the practitioner met with the client during the self-assessment stage, from work history with the client, or by some other means. In reality, there will instances where the practitioner does not have or cannot obtain independent information regarding the dates certain disclosures were placed on the website and made public. For this reason, the practitioner may wish to include the following wording in the management representation letter:

> "We represent that the business practices disclosures for <www.abc.com> are current, accurate, and complete and have been on our website since July 1, 200X."

The practitioner should also obtain supporting documentation from the client in the form of company policy manuals, shipping policies, sales policies, and other company related information.

Transaction Integrity

The principle of *Transaction Integrity* is the principle that most accountants are accustomed to and, therefore, comfortable with. The intent of this principle is to provide assurance that orders placed through electronic commerce will be fulfilled with the correct merchandise, information or service, and in the correct quantity. The principle also is intended to provide a means by which customers may follow up on historic information regarding their order(s).

One of the weaknesses we have encountered is that of compatibility of electronic commerce systems with current accounting systems. Many pioneers in eCommerce have "patched" together a system that allows them to transact business on the Internet. These patched systems are, for the most part, manual in nature and, therefore, require the practitioner's special attention. As with most manual systems, the chance for human error increases dramatically as the information from the eCommerce site is re-entered into the client's order entry and accounting system.

This situation provides an excellent opportunity for consulting with the client and automating this process. One word of caution, however, the concepts of independence and objectivity may be compromised without due professional care.

From a "30,000-foot" vantage point, we can look at both the disclosure principle and the transaction integrity principle and see that these two principles encompass much of what the accounting profession calls an audit. With this in mind, we can see that WebTrust has provided a new attest service by using many of the tools that the practitioner is already using. The new skill set required for a WebTrust engagement comes into play with the *Information Protection* principle.

Availability Principle

The *availability* principle characterizes WebTrust–ISP. Because a customer's own electronic commerce business can be totally reliant on the ISP providing its service and ensuring that the service is available, it is critical that a customer's access to the Internet is available as advertised and promised by the ISP in its service-level agreement. If the ISP's service is unavailable for a significant period of time, each of the ISP's customers may suffer temporary loss of revenue, impaired cash flow, and/or diminished public image.

In this regard, policies concerning matters such as customer notification of planned outages (for system updates), repair time notification and alternative arrangements, if any, for emergency outages also should be disclosed. This principle applies only to WebTrust–ISP engagements and is not a consideration for WebTrust for Business-to-Consumer eCommerce engagements.

Service Integrity Principle

It is important that the ISP maintains effective controls over the electronic processing of its customers' information. Like the availability principle, *Service Integrity* is a principle that is a characteristic of WebTrust–ISP.

The customer's information may take the form of, for example, an e-mail message, an electronic commerce purchase order, a credit card authorization or, simply, a file transfer protocol (FTP) request. In the business and information privacy practices disclosure principle, the ISP discloses its significant business practices related to its ISP services. The service integrity principle addresses the controls that the ISP has in place to effectively meet its disclosed business practices. If the ISP's service integrity is poor for a significant period of time, each ISP customer may suffer temporary loss of revenue, impaired cash flow and/or diminished public image. As a result, it is important that controls are maintained to provide reasonable assurance that incoming messages are processed and delivered accurately and completely to the correct IP address and that outgoing messages are processed and delivered accurately and completely to the ISP's Internet access point. It is also important that controls exist to provide reasonable assurance that the ISP's services perform at the bandwidth and throughput levels advertised for each generally available class of service. Finally, it is also important that transaction histories are retained in a secure location, may not be altered without appropriate authorization, and are retrievable for review/investigation. In this way, the customer has available evidence that they are receiving the quality of service that they have contracted for.

Information Protection/Security and Privacy

Before beginning the discussion on *Information Protection/Security and Privacy,* let's review the definition of private customer information applied to WebTrust.

> Private customer information includes individually identifiable information about the customer. Such information includes, but is not limited to, his or her family (name, address, telephone number, social security or other government identification numbers, employer, credit card numbers, etc.), personal or family financial information, personal or family medical information, employment history, history of purchases or other transactions, credit records, and similar information

Because customers provide private information to the website or ISP, it is important that this information is protected from uses not related to the entity's business. It is important for customers to have confidence that they are using a secure site and that the business represented at the site is taking appropriate steps to protect private customer information. Although it is relatively easy to establish an Internet-based business, the underlying technology can be complex and can entail a multitude of information protection and security issues. The confidentiality of sensitive information transmitted over the Internet, or retained by an ISP or website, can be compromised. For example, without the use of basic encryption techniques, which we discuss later in this book, consumer credit card numbers can be intercepted and stolen during transmission. Without appropriate firewalls and other security practices, which we also describe later in this book, private customer information residing in an on-line computer system can be intentionally or unintentionally provided to third parties not related to the customer's business. Security breaches also may include unauthorized access to corporate networks, including related operating systems, Internet/Web servers, and even access to the consumer's Internet connection (for example, a connection from his or her home computer). Potential participants in electronic commerce may seek assurance that there are effective information protection controls and a history of protecting private customer information.

In an AICPA study (the WebTrust study conducted by Yankelovich in August 1997), more than 60% of the individuals surveyed listed security and privacy as their number one concern about doing business on-line. The European community also lists their number one concern as privacy and security. Similar reactions in both geographic areas reinforce the idea that privacy and security are paramount concerns for those who engage in on-line business.

The *Information Protection/Security and Privacy* principle offers the criteria that require some technological expertise on the part of the practitioner. The required level of expertise may be found within the consulting division of the firm and, therefore, would provide an opportunity for the accounting and the consulting departments to work together on an engagement. If the expertise is not found within the firm, the practitioner will need to look outside to perform the engagement in a professional manner. Consider the merits of looking at a strategic alliance with another CPA firm or other professional who can provide the technological expertise service required (see the section, "Required Skills for Engagements" in Chapter One of this book for additional guidance).

For the practitioner to better understand the potential risks involved regarding information protection issues, we present the following information from a recent FBI survey about computer crime.

FBI Computer Crime Survey

The 1999 FBI Computer Crime Survey details the practices of 521 companies from various industries and of various sizes regarding securing their computer systems. The results highlight why security is a top concern for all kinds of businesses and what security-related issues every business needs to pay attention to.

In summary, the survey results show that:

- 61 percent of the organizations surveyed have experienced losses due to unauthorized computer use.
- 32 percent of the organizations surveyed are now using digital IDs.

- The average loss from theft of proprietary information is over $1.2M.
- The average loss from data or network sabotage is over $1.1M.
- 50 percent of all organizations reported insider abuse of net access.
- 94 percent of organizations now have Web sites.

Here's a closer look at some of the survey questions and results:

What types of security technology do you use?

- Access control, 89%
- Encrypted files, 59%
- Reusable passwords, 59%
- Firewalls, 88%
- Encrypted log-in sessions, 44%
- PCMCIA smart-cards, 37%
- Intrusion detection, 40%
- Digital IDs, certificates, 32%

What is the most likely source of an attack?

- Independent hacker, 74%
- U.S. competitor, 53%
- Disgruntled employee, 86%

Which of the following types of electronic attack or misuse has caused your organization financial loss?

- Theft of proprietary information, 12%
- Sabotage of data or networks, 9%
- System penetration by an outsider, 10%
- Insider abuse of net access, 35%
- Unauthorized access to info by insider, 16%

Has your Web site been accessed without authorization or misused within the last 12 months?

- Yes, 18%
- No, 44%
- Don't know, 38%

Internet Security Problems and Remedies

CHAPTER THREE

Internet Security Problems and Remedies

What Internet Security Problems Pose Challenges?

The threat to computer resources is reaching new heights. Victims range from Fortune 500 companies to home offices, from government laboratories to classroom workstations, and from transportation systems to retail stores. This escalation in computer resource threats is a result of, in large part, the mad rush to wire into the Internet regardless of risk. As the popularity of the Internet as both a place of business and recreation source increases, the threat to computer systems by crackers appears to be climbing.

The threat to the world's computer systems comes from two sources: (1) increasingly sophisticated crackers and (2) systems administrators who are under-equipped to confront today's security hazards.

The best way to confront system threats is to understand the types of crackers and how systems administrators can better educate and prepare themselves to deal with system violations. Internet attacks range from simple probing to extremely sophisticated forms of information theft.

Exploiting weak passwords, piggy backing off other programs, sometimes called *Trojan Horses*, routing attacks, exploiting the use of dangerous Unix functions such as *finger, sendmail, NFS, NIS*, today's crackers possess a truly diversified arsenal of tools.

(NOTE: Refer to Appendix A, "Internet Dictionary," for terms used in this and other sections of the guide. Also see definitions on pages 36 and 37.)

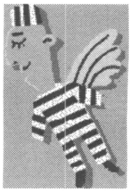
- In February 1995, the worldwide media widely reported the arrest of one of the world's most notorious computer criminals, Kevin Mitnick. Mr. Mitnick is typical of today's sophisticated crackers. He is highly educated, motivated, and possesses intimate knowledge of computer networks and their security systems. Using a laptop computer equipped with a radio modem, Mitnick managed to tap into several long distance phone companies' call-routing systems and, from there, to crack into numerous computer systems across the world. He had the ability to play upon the weaknesses of packet filtering software that brought Mitnick his best results. Though Mitnick's motivation for his activities has yet to be explained, the incentives for other attacks seem much clearer, for example, for financial gain, for prestige, or for the thrill of doing it.
- Some of the most famous attacks were those highlighted in Clifford Stoll's "The Cuckoo's Egg." In this account, Stoll details how a group of East German intelligence agents systematically attacked U.S. government and scientific computer networks via an astronomical laboratory. Stoll uncovered the plot thanks to a 38-cent discrepancy in a telephone bill. Espionage, both political and corporate, is the primary reason for at-

tacks on computer networks. The former director of the FBI Computer Crime group recorded a 400 percent rise in cases of corporate espionage from 1992 to 1993 alone. Since then, the same type of growth has continued to occur throughout the remainder of the decade.

- In 1992, U.S. and European crackers broke into Pentagon computers by "fooling the system into thinking they were Dan Quayle." Files on domestic anti-terrorist activities were targeted. In a celebrated case of corporate warfare, Virgin Atlantic Airlines successfully sued British Airways when it was discovered that BA cracked Virgin's reservation system in an attempt to steal passengers. British Airways was ordered to pay $4 million in damages and legal costs. In 1994, the *CERT* Advisory "Ongoing Network Monitoring Attacks" reported that crackers using a *Trojan Horse* program captured access information for tens of thousands of system. All systems offering remote access via *rlogin, telnet,* and *FTP* were at risk.
- In the fall of 1994, a 16-year-old British boy using cracked accounts on U.S. military computers in Rome transferred hundreds of classified documents from the South Korean Nuclear computer system.
- Compounding the problem, the casual cracker has re-emerged as a dangerous threat to networks security. The casual cracker, often stereotyped as the bored college student joyriding through various sites on the information highway, gained new tools in 1994. The most perilous of these was the suite of tools packaged as *SATAN.* SATAN uses a graphical interface to assist even the most novice crackers in organizing a series of attacks against a given host, with the results displayed in an easily understandable format. Because it searches for all known security holes in a matter of minutes, SATAN can help a cracker find an accessible system in a fraction of the time it would otherwise have taken. SATAN exploits known problems with *NFS, NIX, rexd access, sendmail, TFTP* file access, unrestricted *x-server* access, and *wu-ftp* vulnerability.

Methods of Attack

This section discusses several methods of attack to illustrate the nature of the Internet security problem. This is not intended to be a complete list of the methods. Systems have been breached with simple techniques that take advantage of security loopholes in common system utilities. Other approaches are considerably more sophisticated and require a significant amount of programming.



Trojan Horse

A Trojan Horse is a program that a cracker inserts into a system to replace an existing function with a hidden additional function. Trojan Horses can be extremely difficult to detect because they can have the same name, file size, and last changed date as the mimicked function. Often, by the time a Trojan Horse is discovered, significant damage has occurred.

Trojan Horses have been used to capture User IDs and passwords exposing large numbers of systems, even though only one system was originally compromised. When users login to other systems across the Internet, their User IDs and passwords travel in the open. Intruders exploit this loophole using a Trojan Horse that collects legitimate User

IDs and passwords traveling on the net. The intruder can then use the legitimate User IDs and passwords to gain unauthorized access to other systems. The breached system accepts the intruder as legitimate. Once the intruder has gained access to the first system on a private network, the remaining systems on the network are easy prey.

CGI Exploitation and Web Vandalism

Since March 1996 there have been increasing numbers of attacks on web servers by exploiting the system's cgi-bin scripts. The most common attack uses the "PHF" program installed by default on several commercially available http servers. Crackers use the PHF to obtain copies of the /etc/passwd file, add and delete files, modify existing files, and open terminal windows. Using this security hole, crackers managed to attack the FBI and CIA websites in 1996 replacing pages with modified text and obscene photos. Intruders often rename the PHF program so that its use will go undetected and to ensure that administrators cannot delete the program.

It is possible to use weaknesses in the cgi-bin scripts as opposed to the PHF program to delete the web server operating system, send fake e-mail, and attain root privileges.

Malicious Java and ActiveX

Despite assurances from SUN and Microsoft about the security of these programming and scripting languages, Java and ActiveX are inherently insecure and dangerous for today's web browsing community. Holes in the Java class loaders and the bytecode verifier can be exploited so that malicious applets can execute arbitrary machine code. In February 1996, Princeton researchers demonstrated how using Java applets that exploited DNS weaknesses could force browsers to unwittingly make network connections.

Some web browsers offer user restrictions on Java allowing Java applets and Java Script to be deactivated and not read. It is possible using Java and ActiveX Scripts to insert malicious code that will skirt these controls and run all scripts regardless of the user's desire or without his knowledge.

Hostile or malicious applets are proliferating on the Internet at an alarming pace. There are several sites that distribute source code for malicious applets that can read, alter and delete files, or disrupt the normal operation of the browsing machine. Recorded hostile applets can:

- lock the browser
- lock the browsing machine's keyboard
- make the browser begin barking and then exit
- open a window asking for a user name and password and then return the information to the offending machine
- kill other applets, running programs, and defend against an attempt to use other programs such as ThreadDeath to shut the hostile applet down
- forge and send e-mail

- create a myriad of windows, calculations, noise, run other programs, and report back the results
- disseminate not only Windows-based, but also UNIX-based viruses at an alarming rate

Applets run with the full permission level as the browsing user, so that if a user browses with full root access, any applet it encounters will have the same access permissions.

It is possible to filter applet classes using packet filtering, but weaknesses in the Java Remote Method Invocation class loader and security manager make it possible to dynamically load hostile classes or reclassified hostile classes.

Java and ActiveX scripts are even more dangerous than applets. Scripts are harder to separate from the html transmission than applets and can run before a browser can refuse the script. Like applets, scripts run with the full access of the browsing user. ActiveX scripts can run any application on the browsing machine and make calls to the operating systems. In February 1997, German television reported of an ActiveX control that opened Quicken, the personal finance program, and attempted to transfer funds, add transactions, and modify the application's reports.

Web Spoofing and Hi-Jacking

In the Web Spoofing and Hi-Jacking attack, crackers set up a malicious web server on the Internet between unsuspecting users and the rest of the Web. The spoofing server then hi-jacks all http connections initiated by the browser and forces access to all other sites to pass through. The cracker can then sniff and tamper with all transactions, including previously considered "secured commercial" transactions via the Secure Sockets Layer, pick up account and password information, and permit and deny access to Web resources. In some cases, the spoofing server has inserted offensive material to antagonize the surfer.

Lax Password Security

If a cracker can gain access to the password file on a UNIX or Windows machine, then he or she can apply a fast decryption algorithm to a list of common passwords and permutations on account and user names. Using fast workstations, it takes little time to break into the first account. On a medium to large network, there is bound to be at least one machine for which a cracker can obtain the password file using an unprotected UUCP link, an unplugged loophole in sendmail, or ftp. Because most users select relatively simple and easy-to-guess passwords, the method of table lookup works very well.

In a study conducted by Daniel Klein using password file entries from a database of 15,000 accounts, the following level of success was reported. Using a DECstation 3100, he was able to crack 368 passwords in only fifteen minutes and 3,000 passwords in the first week. Today, crackers have access to faster machines. Using the "Crack" program, they can compromise a system containing 50 accounts in less than a minute. A determined cracker with access to a cluster of parallel workstations using the "Crack" program can achieve access to multiple accounts in a matter of minutes.

Obtaining System Information

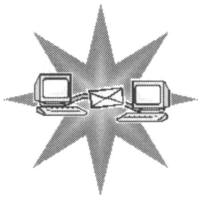
There are several UNIX tools an intruder can use to obtain information about your system. With detailed information about users and network configuration, a cracker can better focus his or her attacks. Some of the most dangerous ones include the following:

- The finger command is extremely dangerous in the hands of an intruder because they can learn account names, when the account was last used, the account's home directory name, and from what host they logged in. This information is very useful for launching an attack on your system.
- The showmount command displays a list of all clients that have remotely mounted a file system.
- The rpcinfo-p command probes the portmapper on a system and prints a list of all registered Remote Procedure Call (RPC) programs. Many system services such as the Network Information System (NIS) developed by Sun Microsystems and licensed to many different UNIX vendors use RPCs. If the system runs NIS and the intruder determines the NIS domain name, the intruder can get the domain maps by issuing the appropriate RPC call.

X-Window

X-Window, if improperly configured, allows an intruder to transparently watch the user's display and capture mouse and keyboard input. When the user logs in to another system, the intruder can see the login ID and password used for that system. If the user does a su to root, then the intruder will know how to access root on that system. A sophisticated intruder can remain undetected while changing the user's input before passing it on to the program. The first hint of tampering could be the discovery of a catastrophic problem.

Sendmail



Sendmail is a commonly used complex mail program that offers endless flexibility. Unfortunately, crackers exploit this flexibility to obtain unauthorized access to system data. Using sendmail, crackers have mailed the /etc/passwd file to their system. Some sendmail bugs have only recently been fixed. Many systems continue to use older versions of sendmail.

Denial of Service Attacks

To reliably establish or terminate a connection, three messages are exchanged:

(1) synchronization (SYN) segment—messages used to create a connection; (2) finish (FIN) segment—messages used to close a connection; and (3) retransmit segment—messages used to retransmit a connection. These three messages make up what is called, in practice, the three-way handshake.

In September 1996, a wave of denial of service attacks using SYN Flooding and extremely large Pings ("Ping o' Death") effectively shut down major Internet providers in the Northeast. Source code to tools that exploited weaknesses in the three-way handshake spread across the Cracker journals and the Internet. The SYN Flood attack sends a high volume of SYN packets to a target host and never responds with the rest of the handshake information, thus filling the targets data structures. This prevents legitimate processes from starting, paralyzing the target machine. Both known machines behind packet filtering routers and firewalls themselves are targeted, which disrupts individual and network service.

The Ping o' Death takes advantage of IP's ability to fragment packets. Extremely large Pings are broken into smaller processable packets that are then sent to the target. The targeted machine receives and attempts to reassemble the huge packet overflowing the 16-bit internal variables causing the system to crash.

The major UNIX vendors have distributed patches to attempt to quell these attacks, each meeting with a reasonable margin of success. There are no NT solutions to these attacks at this date.

Packet-Filtering Weaknesses

Major American corporations, U.S. government agencies, their contractors, and others discovered that sophisticated crackers easily defeat packet-filtering routers. Although routers provide useful functions and a modest level of security, many companies augment routers with firewall systems that sit between the public unsecured and the private secure networks.

Advanced routers provide packet-filtering capabilities. Packet filters drop, reject, or permit packets based on destination IP address, source IP address, and application port numbers. Packet filters allow communications specifically with applications on other "trusted" systems.

Filters base decisions on the contents of the current packet only, with no general context maintained in relationship to other packets. Crackers exploit this situation to leak information past the router (see #7 below for more related information).

Packet filtering is insecure for the following reasons:

1. Packet filtering is a dangerous and error-prone process. To do it right, one needs intimate knowledge of transmission control protocol (TCP) and user datagram protocol (UDP) port utilization on a number of different operating systems. When a site has more than a dozen non-contiguous Class C networks in internal use, routers are often configured with several hundred filters per port. As Steve Wilkens of Simitar Systems indicates, "This is one of the reasons we do not like packet filters very much: if you get these tables wrong you may inadvertently let in the Bad guys."
2. IP addresses make up the basis for packet filtering. Thus, you have to trust everyone on the system. If the trusted host is cracked, the cracker can get through your packet filter.
3. Routers that do not provide for strong user authentication should never allow users into protected systems. During the past year, Trojan Horses that sniffed user IDs and passwords on the Internet compromised more than 100,000 user IDs and static passwords.

4. Routers are subject to various attacks that divert packets through crackers' machines. A routing attack program can use the Routing Information Protocol (RIP) to send bogus routing information to a host. Such actions allow the attacker to create a "new" route for the entire network, enabling the intruder to receive all the packets destined for that network.
5. Crackers can mimic the IP addresses of trusted machines, bypassing packet filters and gaining access to systems. The software on this malicious machine-in-the-middle can pass the legitimate traffic through, thus going undetected. Kevin Mitnick blindly sent command packets bearing trusted internal IP address into networks until the router allowed him access.
6. Some routers do not provide logs of systems, user activity, or records of successful and unsuccessful attempts to use the system. Logging is a fundamental component of Level C2 security and above.
7. Packet filters can leak sensitive information in IP packet fragments. Except for the first packet fragment, other fragments do not contain port numbers, so there is little information to base a filtering decision. Nothing prevents someone from building bogus non-initial fragments and converting them back to packets on some other machine.
8. Routers do not hide internal network structure. Thus, a cracker can easily obtain host names and IP addresses to mount attacks.
9. Three major services are not handled well by packet filters: FTP, DNS, and X11. Normal operation of FTP and X11 both require the use of incoming calls. Even though the FTP client may reside on an internal host, it will require the external FTP server to open an in-bound port for file transfer. Some services use a range of port numbers, thus requiring a range of ports to be allowed access by a packet filter.
10. The complexity of router tables and rules requires large chunks of an administrators' time to monitor and maintain.

Other Problem Areas

- If the system allows read/write access to Network File System (NFS) mounted directories, then it is possible for an intruder to add a .rhosts entry in a guest user home directory. This will allow the intruder to perform a rlogin without having to supply a password.
- If the system is running anonymous ftp, it is possible for an intruder to get in since ftp is often misconfigured. If the ~ftp/etc/passwd file is a complete copy of the /etc/passwd file, then an intruder can retrieve the password file, which can then be cracked using a previously discussed method. If the ftp home directory is writable, then it is possible to add a forward file, allowing the intruder to mail the /etc/passwd file back to his/her machine. This is another example of a single program that provides multiple opportunities for the wily cracker.
- If a system runs the trivial file transfer program (tftp) and is accessible from the Internet, then watch out. The tftp does not require any user password and, if improperly configured, will allow anyone to read or write any data on the system.
- Some older systems may not have the patches for the ftp bug that allowed a remote user to obtain root privileges.

- If the system runs Network Information System (NIS), then it is inherently insecure. NIS uses client server technology to share a single copy of the password file over the private network. NIS is insecure because there is no authentication between client and server. NIS also presents serious security exposures if the /etc/passwd file on the NIS server system is incorrectly configured, thus allowing anyone to login to the NIS server using a plus sign "+" at the login prompt. Improper configuration of the /etc/passwd file on a client NIS system can allow anyone to login as root on the client if the NIS server is down.
- The list of potential security problems and defenses has been the subject of numerous books.
- Bill Cheswick (the self-described "hacker in residence" of Bell Labs) published a research report on attempted break-ins at AT&T Laboratories. The most important lesson learned in the study was "if a hacker obtains a login on a machine, there is a good chance he can become root sooner or later: There are many buggy programs running at high privilege levels that offer opportunities for a cracker. If he gets a login on your computer; you are in trouble."
- Fortunately, the technology exists to not only plug the known security loopholes, but also to strengthen a site's security and to defeat the intruders.

Security and Privacy Components

Security and privacy at any website may include several or all of the following components:

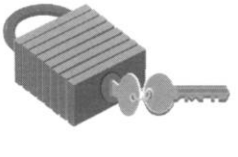
- Physical access restrictions
- Data backup
- Firewalls and routers
- Encryption
- Virus-scanning software
- Passwords

It is not the intent of this work to provide a detailed explanation of the preceding concepts; however, we will attempt to give some introductory material. We have also provided some our favorite websites in Appendix D of this book, where you can find additional information.

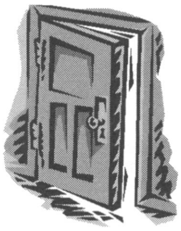
Physical Access and Backups

Often overlooked as a real source of concern, physical access, or the lack there of, can provide real dangers to information systems. Common sense in this area is often the best guide. Is there limited access to the room in which the file server, commerce server, and backup drives are located? Are video surveillance cameras necessary?

The lesson of access to critical hardware was learned the hard way by one of my clients several years ago. Early on a Monday morning, the controller told me that the server was gone and that, as a result, no one was able to work. Upon arriving at the client site, imagine my surprise when I learned that the file server was not down as I had thought but, indeed, it was physically "gone." Apparently, over the weekend, someone had broken into the office and stolen the file server that was on a desktop in the copy room.



The client's physical setup allowed free access for anyone who entered the building to the copy room. The only asset missing was the file server—no other equipment was taken. With this in mind, don't overlook the need to limit access to hardware as an easy step in site security.

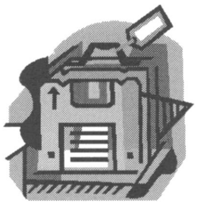


No one can really place the value on a good backup until it is needed. Backups should be stored in a protected environment off-site, and the entire system—including operating system and program files—should be included in the backup. (See next section.)

Physical access includes everything that happens before you start typing commands on the keyboard. It's the alarm system that calls the police department. It's the key lock on the computer's power supply that makes it harder to simply turn off the computer. It's the surge protector and backup power supply that protects the computer from surges and power outages.

Most of the publicity surrounding computer crimes comes from dramatic break-ins from outsiders. What escapes the press is the fact that most security problems are caused by people who have a legitimate reason to use the system, for example, company officers or trusted employees. Don't overlook this potential security problem in your analysis of a commerce system.

Data Backup



As I have often said, there are three rules for data backup:

1. Backup the entire drive(s) daily
2. Backup the entire drive(s) daily
3. Backup the entire drive(s) daily

I don't think there is another more underutilized procedure in common practice. No matter how secure a site may be, it is never going to be foolproof. The practice of backing up your data can save a lot of time and effort if there is a break in (physical or electronic) to a website. Any damage done can quickly be mitigated with a good backup program.

Remember the client who had their file server stolen? The rest of that story is that our office provided the client with a similar machine in which the backup could be restored. It was surprising to discover that the client diligently backed up the system and rotated the tapes. However, the entire tape library was stored next to the file server and, unfortunately, was stolen along with the server.

We did locate a month-old tape of the client. When it was inserted into the tape drive, the tape software was unable to read the tape. We even took the tape to a disaster recovery specialist to evaluate the viability of the tape. It was not too surprising to learn that there were no data that could be recovered because there was nothing on the tape. Even though the backup system reported no errors upon completion of the backup routine, nothing was backed up!

There are two lessons to be learned from this story. One, make sure your clients follow the practice of storing backup tapes off-site, and, two, test the tape backup at least once a month. Your client will thank you even though this will cost the client a little more time. Backup beats the alternative my client faced—entering eight years of customer information including sales and cost of sales information!

Firewalls and Routers

The most important and highly fortified component of a medieval castle was its gateway. It allowed the inhabitants of the keep to come and go while barring entrance to its enemies.

Firewall gateways perform the same function. Firewalls allow access to the outer world while shielding the protected areas from attack. Permission to access the protected network must rely on secure authentication of an individual.

Management must not consider the installation of a firewall as the solution to all of its security problems when connected to the Internet. Firewalls provide a wide variety of control, but, in the end, they are only a tool. A firewall is part of a diversified defense strategy that identifies what must be protected and identifies the potential threats.

It seems obvious, but there is more to protecting a network than just protecting the hardware and software. Security comes from the union of superior technology, active and alert systems administrators, and management decisions regarding user access to the Internet and other computer resources. Prudence demands the development of a comprehensive plan to deal with system security. A working group created by technical personnel who implement part of the policy, management who has the authority to enforce policy, and representatives of the user-community must, at a minimum, do two things:

1. Identify assets to be protected.
2. Identify and assess the risks to those assets.

Firewalls are an important component in the overall security between the Internet site and the client's internal or private network. A firewall is comprised of both software elements and hardware components. An improperly configured firewall is as effective as putting a chain link fence around a tent.

Because this is an area new to most accountants, the following definitions of terms may be helpful:

- Bastion host—a general-purpose system used to control access between the internal network and Internet. Much like a castle and drawbridge (when the drawbridge is lowered, information can flow in both directions), the keeper of the drawbridge determines who/what is allowed in or out. This system allows information to flow in both directions and grants certain privileges to users on the network. Typically, the bastion program runs on a UNIX platform.
- Access control list (ACL)—as the name implies, this list is the matrix to which the firewall or router points to allow or deny access and privileges.
- Router—this is a physical device that allows networks to connect to one another. A router will typically route or manage various network functions and can filter out unauthorized or unwanted information packets.

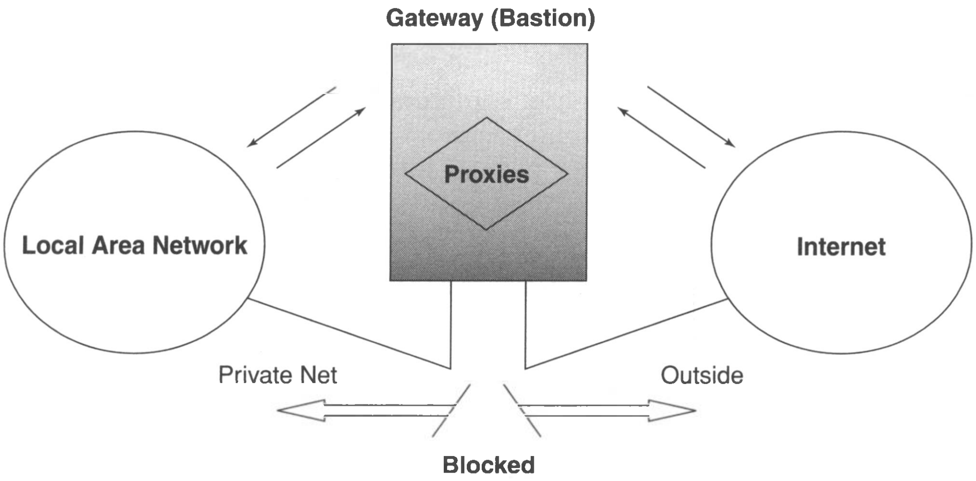
- Packet filtering—this is the process where a router passes information through the ACL and accepts or rejects the information packet. By default, most routers accept all network traffic.
- Proxy server—this is a process where a server will act on behalf of another server and, therefore free up the host server for other functions. The process works as follows: a URL points to a proxy server where there is a request from an end user. The proxy fetches the desired information from the host and transmits it to the user.
- Application gateway—this is a firewall made up of at least one bastion host and acts as a proxy server for a specific application. The clients that access an application gateway must be properly configured to take advantage of this firewall. By default, an application gateway allows no information to pass and, therefore, is the most secure firewall, because it must be specifically configured to allow access.

There are two basic implementations for firewall systems—the dual-homed gateway and the screen-host gateway. In the dual-homed gateway, the firewall machine has two network cards. One is attached to the internal network (local area network) and the other is connected to the untrusted network—or Internet. The machine is configured so that network packets reaching one card are not passed over to the other card. By default, then, the two networks are completely isolated.

However, because there is always a need for some communication between the two networks, specialized programs, called proxies, are run on the firewall machine. The job of the proxy is to selectively filter and forward information from one network to the other. Usually, a different proxy is responsible for each service—one for mail, one for FTP, and so on. Proxies can determine which network packets to forward by looking at the source and the destination addresses, by examining packet types, by examining the source and destination ports, or even by checking the data contained within the packet.

Network packets are never transferred directly. The data is first extracted and repackaged in new packets before transferring the data across the gateway.

The figure below illustrates the dual-homed gateway firewall configuration:



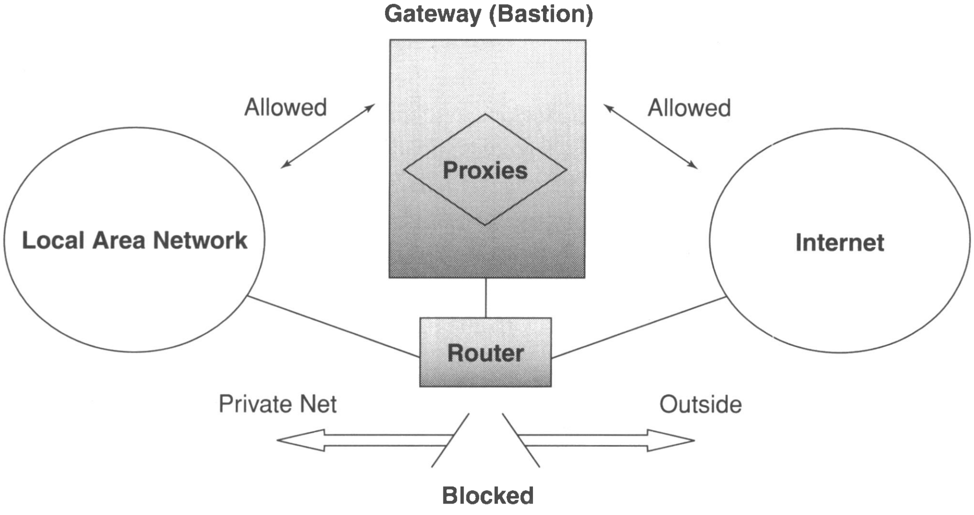
Dual-Homed Gateway Firewall

In a screened-host gateway approach, a network router is used to control access to the local area network. The router's function is to restrict communication between the inner and outer networks by ensuring that packets originating from the Internet can only reach the well-secured bastion machine where proxies repackage and transmit data to the inner network. As with the dual-homed gateway, the packets are examined and data checked before transmission occurs.

The nodes on the inner or local area network are invisible to the Internet machines. Outbound packets from the inner network are either restricted to the firewall machine, where they must be shepherded to the Internet through a proxy program, or the packets are allowed to pass directly through the router after being filtered to ascertain they are safe.

The figure below illustrates the screened-host gateway firewall configuration:

Screened Host Gateway Firewall



Screened-Host Gateway Firewall

Another variation of the screened-host configuration is the "screened subnet gateway." In this scenario, the router gives the outer network access to a small subnetwork known as the demilitarization zone (DMZ; see page 45 for diagram). The bastion host sits in the DMZ as well as all other servers that are to be made available, such as web or FTP servers. Another router, situated between the DMZ and the internal network, provides an additional layer of security.

In a well-designed firewall system, there is no real difference between the dual-home and screened-host systems. In each scenario, the local area network appears to the outside world as a single well-protected machine—the bastion host. All outgoing traffic appears to originate from the bastion, and all incoming traffic is directed to the bastion host. Software on the bastion checks each packet as it arrives, logs it, and allows it to pass through if it meets the rules and regulations set down by the system administrator.

When analyzing a firewall, don't be fooled by vendors that claim their firewall is certified. All this certification means is that it has been certified under certain conditions and specific configuration. Some vendors also claim that their firewall meets the US Department of Defense Orange Book standards. Again, this only means that the firewall was configured to pass a series of tests.

Make sure the firewall and router are configured properly for the conditions under which it will operate. Then, test the firewall and make sure it is doing its job (see the Firewall Evaluation Worksheet in Appendix C.) Finally, a word of caution about firewall configuration: a configuration must be constantly monitored and updated to reflect both changes in the network(s) it protects and advances in technology.

At the time this publication goes to press, seven vendors accounted for the majority of the commercial firewall market.

1. AltaVista (Digital Equipment Corporation) This firewall system uses a combination of packet filters, application-level proxies, and circuit level proxies. It runs on hardened versions of UNIX and Windows NT. Its major distinguishing features are extensive and customizable logging and log filtering. Tunneling is provided as an add-on feature.
2. BorderWare (Secure Computing Corporation) This package is a UNIX only system. It provides both application-level proxies and packet filtering. Administration is by graphical interface only. Tunneling is provided as an add-on feature.
3. CyberGuard Firewall (CyberGuard Corporation) This package is a UNIX only system that covers all the basic areas—packet filtering, application proxies, and stateful inspection. Its features are configured and managed using a graphical user interface.
4. Eagle (Raptor Systems) Eagle uses application and circuit level proxies. It is available for NT as well as a variety of UNIX systems. Currently no tunneling is provided nor is support for certain protocols, e.g. S-HTTP r Quicktime.
5. Firewall-1 (Checkpoint Software Technologies) This system provides a combination of packet filtering and stateful inspection. It is available for NT as well as a variety of UNIX systems. The system has an intuitive graphical interface and provides support for a large number of protocol, including some of the newer multimedia formats. Tunneling is available as an add-on feature.
6. Gauntlet (Trusted Information Systems) This system is available as a software only package or as a turnkey hardware and software system. Gauntlet uses application level proxies for filtering. A general circuit level, plug-in proxy is available as well as packet filtering. Tunneling is provided as an add-on feature.
7. ON Guard (ON Technology Corporation) This product is distinguished from others in that is uses SMLI filters. ON Guard is the only firewall in this group to run on a hardened version of Windows 95/98. Tunneling is not yet available.

Firewall Requirements

Although it is possible to make a single system fairly secure, it is more difficult to secure all systems on a private network, because a private network provides too many opportunities for program errors or configuration errors. If it were possible to secure each machine on the network, its users would probably dislike the required restricted functions.

Using a secure firewall between the Internet and the private network does not eliminate the need for sound security practices on the systems inside the private network. The firewall, when placed in the configuration mentioned, will, however, significantly enhance overall system security by presenting an extremely daunting barrier to the external intruder.

To succeed in repelling unwanted intruders while still providing access to the outside world, the firewall must meet the following requirements:

- The firewall MUST NOT forward IP packets between two networks unless the packets have the firewall system as their destination or origin address. Consequently, a user on an external system must, first, login to the firewall system before gaining access to a protected system. This step adds an extra level of complexity but greatly enhances security.
- The firewall must hide the structure of the internal protected network from the outside network, so intruders do not have this information when attempting to breach system security.
- The firewall MUST NOT provide dynamic routing, because this can be used to support multiple security attacks such as route spoofing. The system administrator should provide static routing.
- The firewall must provide outbound telnet, ftp, Mosaic, and gopher services for users on protected systems.
- The firewall must provide a strong user authentication scheme that does not rely on static User ID and passwords, because they can be compromised.
- External ftp users should NEVER be allowed, because ftp relies on the use of static User IDs and passwords. If a cracker acquires a legitimate user ID and password, then the cracker can ftp to the users system and execute the ftp subcommands. Subcommands provide the cracker with ample opportunity to acquire, alter, or destroy data accessible by the compromised user account.
- The firewall should reject protocols that have dangerous security exposures and should not be used by people outside the protected network access-protected systems. These include the following protocols: rexec, rlogin, rsh, rwho, and tftp. X-window applications running on unprotected systems should not be accessed directly from a protected system.
- The firewall must NOT allow an external user to login as root.
- The firewall must reject unknown protocols.
- The firewall must provide Internet Domain Name Services (DNS) to the outside network for systems in the protected network.
- The firewall must distinguish whether a user comes from an external unprotected system or an internal protected system.
- The firewall must be able to enforce tighter controls on user function when the user logs in from an external system versus an internal system.
- The firewall must eliminate the telnet "open" command.
- The firewall should act as a "simple mail transfer protocol" (SMTP—a protocol used to transfer email from server to server) mail gateway. The systems administrator

should configure the firewall so that all outgoing mail appears to come from the firewall machine. The firewall system should translate all the mail header fields containing internal addresses (To:, From:, CC:) to an external form such as user@bubblegum.com. Because all external mail is routed through the firewall, the system should have a complete set of aliases to redirect the mail to the appropriate internal system and user.

- Only internal users who need access to the outside network and external users who need access to the internal network should have User IDs and passwords on the firewall.
- The firewall system should deactivate all unnecessary functions.
- The firewall should create, maintain, and protect an audit trail of system activity from modification or destruction. Part of the trail of activity should include all successful and unsuccessful attempts to use the system. The audit record should include the user's name, type of event, the event's success or failure, and the origin (IP address) of the event, including date and time.
- The firewall should provide automated procedures to verify that the Trusted Computing Base (TCB) has not been modified. The system should check its own integrity.
- The firewall should provide high levels of performance at a reasonable cost. FTP performance should be limited by the LAN speed not by the firewall. If the firewall is too slow then users will bypass it.
- The firewall must not detract from easy Internet use.
- Access of authenticated authorized users entering the secure network from the Internet must be controlled.

Configuring a Firewall

The remainder of this section will be devoted to the issues of configuring a firewall. To keep the discussion generic when describing routing tables, we will use a table-based format that is not specific to any particular company, and one that has been tested over time. To discuss the application level proxies, examples used in many text-based configuration systems, you may wish to use the TIS Firewall Toolkit. This toolkit can be obtained from: ftp://ftp.tis.com/pub/firewalls/toolkit/.

With a firewall installed, there are two basic issues to address: (1) how to allow people within an organization to safely browse the Internet, and (2) how the client's web site is made available to others when browsing the Internet.

Outgoing connections to the Internet are usually controlled through a pack filter. If the firewall is of the older variety, filter exceptions need to be provided for outgoing connections to the HTTP (port 80), FTP (port 21), SSL (port 443), and Gopher (port 70) services as well as for data sent back in response to those connections. The following table shows a stylized representation of a firewall's filter table.

The first column shows the appropriate action to take—to either block or allow packet flow. The "Service" and "Port" columns represent the source of the packet by TCP/IP address and by port. In the service column, {I Net} represents the organization's network address. The "Destination" and "Port" columns show the intended recipient by the destination address and port. The column labeled "Flags" contains TCP header fields that can be used for filtering. In this example, the only important flag is ACK, representing a continuation of a network conversation initiated earlier.

Action	Service	Port	Destination	Port	Flags	Comment
Block	*	*	*	*	*	Blocked all by default
Allow	{I Net}	*	*	80	*	Outgoing web
Allow	*	80	*	*	ACK	Incoming web
Allow	{I Net}	*	*	21	*	Outgoing FTP control channel
Allow	*	21	*	*	ACK	Incoming FTP control channel
Allow	{I Net}	*	*	≥1024	*	Outgoing FTP data
Allow	*	≥1024	*	*	ACK	Incoming FTP data
Allow	{I Net}	*	*	443	*	Outgoing SSL
Allow	*	443	*	*	ACK	Incoming SSL
Allow	{I Net}	*	*	70	*	Outgoing Gopher
Allow	*	70	*	*	ACK	Incoming Gopher

The filtering rules shown above represent the minimum structure needed to support web browsers. Other rules will be necessary for outgoing email (port 25), SSL (port 443), plus other services provided by the server.

If application-level proxies are used to provide Internet access to the firewall, separate proxies will need to be enabled for each protocol. The TIS Toolkit comes with a proxy called http-gw. This proxy handles both HTTP and Gopher protocols. The kit also contains a proxy, ftp-gw for FTP.

The proxy's functions are to allow incoming connections from one side of the firewall, filter them, and then forward the packets to the other side of the firewall. When proxies are first installed, they do not distinguish whether the proxies will service requests from the local area network or from the Internet. Distinguishing these actions is done by configuration and by policy. In a basic configuration, all hosts on the local area network are allowed access to the proxies—everyone else is denied access.

Assume that the LAN has a TCP/IP address at 192.44.187. Here is a simple illustration of this configuration:

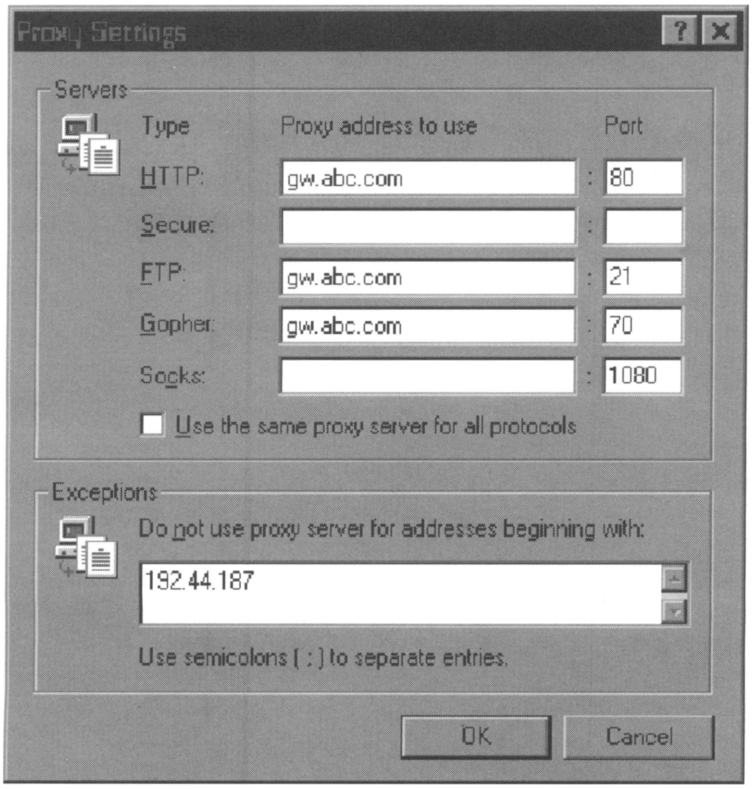
```
# Rules for the FTP Gateway for ABC.COM
    ftp-gw:  denial-msg        /usr/local/etc/ftp-denied.txt
    ftp-gw:  welcome-msg       /usr/local/etc/ftp-hello.txt
```

```
          ftp-gw:  help-msg           /usr/local/etc/ftp-help.txt
          ftp-gw:  timeout            3600
          ftp-gw:  deny-hosts         unknown
          ftp-gw:  permit-hosts       192.44.187.*
     # Rules for http/Gopher Gateway for ABC.COM
          http-gw:  permit-hosts      192.44.187.*
```

The first six lines set up the rules for the FTP proxy including the messages to deliver when a user: (1) is denied access (denied.txt); (2) is permitted access (hello.txt); or (3) needs help (help.txt). The line containing *deny-hosts* prohibits the use of the proxy by any machine that does not have a domain name entry. This prohibition is a good control, because it restricts FTP service originating outside the local area network. The line containing *permit-hosts* allows any host in the internal network to use all proxies. All others outside the local area network are denied access by default.

Once the HTTP and FTP proxies (and any other services to be offered by the server) are properly configured, the browser needs to be configured as well. To overlook this step is to leave the back door open. The figure below shows a screen with the browser configuration from Internet Explorer. A similar configuration screen exists for Netscape Navigator.

Browser Configuration from Internet Explorer



Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:	gw.abc.com	80
Secure:		
FTP:	gw.abc.com	21
Gopher:	gw.abc.com	70
Socks:		1080

□ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

192.44.187

Use semicolons (;) to separate entries.

The port numbers used should be the standard port numbers unless a nonstandard configuration exists. A complete listing of standard ports is included in Appendix G. The secure field is for SSL (not being used in our example). If a private web server or Intranet is running on the internal network, then no *proxy server for addresses* box should be filled in. Filling in this information would prevent the browser from trying to access a proxy server. Socks host should be left blank, unless the firewall uses that service.

If socks is being used for a circuit level proxy, it will be necessary to configure the proxy to allow outgoing connections through the Web, FTP, SSL, and Gopher ports. The following basic configuration for a socks proxy is set up to allow hosts inside the network (199.44.187) to get out but prohibits the use of all proxies from outside hosts.

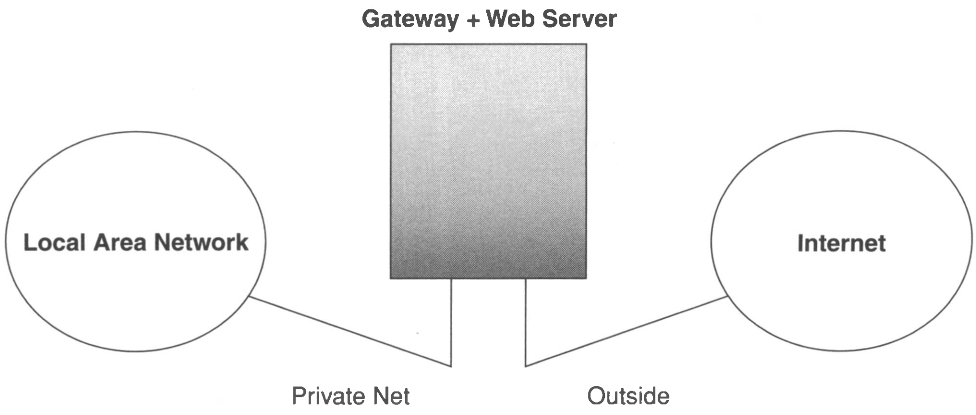
```
#action  #source            #netmask          #destination      #netmask
#deny the world access to the proxy
deny  0.0.0.0               0.0.0.0.          192.44.187.0      255.255.255.0
#permit access to the proxy from anyone on the internal network
permit  192.44.187.0        255.255.255.0
```

Once the socks proxy is configured, make sure the browsers have the correct configuration as well.

Now that outgoing traffic has been secured through the firewall, it is time to address the challenge of permitting the world access to the web server. There are really only three places where a web server can be placed in relationship to a firewall, although several combinations and configurations exist. The web server can go behind the firewall on the inner network, outside the firewall on the outer network, or it can be run on the firewall machine itself.

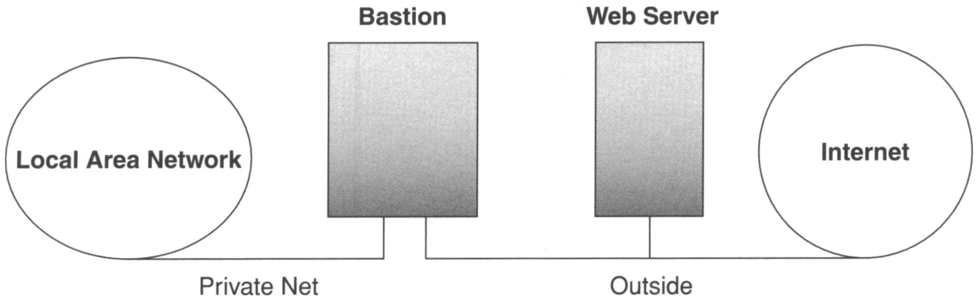
It may seem at first glance that a good place to put the web server is on the same machine as the firewall. This is sometimes called the *Judas server*. The problem with this configuration, shown below, is that the web server software cannot be trusted. Any weakness in the server software that is compromised could permit access to the firewall system.

Judas Server Configuration



The safest place for a web server is outside the firewall, in the area between the firewall and the connection to the Internet service provider. This configuration is sometimes called the *sacrificial lamb* and appears below.

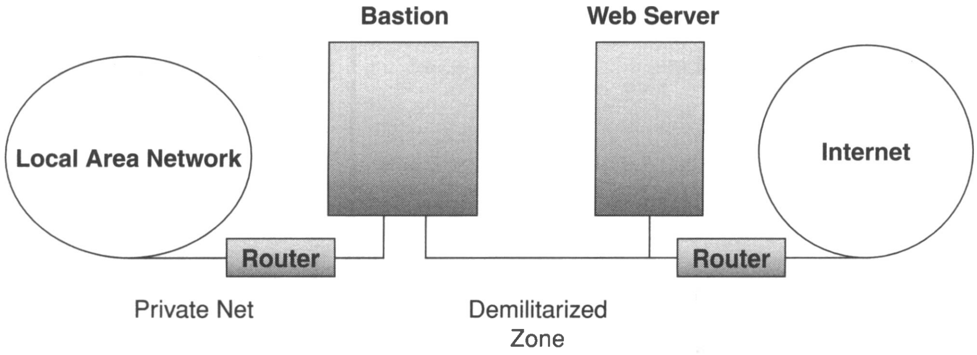
Sacrificial Lamb Configuration



In this configuration, the server is locked outside the protection of the firewall and exposed directly to the attempts of intruder break-ins. With the server isolated, the server should be made as secure as possible. Frequent backups and monitoring of the server logs should be a priority. If the worst-case scenario occurs and the server is compromised, backups and monitoring logs can help ensure that the company network is protected and integrity is not compromised.

If the firewall system creates a DMZ—a segment of network that is separated by routers on both the local area network and the Internet sides—it is possible to create a web site that is not as exposed as it is in the sacrificial lamb configuration. See the figure below, which illustrates the configuration of a server inside a DMZ. By simply placing the server inside the DMZ and configuring the routers and gateway so that the hosts on both the LAN and Internet can establish HTTP connections, there is server protection to both the web server and the LAN. All non-HTTP connections should be rejected.

Server Inside DMZ



The following table illustrates rules for filtering that provide for strong security for the screened-host firewall. The logic here is similar to the filtering already discussed for generic firewalls but more focused for the screened-host.

Action	Service	Port	Destination	Port	Flags	Comment
Block	*	*	*	*	*	Blocked all by default
Allow	{world}	*	Gateway	*	*	World can talk to gateway
Allow	{I Net}	*	Gateway	*	*	Internal net can talk to gateway
Allow	Gateway	*	*	*	*	Gateway can talk to everyone

Encryption

Encryption, or the coding of messages, has been around for as long as we have had secrets to keep. The methods we use to encrypt or decrypt are a key issue in the protection of private customer information. Most encryption today is based on mathematical techniques and formulas called algorithms.

A key is used with the algorithm to convert the text or other material to encrypted text called ciphertext. This same key is used to decrypt the information as well.

There are many symmetric key algorithms in use today. A summary of some of the algorithms commonly used on the World Wide Web includes:

Name	Description
DES	The Data Encryption Standard was adopted as a US government standard in 1977 and as an ANSI standard in 1981. The DES is a block cipher that uses a 56-bit key.
DESX	DESX is a simple modification to the DES algorithm that is built around two whitening steps. These steps improve the security of the algorithm and render key searches impossible.
Triple-DES	Triple-DES is a way to make the DES at least twice as secure by using the DES encryption algorithm three times with three different keys. Triple-DES is currently being used by financial institutions as an alternative to DES.
Blowfish	Blowfish is a fast, compact, and simple block encryption algorithm invented by Bruce Schneier. The algorithm allows a variable length key, up to 448 bits, and is optimized for execution on 32- or 64-bit processors. For this reason it is popular with today's processors. The algorithm is unpatented and is in the public domain.
IDEA	The International Data Encryption Algorithm (IDEA) was developed in Zurich by James Massey and Xuejia Lai and published in1990. IDEA uses a 128-bit key and is used by PGP (Pretty Good Privacy) encryption program.
RC2	This block cipher was developed and kept a trade secret by RSA Data Security. The algorithm allows for keys between 1 and 2048 bits. The key is often limited to 40 bits and used in software sold for export.
RC4	This block cipher was developed and kept a trade secret by RSA Data Security. The algorithm allows for keys between 1 and 2048 bits. The key is often limited to 40 bits and used in software sold for export.
RC5	RC5 allows for a user-defined key length, data block size, and number of encryption rounds.

Cryptographic Strength

All forms of encryption are NOT equal. Some systems are not very good at protecting data. Others are quite strong and resistant to the most determined attack. The ability of cryptographic systems to protect information from attack depends on many factors, including:

- The secrecy of the key
- The difficulty of guessing the key—longer keys are generally more difficult to guess or find
- The existence (or lack of) back doors or other ways by which an encrypted file can be decrypted without knowing the key
- The ability to decrypt an entire message from knowing the way that a portion of it decrypts—often called a *known plaintext attack.*
- The properties of the plaintext and knowledge of those properties by an attacker. For example, a cryptographic system may be vulnerable if all messages are encrypted with a known piece of plaintext at the beginning or end of the message.

Cryptographic strength can almost never be proven; instead, it must be disproved. Creators of new algorithms believe that the new algorithms are perfect. There is evidence that the newly developed algorithm is resistant to specific known attacks. As time passes, new attacks are developed, and if a weakness is discovered, information about the weakness is quickly published on the Internet.

Attacks on Encryption Algorithms

Attacks against encryption information fall into three main categories:

1. Key search—or brute force attacks
2. Cryptoanalysis
3. Systems-based attacks

The simplest way to crack a code is by trying every possible key, one after the other. This method of code cracking is called a key search attack. Most key search attacks will not be successful, although it is possible to crack an encryption code in this manner. There is no way to defend against a key search attack, but such attacks are extremely inefficient.

How easy is it to break the code? The amount of time it takes to break the code depends on the length of the key used to encode the message. A 56-bit key has 2^{56}, or roughly 72,057,594,037,900,000 different keys. The following table gives the estimated times to crack symmetric algorithms with various key lengths with current technology.

	Cost ($)	
Key Length	Thousands to Invest	Millions to Invest
40 bits	Seconds	<1 second
56 bits	Days	Hours
64 bits	Months	Days
80 bits	Eons	Millennia
128 bits	>Age of the Universe	>Age of the Universe

Cryptoanalysis is the "science" of encryption. By using mathematics and computers, the cryptoanalyst has two possible goals. If the analyst has the ciphertext, he or she might want to discover the plaintext message, or if the analyst has the plaintext, he or she might want to discover the encryption key. By using pure mathematics and the power of today's desktop computers, some encrypted messages can be deciphered without knowing the key.

Another way of breaking the code is to attack the system that uses the cryptographic algorithm without attacking the algorithm itself. An example of one such attack occurred when there was an attack on the random number generator that SSL uses to generate its session key. A weakness was discovered where the random number generator was bypassed, therefore eliminating the need to guess a key.

Consider the following examples reflecting two types of cryptography: (1) single-key and (2) public/private key.

Single-Key Cryptography

Bob has one secret key. If Alice wants to send Bob a secret message:

- Bob sends Alice a copy of his secret key
- Alice encrypts message with Bob's secret key
- Bob decrypts message with his secret key

- Problems:
  - How does Bob get his secret key to Alice?
  - What if Alice is a double agent?
  - What if Alice, Bob, Charley, and Dan need to exchange messages? In this case, they would need n! secret keys

Public/Private Key Cryptography

Bob has two *complimentary keys.* What one key encrypts, only the other key can decrypt.

- Bob keeps one key private (private key)
- Bob keeps one key public (public key)
- If Alice needs to send Bob a message
  - Bob sends Alice a copy of his public key
  - Alice encrypts message with Bob's public key
  - Bob decrypts message with his private key

- Advantages:
  - Bob can distribute public key freely
  - If Alice is a double agent, she can't do any harm with Bob's public key
  - Bob only needs one key pair, no matter how many people he speaks to
  - Bob can digitally "sign" messages by encrypting with his private key

For additional information on the workings of public/private key encryption visit http://www.verisign.com/server/whitepaper/secure/nav.html.

The following information summarizes the public key systems in common use today:

- Diffie-Hellman key exchange

A system for exchanging cryptographic keys between active parties. This system is not actually a method of encryption and decryption; instead, it is a method of creating and sharing private keys over nonsecure public channels. The system works by having the two parties agree on common numerical values; then, each party creates a key.

- RSA

RSA, developed by MIT professors, is perhaps the most well-known public key cryptography system available for both encrypting data and serving as the basis of a digital signature system. Digital signatures can be used to authenticate the data or prove authorship. The key can be any length and depends on the implementation used.

- ElGamal

This system bears the name of its creator, Taher ElGamal, and is a public key encryption system that is based on the Diffie-Hellman key exchange.

- DSS

The Digital Signature Standard (DSS) was developed by the National Security Agency (NSA) and has been adopted as the Federal Information Processing Standard by the National Institute for Standards and Technology. DSS can only be used for digital signatures.

Attacks on Public Key Algorithms

In theory, attacks on public key algorithms are easier because the attacker has the public key of the algorithm. The job of attacking public key algorithms is made even easier because the public key message identifies which public key encryption algorithm was used. There are two basic methods of attacking a public key algorithm:

- Factoring attacks
- Algorithmic attacks

Factoring attacks are the most common type of attack on public key encrypted messages, because they are the easiest to understand. Attacks of this nature attempt to derive the private key from the corresponding public key. For example, an attack on an RSA key would be performed by factoring a number that is associated with the public key. Other public key attacks would use similar methods involving complex mathematical equations.

The strength of RSA and other algorithms comes from the difficulty of factoring large numbers. RSA is confident with its algorithms so much so that it sponsors factoring challenges from time to time. You can obtain a complete list of the current challenges along with the corresponding cash reward by sending a message to challenge-rsa-list@rsa.com.

Algorithmic attacks are more difficult to perform because these attacks are based on the algorithm itself. The attacker attempts to find and then exploit a flaw or weakness in the formula.

Although cryptography is an important element in Web security, it is not all-powerful. The following scenarios are beyond the scope of cryptography and require other forms of security:

- Cryptography cannot protect unencrypted data
- Cryptography cannot protect against stolen/compromised keys
- Cryptography cannot protect against denial-of-service attacks
- Cryptography cannot protect against encryption software bugs or flaws
- Cryptography cannot protect against mistakes or collusion

Current Working Encryption Systems

There are two basic categories of encryption systems in widespread use: those that encrypt emails, e.g. PGP and Secure/MIME (S/MIME); and network protocols used to provide confidentiality, authentication, integrity, and nonrepudiation, e.g. SSL, S-HTTP, SET, and SSH.

- PGP

One of the first widespread public key encryption programs, "Pretty Good Privacy" (PGP, developed by Phil Zimmermann) was released in June 1991. PGP, in addition to being a complete system for encrypting emails and files, is a set of standards that provide layouts for messages, keys, and digital signatures.

PGP is a hybrid system that uses RSA public key encryption for key management and IDEA symmetric cipher for the bulk encryption of data. One of the main drawbacks of PGP is the management and certification of public keys. The key never expires. So, when a key is compromised, it is up to the holder of the key to distribute a special PGP revocation certificate to everyone with whom they have communicated.

- S/MIME

The Multipurpose Internet Mail Extensions (MIME) is a standard for sending messages with binary attachments. S/MIME extends this standard to allow for encrypted email. S/MIME was implemented as a toolkit designed to be added to existing packages as opposed to being a stand-alone program.

This toolkit comes from RSA Data Security and includes all of the needed licenses, algorithms, and patents. Because many technology companies already have a business relationship with RSA, it would appear that S/MIME would be adopted by most vendors in preference to PGP.

- SSL

SSL, or Secure Socket Layer, is a general-purpose cryptographic protocol for securing communication channels both coming from and going to a server. It is commonly used with the TCP/IP protocol. SSL connections are initiated on the Internet through the use of a special URL such as "https" to indicate a secure http session or "snews" for a secure news session.

Confidentiality is achieved through the use of a user-specific algorithm. Each new SSL session generates a new key. Microsoft's version of SSL is called PCT. It would appear, however, that PCT will not become an industry standard, despite Microsoft's backing. See more information about the features of SSL in the section "Understanding More about SSL" below.

- S-HTTP

S-HTTP is a system for encrypting and signing data over the http protocol. S-HTTP was developed before SSL was adopted.

- SET

Secure Electronic Transactions (SET) is a protocol designed for sending encrypted credit card numbers over the Internet. SET offers confidentiality for credit card numbers, because they are encrypted and sent directly to the clear bank or agency. Other information, such as the customer name and address is not protected.

- SSH

SSH is the secure shell. It allows for encryption and protection of the virtual terminal (Telnet) and file transfer (rcp) functions. SSH is available for UNIX, Windows, and Macintosh systems.

Other Protocols

We present a summary of current working encryption systems below, including other protocols such as DNSSEC and others that are not common but have some Internet use.

Summary of Current Working Encryption Systems

System	Definition	Algorithms Used	Provides
PGP	Application program for encryption of email	IDEA, RSA, MD5	Confidentiality, authentication, integrity & nonrepudiation
S/MIME	Format for encryption of email	User specified	Confidentiality, authentication, integrity & nonrepudiation
SSL	Protocol for encryption of TCP/IP transmissions	RSA, RC4, RC5, MD5	Confidentiality, authentication, integrity & nonrepudiation
PCT	Protocol for encryption of TCP/IP transmissions	RSA, RC4, RC5, MD5	Confidentiality, authentication, integrity & nonrepudiation
S-HTTP	Protocol for encrypting HTTP	RSA, DES	Confidentiality, authentication, integrity & nonrepudiation
SET	Protocol for sending secure payment	RSA, MD5, RC2	Confidentiality of credit card information, integrity of entire message, authentication of buyer and seller & nonrepudiation of transaction
DNSSEC	Secure domain name system	RSA, MD5	Authentication & integrity
Ipsec and Ipv6	Protocol for encrypting IP packets—low level encryption	Diffie-Hellman	Confidentiality, authentication & integrity
Kerberos	Network security service for securing high level applications	DES	Confidentiality & authentication
SSH	Encrypted remote terminal functions	RSA, Diffie-Hellman, DES, Triple DES, Blowfish	Confidentiality & authentication

Understanding More about SSL

Because many web sites will make use of SSL for securing transactions, we revisit the topic here in more detail. Developed by Netscape, SSL was first used in Netscape's browsers and web servers. The SSL concept was developed to encourage the sale of Netscape's web server by providing a free client in the browser that utilized the same cryptography protocol.

Now, SSL is incorporated into most browsers and servers, because it has become a necessity for Internet security. The Internet Engineering Task Force is now in the process of creating a Transport Layer Security (TLS) based largely on SSL version 3.0.

SSL is a layer that exists between the TCP/IP protocol and the application layer. Standard TCP/IP sends anonymous, error-free data between two computers; SSL adds several features including:

- Authentication and nonrepudiation of the server using digital signatures
- Authentication and nonrepudiation of the client using digital signatures
- Data confidentiality through the use of encryption
- Data integrity through the use of message authentication codes

SSL uses separate algorithms for encryption, data integrity, and authentication with different keys or secrets for each function. This feature is much like segregation of duties that provides functionality and protection. The primary advantage of this segregation of duties is to allow for longer keys for authentication and data integrity than the key length used for privacy. Because key length is an issue for products exported outside the US and Canada, SSL is well suited for global applications. The Federal government has placed limitations on key length for confidentiality, but not for authentication or data integrity.

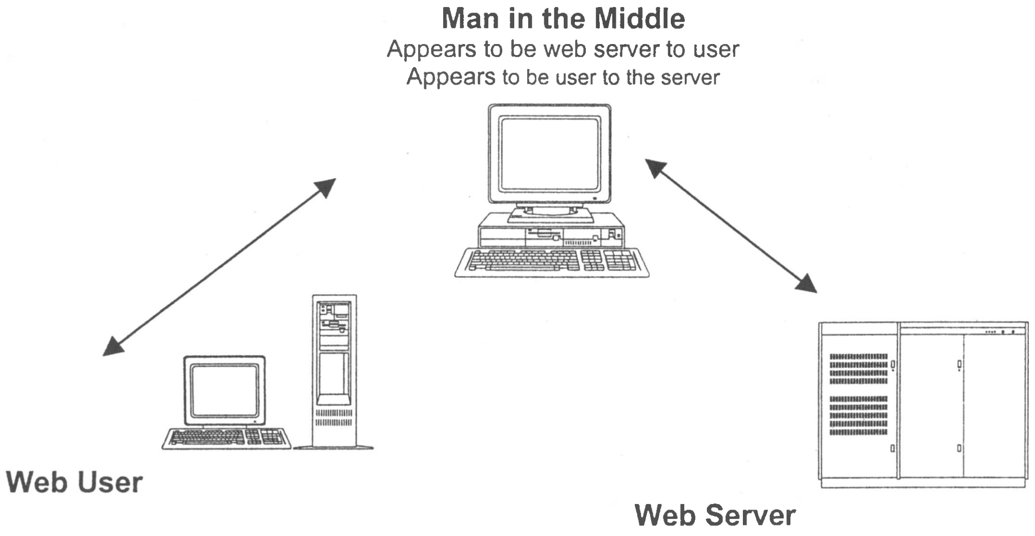
The choice of the algorithm and corresponding key length used is determined first by SSL server and then limited by the client.

Efficiency is another feature that makes SSL a useful Internet tool. Public key encryption/decryption is a time-consuming process. Rather than repeat this process for each communication between the server and the client, SSL caches a "master secret" that is preserved between SSL connections. This allows new SSL connections to immediately begin secure sessions with the need to produce another public key.

SSL was designed initially for TCP/IP communications but can run on top of any reliable protocol, such as X.25 or OSI. A nonreliable protocol such as UDP (User Datagram Protocol) will not permit an SSL connection. The following exhibit shows the ports that SSL uses and their functions:

Keyword	Decimal Port	Function
https	443/tcp	Secure HTTP
Ssmtp	465/tcp	Secure send mail
Snews	563/tcp	Secure Usenet news
ssl-ldap	636/tcp	Secure LDAP
spop3	995/tcp	Secure receive mail

SSL was specifically created to protect against "Man-in-the-Middle" and "Replay Attacks." In a man-in-the-middle attack, an attacker intercepts all of the communication from the client and server, making the client think it has communicated with the server and the server with the client.


Man in the Middle
Appears to be web server to user
Appears to be user to the server
Web User
Web Server

SSL provides protection from this type of attack by using digital certificates to allow the client to "learn" the validated name of the web site.

A replay attack includes an attacker who captures the communications between the server and the client and then replays the messages. For example, an attacker may capture personal financial data, e.g., credit card numbers and passwords, while the customer is making a payment for merchandise.

Encrypted data cannot be compressed because good encryption algorithms remove any repetition or self-similarity that is typically removed for compression. If data can be compressed after it has been encrypted, then the encryption program has serious flaws.

Because encrypted information cannot be compressed, SSL allows for the data to be compressed before it is encrypted. SSL supports many compression algorithms. More information can be obtained about SSL from the following source: http://developer.netscape.com.

As stated previously, a task force has been created that is putting together standards regarding security. Information concerning the history, standardization and on-going activities of Transport Layer Security (TLS) can be found at:

http://lists.w3.org/archives/public/ietf-tls/msg00185.html

http://lists.w3.org/archives/public/itef-tls/msg00211.html

http://lists.w3.org/archives/public/itef-tls/msg00212.html

http://www.consensus.com/ietf-tls/

Virus-Scanning Software

Viruses come in all shapes and sizes. Viruses are the topic of many news groups and emails, and new ones spring up all the time. For these reasons, virus software companies have a hard time keeping up with the rapid pace of change required. Nevertheless, virus-scanning software is a must on any system accessing the World Wide Web.

The best protection against viruses is only as good as the software release. Make sure the virus software you have is the most current version of the product with the correct patch installed. Then make sure that you have the most up-to-date copy of the virus list with its associated "footprint." The footprint is how the software detects a virus or potential virus. All viruses leave their mark or footprint on a file. By looking for this footprint, the software can detect and hopefully remove a virus.

Because viruses change at such a fast rate, it might be a good idea to consider running two different scanning softwares on systems at all times. What one software misses the other should pick up. The overall overhead of running two softwares might reflect some losses in system efficiency. However, the losses experienced are not significant when compared with the gains offered in added protection.

In a biological world, differences between species prevent germs and illnesses from becoming a plague that will wipe out all life forms. No two individuals are exactly alike—some are susceptible to a disease, whereas others are resistant. In a software/hardware world, the differences in operating systems are equivalent to biological variability. A virus that is harmful in a Windows environment does not affect a Macintosh machine. This phenomenon, however, is changing.

As we move toward network platforms that allow for access of data among Windows, Macintosh, Unix, and other systems, there is a need for these machines to run the same programs and share files and other information in a seamless manner. The most likely sources of this cross-platform equalization are Sun Microsystem's Java and Microsoft's ActiveX.

If Java and ActiveX programs can run on all computers, so can Java and ActiveX viruses. Although these viruses don't exist, as this document goes to press, they will exist in the foreseeable future. These viruses will be able to spread from machine to machine across the Internet, unimpeded by small details like operating systems and hardware type. This situation is similar, but perhaps more threatening, to the cross-platform Microsoft Word macro viruses that spread, easing from Windows to Macintosh machines in concealed Word document files.

For this reason, it is imperative that you stay current with the developments in the area of viruses and changes in virus-related programs. Not only should you ensure that your virus software is current, but also make sure that you remain abreast of developments in this area. Sites like http://ciac.llnl.gov/ciac/CIACWelcome.html, Computer Incident Advisory Capability, provides information regarding computer security incidents, hoaxes, and viruses or http://kumite.com/myths, Computer Virus Myths, are an excellent source of virus information readily available on the Internet.

Passwords

Easily implemented and often overlooked, passwords are in every facet of our society. The problem with passwords is that most people either don't use them or, if they do, everyone in the office knows what the password is.

The following are some tips that the practitioner should consider in an evaluation of the password policy for a WebTrust client. You may use these tips in your own security document.

- Passwords should not be the same as a log-in name or other familiar piece of information (birthday, street address, type of car, etc.).
- Passwords should not be comprised of cute or clever phrases such as "password," "comein" or "letmein."
- Make passwords longer than 4 characters and require non-alpha numeric characters in the password – #, $, &, ^ etc.
- Make sure passwords do not contain repeated (bbbbbbb) or sequential digits (12345678 or zxcvzxcv).
- Create passwords from everyday phrases and use the first letter of each word to form the password—one small step for man becomes ossfm# (adding the # for more protection).
- Passwords should not be a word found in the dictionary or words from the dictionary appended with a digit (computer7). Dictionaries are the first place a cracker goes.
- If the system is case-sensitive, use mixed case passwords for additional security—wiLdmAn, for example.

One final comment about passwords—don't keep a listing of passwords where it is easy to copy. For example, a document containing a password list stored on-line is vulnerable; also, the password written on a "post it" note and stuck to the monitor or under the keyboard is likely to be compromised. Common sense in password protection cannot be overemphasized.

Major Host Security Problems

Many times security problems at a site result more from not paying attention to details rather than from some other issue. We provide a checklist of details for your information:

- Failure to think about security as a fundamental aspect of systems setup and design—no established security policy
- Transmission of plaintext, reusable passwords over networks
- Failure to use security tools—COPS, SATAN, etc.
- Failure to obtain and maintain software that is free of bugs and security holes
- Failure to track security developments (and published bugs) and take preventive action
- Lack of adequate logging
- Lack of adequate system monitoring and network monitoring

Security Policies

Security is defined by policy. In some environments, every user is allowed access to install, modify, and delete web content. In other situations, only a few individuals with the right permissions have this ability. The topic of policy is so complex that we only outline some of the major points about policy. Give consideration to the following policy-related items:

- Who is allowed access, what is the nature of that access, and who authorized such access?
- Who is accountable for security, upgrades, backups, and maintenance?
- What kind of material is allowed on server pages?
- Which sites and external users are to be allowed access to pages and data?
- What testing and evaluation must be performed on software, pages, and scripts before they are installed?
- How are complaints and requests about server and page content to be addressed?
- What is the procedure to handle security incidents?
- What is the process to monitor, evaluate, and update the security policy itself?

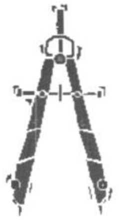
Password Policies

Undoubtedly, the most significant security risk on the Internet today is the use of plaintext, reusable passwords. Usernames and passwords are the most common way to authenticate users. For that reason, it is important for organizations to follow a clear and consistent policy regarding passwords. Consider the following aspects of password attributes:

- Structure—length and character composition
- Life span—period of time password is valid
- Risk evaluations
  - Plaintext
  - Password sniffing
  - Common words or phrases

Security Tools

A security tool is a special program that is executed to evaluate, enhance, or monitor the security of a site. Most security tools were written at universities or by independent specialists and are freely distributed over the Internet. You can bet that potential intruders are using these tools to find, and possibly exploit, security weaknesses. There are four types of tools to consider:



(1) *Tools that take a "snapshot" of the system and look for potential weaknesses:*

- COPS—UNIX
- Tiger—UNIX
- Kane Security Analyst—Windows NT

A snapshot program should be run on a regular basis—no less than once a month and ideally once a week. The client should not leave the output from a snapshot program in a place where it is accessible to others, because by definition, the holes that these programs reveal can be exploited by others.

(2) *Tools that monitor the system over time, looking for unauthorized changes:*

- Tripwire—UNIX
- Intrusion Detection—Windows NT

It is important to monitor the system on a regular basis for unauthorized changes. The first thing an attacker usually does after gaining access to the system is to modify it to make it easier to regain access in the future. Most break-ins go unnoticed for some time, therefore, change-detecting tools may be the only way your client will be alerted to an intruder's presence so that he or she can take appropriate action.

(3) *Tools that scan the network, looking for network-based weaknesses:*

- SATAN—UNIX
- ISS (Internet Security Scanner)—UNIX
- SomarSoft—Windows NT

Tools that scan the network automate many security procedures on the network. They check for well-known security-related bugs such as sendmail and ftpd. Your client's systems are certain to be scanned by crackers interested in gaining access to your systems, so your client should run these programs and learn what weaknesses they reveal.

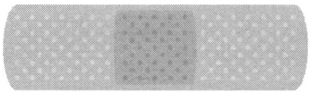
(4) *Tools that monitor the system and network looking for attacks in progress:*

- Stalker and WebStalker—Haystack Labs
- NetRanger—WheelGroup
- Gauntlet ForceField—Trusted Information Systems

Monitoring tools are the operation system equivalent of a burglar alarm. As their name implies, these tools scan a computer as it runs, watching for telltale signs of a break-in, much like a virus-scanning software.

Software—Patches, Bugs, and Updates

Another potential area of weakness in your client's systems will be the software that runs on the system itself. The presence of bugs can cause the server or client to crash or corrupt the information, or, worst of all, bugs can allow outsiders unauthorized access.



When purchasing new software consider the following:

- Proof of good software engineering practices in the design, coding, and testing
- Documentation showing the results of operational and stress testing in an environment similar to the one you intend to use
- A written statement of the vendor's policy for accepting, documenting, responding, and communicating reports of product faults

Your client should also subscribe to the software vendor's newsgroup to remain informed on a timely basis of new versions or patches for the specific programs the client is using. If the vendor does not provide such a system, you should consider an alternative method of gathering and implementing this information.

Most of the patches and fixes to software are security-related. Failure to follow developments made with patches and fixes will make the system vulnerable. In addition, services not being used should be turned off so that you can consider services in use when maintaining and updating the systems. Therefore, these older services will have had time to have their weaknesses revealed and exploited.

The following table provides a listing of known server and CGI Script problems:

Software	Versions	Description
UNIX Web Server		
NCSA httpd	1.0–1.5a	Remote users can execute UNIX command with server privileges
Apache	1.0–1.1.1	Remote users can execute UNIX command with server privileges; remote users can obtain directory listings even when the feature is turned off
Windows NT Web Servers		
Netscape	1.0–1.12	Remote users can execute NT commands with server privileges
WebSite Server	1.0–1.1b	Remote users can execute NT commands with server privileges
Microsoft IIS	1.0	Remote users can execute NT commands with server privileges
Microsoft IIS	1.0–3.0	Remote users can obtain CGI script contents
CGI Scripts and Server Extensions		
Mindshare Out Box webdist.cgi	1.0–1.2	Remote users can execute NT commands with server privileges
Microsoft FrontPage Extensions	1.0–1.1	Unauthorized users can overwrite and/or append existing files. If server side includes turned on, users can execute commands with server's privileges
Selena Sol's Guestbook scripts	All versions	If server side includes turned on, users can execute commands with server privileges
nph-test.cgi	All versions	Remote users can obtain file listing from any directory on web server
nph-publish.cgi	1.0–1.1	Remote users can overwrite files outside document directory if web server permission permit
PHP extensions	Various versions	Remote users can execute commands with server privileges
AnyForm	1.0	Remote users can execute commands with server privileges
FormMail	1.0	Remote users can execute commands with server privileges
phf phone book	All Versions	Remote users can execute commands with server privileges

Server Logs

Logging

Log files are invaluable when recovering from a security-related incident. Logs can tell you how an attacker broke through your security system and even provide clues to the identity of the attacker. Log files can be submitted as evidence in a court of law for criminal or civil suits. Be warned, however, that one of the first things done after a successful break-in will be changing the log files to cover up the intrusion. For this reason, you may wish to set up secured log server either inside or outside your firewall.

The log server should be a system that offers no service to the network and does not support user accounts. Setting up the server in this manner helps avoid having people break into the log server after they have compromised other servers. You should have logging enabled for all of the servers on the system and be sure to examine the logs on a regular basis.

Note that on NT systems, all auditing is shut off by default. As a minimum, you should enable logs to catch bad login attempts and to watch the IP services you offer.

Log files have other, non-security-related uses. They can show:

- Utilization of external network connection
- Utilization of internal network
- CPU load of the servers
- Disk utilization

System Logs

UNIX/NT keeps a series of logs. Depending on the system used, they have various names and can be found in various locations. The usual locations include /var/log, /var/adm, /usr/adm. The standard system log allows for customization of what is and what is not recorded. Control over what is captured and stored in the systems configuration file, /etc/syslog.conf, is well-documented in the UNIX or NT manual.

Although the location of the log files varies, the format is similar from system to system. The following is a sample listing from a web server named "yoda."

```
March 8 16:25:20 yoda sshd[388] : Connection from bozo port 1022
March 8 16:25:23 yoda sshd[388] : Password authentication for r2d2 accepted
March 8 16:25:54 yoda su : r2d2 on /dev/ttyp1
.
.
.
March 9 03:30:56 yoda sshd[13615] : connect from vader port 1023
March 9 03:30:56 yoda sshd[13617] : executing remote command as root:  ps auxwww
March 9 03:30:58 yoda sshd[13619] : connect from vader port 1023
March 9 03:30:58 yoda sshd[13620] : executing remote command as root:  ps auxwww
March 9 04:30:08 yoda rdist[16307]  : c3po:  LOCAL ERROR:  Response time out
.
.
.
March 9 19:15:32 yoda in.telnetd[3212] : connect from 148.45.57.125
March 9 19:15:55 yoda login: 2 LOGIN FAILURES FROM h125n57.names.hal.com, quit
March 9 19:15:59 yoda login: 3 LOGIN FAILURES FROM h125n57.names.hal.com, end
March 9 19:16:02 yoda login: 4 LOGIN FAILURES FROM h125n57.names.hal.com, stop
March 9 19:16:10 yoda login: 5 LOGIN FAILURES FROM h125n57.names.hal.com, quit
March 9 19:16:15 yoda login: 5 LOGIN FAILURES FROM h125n57.names.hal.com, finish
March 9 19:16:29 yoda login: 6 LOGIN FAILURES FROM h125n57.names.hal.com, out
```

The first excerpt starts at 4:25 in the afternoon when a user named *r2d2* used the encrypted secure shell program to login to yoda from a machine named bozo. After logging in he used the *su* command to become root.

Because we know that r2d2 is an authorized system administrator and his workstation is named bozo, this information provides nothing to arouse suspicion. If r2d2 were to login on a machine outside the local network, a machine other than bozo, or if he were logging in outside his normal working hours, this would be cause for concern and additional analysis.

The next excerpt shows user *root* on a machine named *vader* logging in and trying to execute the command *ps auxwww* twice. This is expected—it is part of the automated purge and backup procedure that runs on *vader.*

At 4:30 AM, there is a time-out error message from the *rdist* program. This machine uses the *rdist* command to mirror its server logs to a backup server named c3po. After some inquiries, it was discovered that c3po was down due to hardware failure, so no additional investigation was required.

The final excerpt shows a more suspicious series of entries starting at 7:15 PM. The incoming telnet program that has been left running on this machine for emergency purposes (not a real good idea) reports a connection from IP address 148.45.57.125. Seconds later the log shows a series of login failures as the person connected tries a series of invalid user names. This could be evidence of a break-in attempt, but an analysis of the user names used (quit, end, stop) point more toward a neophyte who wandered into the system, started the telnet, and did not know what to do.

Best practices indicate the need to log everything and then run the entire log nightly through a script that will filter out expected patterns. After this is done, it is a good idea to examine what remains to follow up on unusual entries performed.

Because logs can be evidence of unauthorized access, intruders will often try to delete or remove unwanted entries. If an attacker has gained access to the root directory, there is no way to protect information, files, and other data stored on the local system. However, many versions of the *syslog* program allow for redirection of the log files to other servers. This makes it more difficult for attackers to gain access to log files.

Web Server Logs

Logs created by the server are also very helpful in detecting problems. Most servers create at least two logs—the access log and the error log. The access log provides the details, request by request, of all requests made to the server. Included within this log is the URL requested, host name of the requester, and the day and time of the request.

The error log, as the name implies, records errors—requests for documents that don't exist, attempted access to protected documents or CGI scripts that produce internal errors.

The following is an excerpt from an access log:

```
portio.wi.mit.edu - - [15/March/1999 : 22:46:58 –0500]  "GET /index.html
 HTTP/1.0" 200 1523
```

Each line in an access file represents a separate request for a URL. There are seven fields in each line—*host, rfc931, username, [date/time], request, status, bytes.*

1. **host:** The name or IP address of the user's machine. In our example protio.wi.mit.edu
2. **rfc931:** The user's login name on the local machine. This is provided by the "ident" command. This command runs on some UNIX machines, so the field is usually displayed as -.
3. **username:** For password-protected pages, this field holds the account name provided by the user. The field is – id not applicable.
4. **date/time:** The local time of access.
5. **request:** The URL requested, including any CGI script parameters if any.
6. **status:** The status code of the server's response – 200 for OK.
7. **bytes:** The number of bytes transferred, or – if not applicable.

The error log has a simpler format in which time-stamped error messages from the server, CGI scripts, and server plug-ins are recorded. A typical excerpt follows:

```
[Tue Feb 3 22:01:53 1998] httpd:  malformed header from script
ppmtogif:  computing colormap. . .
ppmtogif:  4 colors found
[Tue Feb 3 22:10:11 1998] httpd:  malformed header from script
g[Tue Feb 3 22:11:45 1998] killing CGI process 638
[Wed Feb 4 12:15:22 1998] httpd: connection times out for m1.abc.mil
Identifier  "main::q" used only once:  possible type at test line 1
Tie: no such file or directory
```

The error log grows at a much slower rate that the other logs, and its entries warrant analysis, if only to identify problems with the site. Some error messages that can be expected are:

- **"File does not exist" or "no multi in this directory."** These messages let you know that someone tried to access a nonexistent directory or URL. This message is usually the result of a broken link in one of the web documents or a user's typographical error. Sometimes it can indicate a URL-based attack if the message is occurring at a high rate.
- **"File permissions deny server access."** The server has tried to retrieve a document but did not have sufficient permissions to read. This problem could indicate that a document needs to have its permissions updated, or it could indicate that the server is misconfigured and that someone is using it to try to get at files outside the document tree.
- **"Passwords mismatch."** This error indicates that a user tried to access a document and entered the wrong password. Often, this is a user error, but a series of this type of error may indicate an attempt to break-in to the system.

- **"Client denied by server configuration."** Access to a directory was restricted to specific IP addresses, and someone outside the list of approved IP addresses has tried to gain access. A series of these errors may also indicate an attempt to gain unauthorized access.
- **"Malformed header from script."** This is a warning that CGI script is producing bad output that the server cannot interpret. These messages should be taken seriously because weak CGI scripts are often the first foothold an attacker has.

Like the strategy used with system logs, a good strategy to consider using with Web system logs should be to attempt to filter out the expected events and ones that are benign in nature. Make sure the procedure for filtering out and organizing logs makes sense and is applied on a consistent basis. Also check the frequency with which logs are filtered and analyzed. The following figure represents several of the commercial programs that are used to filter and organize web logs.

Program	Manufacturer	Operating System	Notes
Analog	Stephen Turner	NT/UNIX	Freeware
Wusage	Boutell Corporation	NT/UNIX	
Wwwstat	Roy Fielding	NT/UNIX	Freeware
Site Tracker	Tucker Info. Services	All OS	Subscription service
net.Analysis	net.Genesis	NT/UNIX	

Firewall Logs

Firewall logs provide an additional tool that allows you to monitor activity on the Internet and to detect possible break-ins. Ordinarily, the server should be fairly quiet with regard to network traffic. Connections between the LAN and the Internet servers should be limited to outgoing connections initiated by the company's employees. **If the server suddenly starts initiating its own connections to the firewall there is a potential problem.**

An early sign of an attack is the "door rattling" approach of scanning all ports on the firewall to find out which ones are active. Many firewall logs track this information, and because it is a good sign of potential problems, this feature should not be turned off. An example of port scanning might look like the following:

```
Mar 22 03:13:10 gw kernel:  tcp from www/192.44.187.62:1320 to gw/192.44.187.63 on unserverd port 19
Mar 22 03:13:12 gw kernel:  tcp from www/192.44.187.62:1321 to gw/192.44.187.63 on unserverd port 20
Mar 22 03:13:14 gw kernel:  tcp from www/192.44.187.62:1326 to gw/192.44.187.63 on unserverd port 21
Mar 22 03:13:20 gw kernel:  tcp from www/192.44.187.62:1327 to gw/192.44.187.63 on unserverd port 22
Mar 22 03:13:25 gw telnet-proxy: [1414]:  deny host=www/192.44.187.62 use of gateway
Mar 22 03:13:30 gw kernel:  tcp from www/192.44.187.62:1331 to gw/192.44.187.63 on unserverd port 24
```

In the following example, here is what might appear in the firewall logs if a compromised server makes repeated attempts to access the gateway's FTP server using guessed passwords (FTP is used in this example, however, SMTP, WWW, or any other service running on the server could be used).

```
Mar 22 04:04:33 gw ftpd  [2940] : failed login from www/192.44.187.62, guest
Mar 22 04:04:38 gw ftpd  [2949] : failed login from www/192.44.187.62, system
Mar 22 04:05:03 gw ftpd  [2957] : failed login from www/192.44.187.62, root
```

It is important to note that the activity to cause concern for your analysis is activity initiated by the Internet to the firewall.

A comprehensive discussion of a physical security and disaster recovery plan is beyond the scope of this publication. However, you should consider the following items related to physical security and recovery plans:

- Create a physical security plan—and make a physical inventory
- Make sure there is adequate protection against fire, smoke, explosions, dust, and humidity
- Protect against earthquake, storms, and other natural disasters
- Protect against lighting and electrical noise
- Provide adequate ventilation and humidity controls
- Restrict food and drink from mission-critical computers
- Restrict physical access to computers
- Physically secure computers so they cannot be stolen or vandalized—mark them with indelible inventory control markings

Protect the network cables from eavesdropping and destruction

Sample Security Policy

We include an example of an adequate company security policy for ABC Company in the following table.

ABC Company, Inc Security Policy
Current as of May 31, 19XX

PERSONNEL

Access Levels

The Web site grants five levels of access:

1. The public—read only access to all URLs with the exception of the /private directory where no access is granted
2. Employees of ABC company—ready only access to all areas of the site including access to the /private directory
3. HTML authors—ability to create, modify, and delete HTML files in the document tree
4. Site administrators—ability to modify the server configuration files, install CGI scripts, start and stop the server. Site administrators inherit all privileges of levels 1, 2, and 3.
5. System administrators—ability to modify the server host configuration, start and stop the host machine. System administrators inherit all privileges of all other levels.

Authorization Procedure

For access levels 3, 4 and 5, personnel must obtain written authorization from the CIO or CEO. This authorization will then be presented to a system administrator who will set up an appropriate account and access privileges. Level 2 access is automatically granted to all new employees when they are given a network password and email account.

Revocation Procedure

For access levels 2 through 5, authorization may be canceled at any time without warning at the discretion of the CIO or CEO. In the case of an emergency, a system administrator may also revoke access temporarily. This action must be ratified by the CIO or CEO within 24 hours.

ACCESS PRIVILEGES

Local Login

Local (console) login to the server host is allowed for system and site administrators only. Logins are for the purpose of site maintenance only.

Network Login

All forms of network login are prohibited—including file sharing.

Authoring Access

HTML authors and site administrator can make changes to the document tree. All such access is via FTP machines located within the company domain. These modifications shall be time/date stamped and logged. Except in rare emergencies, direct modifications to the document tree is not permitted, and a detailed exception report is due within 24 hours of the modification.

Remote Server Administration

Prohibited. ALL server administration is to be done locally.

Browsing Access

With the exception of the /private directory, anonymous browsing is allowed. The /private directory is restricted to systems in the company domain.

CGI Script Installation

CGI scripts can be installed by site administrators after two or more members of the site administrators group have reviewed and approved the code and tested it on the test server. CGI scripts that do not have code are not allowed on the server without written approval from the CIO or CEO.

Access to the /private Directory

The /private directory contains information that is confidential or proprietary to the ABC Company. Access to this directory is password protected and restricted to systems within the company domain (abc.com).

NETWORK SERVICES

Web

The Internet will serve static HTML documents and the output of CGI scripts. Incoming data is limited to customer feedback, order forms, and discussion groups whose scripts deposit their information in the appropriate and separate databases. Neither the CGI scripts nor the server shall initiate connections with other databases, files or other services on the LAN without authorization of the CIO.

FTP

Both incoming and outgoing FTP is allowed solely for the purpose of updating web pages. FTP access is restricted to HTML authors, site and system administrators. FTP access is restricted to machines located within the company domain. ALL anonymous FTP and access from outside the company domain is strictly prohibited.

Other Services

No other services (Gopher, Finger, etc.) are provided by the web host.

MAINTENANCE

24 × 7 Operation

The site will be accessible 24 x 7, except for a one-hour maintenance period on the first Sunday of each month between 8 AM and 9 AM. The UPS and other backup equipment should be tested monthly during this maintenance interval.

Backups

A complete backup of the server will be done daily. The company will maintain 14 generations of backup tapes off-site in a secure facility.

Software

A site administrator is responsible for maintaining all software at current release levels with the appropriate patch installed. Virus-scanning software should be checked and updated weekly if appropriate.

Monitoring

A system administrator is responsible for monitoring the server host logs for errors and other unusual activity. A site administrator has similar responsibilities for web server logs. Both COPS and SATAN program shall be run weekly and the results studied. ANY suspicious activity should be brought to the attention of the CIO immediately. If there is any reason to suspect that the integrity of the system has been compromised, a system or site administrator is authorized to immediately take the server off-line.

File Access Rights Summary

User	Configuration	Tools	Logs	CGI	Documents
System Administrator	RW	R	R	RW	RW
Site Administrator	R	R	R	RW	RW
HTML Author	—	—	—	R	RW
Users	—	—	—	R	R
R=Read access; W=Write access					

Minimizing Risk by Minimizing Services

An important way to reduce the risks the web server is exposed to is to minimize the other services offered by the computer that acts as host for the web site. The table below outlines these other computer services and the reasons they should be eliminated or restricted:

Service to Eliminate/Restrict	Explanation
Berkeley "r" commands (rlogin, rsh, rdist, etc.)	These commands use IP addresses for authentication and should be disabled. The only exception to this is if you use a version of these commands that are based on SSL.
Chargen, echo	These services are typically used to launch data-driven or denial-of-service attacks.
Domain Name System (DNS)	Weaknesses in DNS implementations can be used to compromise the web server. DNS should be run on its own secure server.
Finger	Finger can be used to gather information about another computer system. Information gathered can allow an attacker access to launch programs, copy/delete files, etc.
FTP	Standard FTP sends user names and passwords in an unencrypted format. If FTP is required another control should be used e.g., one-time passwords, SecureID keys. FTP should only be used to update the web server. If anonymous FTP is required it should be run on a separate computer
Mail (SMTP)	Inherent weaknesses in sendmail and other mailers can be used to break into another system.
Netstat, systat	Netstat and systat have the ability to display a system's configuration and usage patterns. From this information an attacker can gain access to the server.
Telnet	Interactive logins should be prohibited to anyone except the webmaster. Telnet should only be used in its encrypted form (ssh). If this is not possible use another control like one-time passwords. Telnet allows access to the root directory.

System Security Clues

Hackers prey on the weaknesses of specific software and operating systems. As a result, the indications that a site's security has been breached are similar. The following list represents areas to examine when testing the security of a site:

- **Examine log files for connections from unusual locations or other unusual activity.**

  For example, look at the 'last' log, process accounting, all logs created by syslog, and other security logs. If the firewall or router writes logs to a different location than the compromised system, remember to check these logs also. Note that this is not foolproof unless you log to append-only media; many intruders edit log files in an attempt to hide their activity.

- **Look for setuid and setgid files (especially setuid root files) everywhere on the system.**

  Intruders often leave setuid copies of /bin/sh or /bin/time around to allow them root access at a later time. The UNIX find(1) program can be used to hunt for setuid and/or setgid files.

- **Check your system binaries to make sure that they haven't been altered.**

  Intruders have changed programs on UNIX systems such as login, su, telnet, netstat, ifconfig, ls, find, du, df, libc, sync, any binaries referenced in /etc/inetd.conf, and other critical network and system programs and shared object libraries. Compare the versions on the system(s) with known good copies, such as those from the initial installation media. Be careful of trusting backups—backups could also contain Trojan Horses. Trojan Horse programs may produce the same standard checksum and timestamp as the legitimate version. Consequently, the standard UNIX sum(1) command and the timestamps associated with the programs are not sufficient to determine whether the programs have been replaced. The use of cmp(1), MD5, Tripwire, and other cryptographic checksum tools is sufficient to detect these Trojan Horse programs, provided the checksum tools themselves are kept secure and are not available for modification by the intruder. Additionally, you may want to consider using a tool (PGP, for example) to "sign," or fingerprint, the output generated by MD5 or Tripwire for future reference. Use fingerprints to compare binaries and other system files. The fingerprint produces a hash of the file. A single-bit change in the file produces a completely different hash. There is no way currently known to discover a file that produces a particular hash—making file forgery virtually impossible.

- **Check the system(s) for unauthorized use of a network-monitoring program, commonly called a sniffer or packet sniffer.**

  Intruders may use a sniffer to capture user account and password information.

- **Examine all the files that are run by 'cron' and 'at.'**

  Intruders have been known to leave back doors in files run from 'cron' or submitted to 'at.' These techniques can let an intruder back on the system (even if you believe you had addressed the original compromise). Also, verify that all files/ programs referenced (directly or indirectly) by the 'cron' and 'at' jobs, and the job files themselves, are not world-writable.

- **Check for unauthorized services. Inspect /etc/inetd.conf for unauthorized additions or changes.**

  In particular, search for entries that execute a shell program (for example, /bin/sh or /bin/csh), and check all programs that are specified in /etc/inetd.conf to verify that they are correct and haven't been replaced by Trojan horse programs. Also check for legitimate services that have commented out in the /etc/inetd.conf. Intruders may turn on a service that was previously turned off, or replace the inetd program with a Trojan Horse program.

- **Examine the /etc/passwd file on the system and check for modifications to that file.**

  In particular, look for the unauthorized creation of new accounts, accounts with no passwords, or UID changes (especially UID 0) to existing accounts.

- **Check your system and network configuration files for unauthorized entries.**

  In particular, look for '+' (plus sign) entries and inappropriate non-local host names in /etc/hosts.equiv, /etc/hosts.lpd, and in all .rhosts files (especially root, uucp, ftp, and other system accounts) on the system. These files should not be world-writable. Furthermore, confirm that these files existed before any intrusion and were not created by the intruder.

- **Look everywhere on the system for unusual or hidden files (files that start with a period and are normally not shown by 'ls')**

  These files can be used to hide tools and information (password cracking programs, password files from other systems, etc.). A common technique on UNIX systems is to put a hidden directory in a user's account with an unusual name, something like '...' or '.. '(dot dot space) or '..^G' (dot dot control-G). Again, the find(1) program can be used to look for hidden files, for example: find /-name ".. " -print -xdev find /-name ".*" -print -xdev | cat -v. Also, files with names such as '.xx' and '.mail' have been used (that is, files that might appear to be normal).

- **Examine all machines on the local network when searching for signs of intrusion.**

  Most of the time, if one host has been compromised, others on the network have been, too. This is especially true for networks where NIS is running or where hosts trust each other through the use of .rhosts files and/or /etc/hosts.equiv files. Also, check hosts for which your users share .rhosts access.

Network Monitoring Tools

Practitioners might benefit from acquiring the following monitoring tools to help the practitioner in a WebTrust engagement. Many of these tools will be running on the system(s) used by the client in the client's eCommerce system.

- Argus

Argus is a network-monitoring tool that uses a client-server model to capture data and associate it into "transactions." The tool provides network-level auditing and can verify compliance to a router configuration file. It allows information to be easily adapted to protocol analysis, intrusion detection, and other security needs. Argus is available from many sites, including ftp://ftp.sei.cmu.edu/pub/

- Swatch

Swatch, the Simple WATCHer program, is an easily configurable log file filter/monitor. Swatch monitors log files and act to filter out unwanted data and take one or more user-specified actions based on patterns in the log. Swatch is available from ftp://ftp.stanford.edu/general/security-tools/swatch/.

- Crack

Crack is a freely available program designed to identify, by standard guessing techniques, UNIX DES encrypted passwords that can be found in widely available dictionaries. The guessing techniques are outlined in the Crack documentation. Many system administrators run Crack as a regular system administration procedure and notify account owners who have "crackable" passwords. Crack is available from ftp://info.cert.org/pub/tools/crack/.

- Shadow passwords

If your UNIX system has a shadow password capability, use it. Under a shadow password system, the /etc/passwd file does not have encrypted passwords in the password field. Instead, the encrypted passwords are held in a shadow file that is not word-readable. Consult the system manuals to determine whether a shadow password capability is available on your system and to get details of how to set up and manage it.

- TCP/IP wrapper program

The TCP/IP wrapper program provides additional network logging information and gives a system administrator the ability to deny or allow access from certain systems or domains to the host on which the program is installed. Installation of this software does not require any modification to existing network software. This program is available from ftp://info.cert.org/pub/tools/tcp_wrappers/.

- ISS (Internet Security Scanner)

ISS is a program that will interrogate all computers within a specified IP address range, determining the security posture of each with respect to several common system vulnerabilities. ISS is available from many sites, including http://www.iss.net/~iss/.

- SATAN (Security Administrator Tool for Analyzing Networks)

SATAN is a testing and reporting tool that collects a variety of information about networked hosts. SATAN is available from many sites, including ftp://ftp.win.tue.nl/pub/security/.

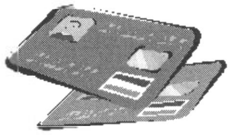
- COPS (Computer Oracle and Password System)

COPS is a publicly available collection of programs that attempt to identify security problems in a UNIX system. COPS does not attempt to correct any discrepancies found; it simply produces a report of its findings. COPS is available from ftp://info.cert.org/pub/tools/cops/.

- Tripwire

Tripwire checks file and directory integrity; it is a utility that compares a designated set of files and directories to information stored in a previously generated database. Any differences are flagged and logged, including added or deleted entries. When run against system files on a regular basis, Tripwire enables you to spot changes in critical system files and to immediately take appropriate damage control measures. Tripwire is available from many sites, including ftp://info.cert.org/pub/tools/tripwire/.

Evaluating a Credit Card Payment System



There are a number of credit card systems available for use on the Internet. Any cards listed here would be out of date by the time this book was published. So, rather than listing systems and other sources, we provide the following list of criteria to consider in making an analysis of an Internet payment system:

- If the system stores credit card numbers and other information on the customer's computer (usually by using cookies), the information must be encrypted.
- If the system stores credit card numbers and other information on the web server, this information must be encrypted. Credit card and other information should be stored off the web server for optimal security and credit card information should only be stored if recurring charges are expected.
- Unless recurring charges are anticipated, all credit card information should be purged at the end of the transaction.
- The system should validate the credit card information from the on-line merchant bank or by using the check-digit test while the customer is still on-line.
- The system should allow for credits to be posted from time to time. Check on the process to allow the posting of credits. Does there need to be a matching charge, special password, or other access restriction? Are there exception reports for the processing of credits? Issuing credits to a credit card is one of the easiest ways to steal money from a business.
- The system should allow for customer charge-backs. Does the charge-back automatically get entered into the customer's account, or is the process handled manually?

Web Privacy

A recent *Business Week*/Harris poll confirms that Americans care deeply about their privacy and that their concerns about the lack of privacy on-line are keeping many would-be-users off the Internet. The poll, published in the March 16, 1999 issue of *Business Week*, reveals that almost two-thirds of non-Internet users would be more likely to start using the Internet if the privacy of their "personal information and communications would be protected." Privacy was the number one reason individuals are choosing to stay off the Internet, coming in well ahead of cost, concerns with complicated technology, and concerns with unsolicited commercial email.

There is a rising tide of concern about privacy on the Internet, as we've mentioned previously. The extent of this concern is evident when examining other results showing that more than half the respondents believe government should regulate the use and collection of personal information on the Internet and that 65% are "very" and 15% "somewhat" concerned about using a credit card to make an on-line purchase. This concern has components of security as well as privacy.

A recent article in the *Los Angeles Times* noted that the State of California plans to sell information from quarterly and annual payroll reports to banks and other agencies. Much of this information is provided to the California Employment Development Division (EDD) electronically. It is anticipated that banks will use this information in evaluating loan worthiness. The EDD stated that the consumer will have to provide permission before the bank can obtain this information. Within a matter of days after this story appeared, the law was removed due to strong public outcry, underscoring the value the public places on privacy.

In October of 1998, the European Union (EU) adopted privacy standards for companies doing business with member countries. The FTC has adopted safe harbor provisions that are an attempt to meet the European regulations. At the time this work will be going to press, it is unclear whether the safe harbor provisions will be adopted.

WebTrust has had elements of privacy since its inception. However, in future releases of the Principles and Criteria, privacy standards will be focused and refined. The greatest risk to privacy is information that is voluntarily provided to a web site. User feedback forms, requests for additional information, on-line orders, and posts to news groups may be stored for an indefinite period of time and used as the site desires.

On the other side of the coin, however, researchers, advertisers, and Web sites use customer information to tailor site content, provide better products and improve the overall browsing experience. So the challenge becomes one of balance. Time, technology, and perhaps, government regulation will provide solutions and additional problems to the privacy conflict.

Server Logs and Privacy

Much of the information that is captured during a web session is recorded in the log files of the server. To understand just how much information is gathered on-line, we provide the following log excerpt from a server's log over a two-minute period:

```
ppp.byu.edu - - [09/May /1999:20:31:56  -0500] “GET / HTTP/1.0” 200 4029
ppp.byu.edu - - [09/May /1999:20:31:58  -0500] “GET /www/lcalogo.gif HTTP/1.0” 200 620
ppp.byu.edu - - [09/May /1999:20:32:10  -0500] “GET /www/wt.gif HTTP/1.0” 200 154
ppp.byu.edu - - [09/May /1999:20:33:22  -0500] “GET /cgi-bin/wwwais?webtrust+privacy HTTP/1.0” 200 527
```

Each line contains information about a separate request or hit. In the previous example, four requests came from a user at ppp.byu.edu. In the first line, the user requests the home page by downloading the "/" URL. This page contains two graphics, lcalogo.gif and wt.gif. The next two lines in the example show the request for these graphics files. In the last line, the user performs a search using the words webtrust and privacy.

What else can we learn from these four lines in the log file? More than you might think. For example, the user is probably someone who works for Brigham Young University and is probably working from home. We can deduce this because it is 8:30 PM and because the remote address indicated the use of one of the university's PPP lines.

Information that is recorded on server log files can be customized. In addition to the information contained in the example above, server logs can record:

- The URL of the referring document, showing the page the user was viewing before requesting the current page
- The browser's manufacturer and version number
- The user's operating system
- The amount of time taken to process a request
- The list of MIME types that the browser supports that can reveal which "plug-ins" are installed

Other Logs

Other information available to the website comes from various sources. One such source is a referrer log. The referrer log maintains information similar to that the server log contains, but reveals where the user came from before browsing the current web site. For example, if a user had come to our site from link at CPAWEBTRUST.ORG we might see the following entry in our server's referrer log:

```
User1.abc.com http://www.cpawebtrust.org/map.html  -> / lca.html
```

In this example, a user (user1) at abc.com visits cpawebtrust.org. On that page is a link from the map.html page to our home page. This information is one way marketing professionals measure the success of their efforts.

A **bookmark referral** looks like the following:

```
gate.swm.de http://ws084242.swm.de/~brudder/bookmarks.html  ->
```

This entry shows that someone behind a firewall in a German company (de denotes Germany) named Brudder has a link to my homepage in his bookmark file.

This **search engine referral** shows that a user whose IP address is not listed in the domain name system has used the Lycos Web search engine to search for documents containing the words webtrust, cookies, and privacy.

```
200.10.239.68 http://www.lycos.com/search.gw?
search=webtrust+cookies+privacy&collection=web ->
/why-webtrust.html
```

He located the Why WebTrust html—a good choice.

Because of the potential for the referrer field to "leak" information from one web site to another, referrer logs can lead to some serious privacy issues. A recent case involved the leakage of credit card numbers. The problem occurred in the following manner:

1. The user browsed a web site and decided to make a purchase
2. The user entered the credit card number into the on-line form and submitted it after confirming that the site has SSL running
3. The user received a confirmation of the order
4. The confirmation page contained an advertisement that pointed to another site
5. The user clicked on the advertisement and jumped to the new site
6. The following information showed up in the referrer logs of the NEW site

```
Pressrm.dp.com http://www.merchant.com/cgi-bin/order?name=Clark+Kent&
address=Daily+Planet, Anywhere+City&item=digital+altimeter&
quantity=1&credit+card=1838302412811338-> /index.html
```

How could something like that happen when SSL was running at the merchant's site? The problem can be found in the scripting of the form the customer filled out. The designers of the site used the GET rather that the POST command for submitting the contents to the CGI script that handles the form. This situation illustrates why it is extremely important to evaluate the impact CFI scripts have on the engagement.

In another scenario, consider this entry that was occurring with frequency in the log file of a small company whose stock was falling in value:

```
dg7231.mcig.com file\\SRVR1\HOT\stocks2sellshort.html -> /index.html
```

This entry indicates that a document named stocks2sellshort.html located on the company's internal server at the MCIG company has a link to the company's homepage on the Internet. The presence of a firewall system would be entirely ineffective at preventing this information leak unless it was specifically configured to strip out the referrer field from outgoing web requests.

Web proxies are modified web servers that act as middlemen between the user and the remote server. When a proxy is in use, all requests for documents are indirect. Proxies are used to reduce network traffic and in many instances make use of caching for quicker speed. Proxies are a requirement for many firewall systems.

Proxies maintain logs called, **proxy logs** (no surprise here). Proxies are generally transparent to the user and web access occurs normally. Because a proxy server acts as a middleman by definition, the proxy server logs everything.

Every URL, along with user identification, time and date, and referrer information is logged. The implication of this structure is that the proxy log from a corporate firewall can be used to determine who is surfing non-business-related sites on company time. Internet Service Providers can compile detailed statistics on their customers' habits and associate them to specific sites, thus compromising privacy.

Cookies

Cookies were designed with the best of intentions to solve the problem of providing dynamic content in a static HTTP environment. Cookies come in all sizes and shapes—that is they can contain a large amount of information or little information. For example, cookies can contain the entire contents of a shopping cart or simply the identity of a repeat visitor to a specific site.

Cookies have two basic forms. Cookies that disappear when the browser session is terminated are called "transient." Cookies that remain and are stored on the hard drive of the user are called "persistent." Cookies also have names, and a server can hand a single browser several cookies, each with a different name to track. Some cookies are restricted to certain parts of a site's document tree, or they can be made to act only in an SSL session.

The cookie protocol was designed to prevent leakage of information from one site to another in two basic ways: (1) the ability to designate secure cookies for SSL sessions, and (2) the fundamental inability to share cookies among sites. Although a web site can create cookies that are valid on more than one server within its own domain (www.abc.com and ftp.abc.com), it is currently impossible to make a browser return a cookie to a foreign domain.

In addition, because a cookie is generated by the web server and not the browser, a cookie cannot hold information that the user has not voluntarily provided to the site. For example, a cookie cannot hold an email address unless the user supplied the email address to the site.

WebTrust Marketing Tips

CHAPTER FOUR

WebTrust Marketing Tips

Make Marketing Work

Up until now, this guide has been concerned with the specific tasks in performing a WebTrust engagement. Perhaps the greatest challenge the practitioner will find is in marketing and selling a WebTrust engagement to potential and current clients. So, although we may know all of the ins and outs of performing an engagement, if we don't have an engagement to perform, that skill is moot. For this reason, it is important to address the unique attributes and challenges in marketing a WebTrust engagement.

Many practitioners are constantly ask how to market the WebTrust service to clients and potential clients. My answer is always the same—one prospect at a time. Accountants are sometimes considered to be lacking in marketing skills and to have entered the accounting profession because it historically did not require the disposition it takes to become a salesperson. Those days are gone. The accounting profession needs to be more responsive to consumer needs, wants, and concerns if it is to survive into the next century. Here are some of the most common objections offered by potential WebTrust clients and corresponding suggested answers for each:

Comment: This is a great program, but I can't afford it right now.

Response: You can't afford not to! Then ascertain how important the Internet is to the company's overall sales program. If the Internet is critical, review the data about growth of electronic commerce and then tell the prospect that it is important to find a way to come up with the needed funds. Follow this by a review of the budget.

Comment: Consumers are saying that a seal really won't make a difference.

Response: Then the studies done by various consumer groups are wrong. Return to studies such as the Yankolovich study and review the actual facts.

Comment: If the AICPA doesn't advertise this program to the consumer, it will never take off.

Response: The AICPA is targeting both the developer and consumer groups. Then, try to refocus the topic to the real problem, that of the CPA not wanting to sell the service

Comment: What about all the other competition out there?

Response: Yes, there is competition, but no other program is as full-featured as WebTrust—covering ALL aspects of consumer concerns: business disclosures, transaction integrity, and information protection. Other programs cover a single principle or part of a principle. None has the independence or objectivity of a CPA. (See the competitive grid presented in Appendix F which reflects the various seal programs in existence at the time this guide goes to press. It is interesting to note that competitors' programs offer only some of the features that WebTrust provides.)

Comment: This program is for larger companies with Internet sites.

Response: Smaller companies have a lot of credibility to gain from the consumer. Again, refocus the objection to the fact that consumers are looking for a measure of security on the Internet that WebTrust offers.

Comment: There are so few seals on the web, we don't want to be first.

Response: You're right, there are not a lot of WebTrust seals on the Internet yet, because the program is so new. This gives you an opportunity to be a leader and set the standard for your competition.

The tactic the accountant needs to take is one of listening to the objection from the client and then refocusing the discussion back to the benefits of WebTrust and eCommerce. Consider the following benefits:

- Reduced sales costs
- Increased sales at the eCommerce site
- Increased consumer confidence
- Larger global customer base
- Perceived as a leader

Understand that WebTrust is not about accounting. Rather, WebTrust is about consumer confidence on the World Wide Web. The last person to market a WebTrust engagement to is the controller or CFO whose budget is exhausted and just got the audit bill from your firm WebTrust and its concepts are better understood by the sales and marketing departments whose job it is to reach the consumer and build confidence. This situation poses two problems:

- Accountants often don't have any contact with the sales or marketing departments of their clients because historically they have worked with the accounting department.
- Sales and marketing people get "pitched" to on a regular basis. A one-time sales pitch on the part of the accountant is not likely to get you a new engagement. On the average, it will take 3–5 sales calls to the same prospect to win an engagement.

Accountant's attitudes must change to realize that it will take effort on our part to launch this service. Neither the AICPA nor state organizations have the resources required to put forth a marketing campaign like Microsoft or IBM Accountants, however, have a national "sales force" of over 300,000 members. We also have materials provided by the AICPA to help market this vital service. And, who knows, as accountants become better at selling WebTrust engagements, they may find it easier to sell other services as well.

Favorite Websites

See Appendix D for selected Websites that might be helpful in your WebTrust engagements.

WebTrust Presentation on Microsoft Power Point

Included with this book as Appendix E is a copy of information to consider if you want to develop a Microsoft Power Point presentation for WebTrust. The information includes a review of the explosive growth of eCommerce and an introduction to the WebTrust Principles and Criteria. Feel free to adapt the information to meet the particular needs of your firm and the audience. Be sure to look at the notes which provide additional information or discussion points to consider.

Seal Programs

Various competitors offer seal programs that address some of the features that the WebTrust Seal Program includes. See Appendix F, which includes a copy of the Seal Program Comparison grid, indicating the competitive and technical differences between WebTrust and other seal programs.

Conclusion

eCommerce represents one of the most exciting opportunities and adventures for both clients and accountants. As our clients look for newer more efficient ways to reach their customers, accountants should be leading the way with electronic commerce. Forrester Research stated: "The rapid growth of inter-company electronic commerce will cause businesses to adopt dynamic trading processes—July 1997."

As information and accounting professionals, we should be leading the way in educating our clients as to the benefits of electronic commerce. In many cases, we will need to assist them in taking advantage of the opportunities eCommerce provides. Yes, there will be risks, but there will also be opportunity and reward. Consider these points taken from great leaders in our history:

> Opportunity is missed by most people because it is dressed in overalls and looks like work. —Thomas A. Edison
>
> Security is mostly a superstition. It does not exist in nature...life is either a daring adventure or nothing. —Helen Keller
>
> Nothing is particularly hard, if you divide it into small jobs. —Henry Ford
>
> He who waits for a roast duck to fly into his mouth must wait a very, very long time. —Chinese Proverb

It is my sincere wish that we all look ahead with great excitement to the opportunities and challenges offered by electronic commerce and WebTrust. The wave of technology is before our clients and us. Now it our choice—to either ride the wave of technology into the 21st century or be buried by it.

Appendices

APPENDIX A

Internet Dictionary and Common Internet File Formats

INTERNET DICTIONARY

Address

See either **IP Address** or **Email Address**.

Address Mask

The address mask is used to identify the parts of an **IP address** that correspond to the different sections (separated by dots). It's also known as the "subnet mask" because the network portion of an address can be determined by the encoding inherent in an IP address.

Advanced Research Projects Agency Network (ARPANET)

A pioneering long-haul network funded by what's now-called DARPA (formerly known as ARPA). It was the foundation on which the **Internet** was built.

Agent

The part of a system that performs information preparation and exchange on behalf of an application.

Alias

A type of nickname (usually short and easy to remember) that refers to a type of network resource. Aliases are used so you won't have to remember the long and difficult names typical of network resources.

Anonymous FTP

By using the word "anonymous" as your user ID and your email address as the password when you login to an **FTP** site, you can bypass local security checks and gain limited access to public files on the remote computer. This type of access is available on most FTP sites, but not all.

Applet

A small *Java* program that can be embedded in an *HTML* page. Applets differ from full-fledged Java applications in that they are not allowed to access certain resources on the local computer, such as files and serial devices (modems, printers, etc.), and are prohibited from communicating with most other computers across a network. The current rule is that an applet can only make an Internet connection to the computer from which the applet was sent.

See **HTML** and **Java**.

Application

Sometimes known as a **client** or an "app" it's a program that performs a specific function. FTP, Mail, Gopher, Mosaic, and Telnet clients are the most common examples of Internet applications.

Archie

You'll usually hear this term referred to in the phrase archie search. Archie is a way of automatically gathering, indexing, and sometimes even retrieving files on the Internet. Most good archie clients are able to **FTP** files once you've found the information you're looking for.

Archive

A collection of files stored on an Internet machine. **FTP** sites are known as archives.

ARPANET

See **Advanced Research Projects Agency Network**.

Asynchronous Transfer Mode

A transfer method that dynamically allocates bandwidth using a fixed-size **packet**, or cell. Also known as fast packet.

ATM

See **Asynchronous Transfer Mode**.

Authentication

Any process that ensures that users are who they say they are. When you type your name and password, you are authenticated and allowed access.

Bandwidth

This refers to the difference (measured in Hz) between the highest and lowest frequencies of a transmission. Most people loosely refer to bandwidth as the amount of data that can be transferred over a network connection.

BBS

See **Bulletin Board System**.

Berkeley Internet Name Domain

An early version of a **DNS** server developed by the University of California at Berkeley. Most Internet hosts run a version of BIND.

Bitnet

A computer network devoted to academic use that provides **email** and file transfer services using a store-and-forward **protocol**. It is based on the IBM Network Job Entry protocols. A more recent version of Bitnet (known as Bitnet-II) encapsulates the Bitnet protocol within IP packets.

Bounce

If you send **email** and it fails to arrive at its intended recipient for any reason (incorrect user name, network failure, etc.), the message "bounces" and returns to you. The subject line in a bounced message usually says something like: **Undeliverable Mail** or **Message Undeliverable.**

BTW

Acronym meaning **By The Way.** Seen mostly in **IRC** sessions.

Bulletin Board System

A computer that typically provides **email** services, file **archives**, and announcements of interest to the bulletin board system's operator (known as a sysop). BBS's started out as hobbies for computer enthusiasts, and were mostly accessible by modem. Recently, however, more and more BBS's are being connected to the **Internet**.

CCIRN

See **Coordinating Committee for Intercontinental Research Networks**.

CCITR

See **Comite Consultatif International de Telegraphique et Telephonique**.

CERT

See **Computer Emergency Response Team**.

CGI

(Common Gateway Interface)—A set of rules that describe how a *Web Server* communicates with another piece of software on the same machine, and how the other piece of software (the "CGI program") talks to the web server. Any piece of software can be a CGI program if it handles input and output according to the CGI standard.

Usually a CGI program is a small program that takes data from a web server and does something with it, like putting the content of a form into an email message, or turning the data into a database query.

You can often see that a CGI program is being used by seeing "cgi-bin" in a URL, but not always.

See **cgi-bin**.

cgi-bin

The most common name of a directory on a web server in which **CGI** programs are stored. The "bin" part of "cgi-bin" is a shorthand version of "binary," because once upon a time, most programs were referred to as "binaries." In real life, most programs found in cgi-bin directories are text files—scripts that are executed by binaries located elsewhere on the same machine.

See **CGI.**

Challenge-Handshake Authentication Protocol (CHAP)

An **authentication** method that can be used when connecting to an **Internet Service Provider**. CHAP allows you to login to your provider automatically, without the need for a terminal screen. It is more secure than the **Password Authentication Protocol** (another widely used authentication method), because it does not send passwords in text format.

CHAP

See **Challenge-Handshake Authentication Protocol**.

Chat

Another term for **IRC**. Also, an acronym meaning **Conversational Hypertext Access Technology.**

CIX

An acronym meaning **Commercial Internet Exchange.**

Client

In **Internet** terms, it is an application that performs a specific function, such as **Telnet** or **FTP**. It's the **front-end** to an Internet process. In more general terms, a client is the computer system or process that requests a service of another computer system or process. The much talked about **client-server architecture** refers to a workstation requesting the contents of a file from a **server**.

Comité Consultatif International de Telegraphique et Telephonique (CCITT)

French for **International Telephone and Telegraph Advisory Council**—an organization that plays a major role in the United National International Telecommunications Union (ITU). The CCITT is responsible for making technical recommendations about communications systems worldwide. Every four years, CCITT updates the standards, most recently in 1996.

Computer Emergency Response Team (CERT)

The CERT was formed by DARPA in November 1988 in response to the Internet worm incident. CERT exists to facilitate **Internet**-wide response to computer security events involving Internet **hosts** and to conduct research targeted at improving the security of existing systems. They maintain an **archive** of security-related issues on their **FTP** server at **ftp.cert.org**, their **email** address is **cert@cert.org**, and their 24-hour telephone Hotline for reporting Internet security issues is (412) 268-7090.

Cookie

The most common meaning of "Cookie" on the Internet refers to a piece of information sent by a Web *Server* to a Web *Browser* that the Browser software is expected to save and to send back to the Server whenever the browser makes additional requests from the Server.

Depending on the type of Cookie used, and the Browser's settings, the Browser may accept or not accept the Cookie, and may save the Cookie for either a short time or a long time.

Cookies might contain information such as login or registration information, online "shopping cart" information, user preferences, etc.

When a Server receives a request from a Browser that includes a Cookie, the Server is able to use the information stored in the Cookie. For example, the Server might customize what is sent back to the user, or keep a log of particular user's requests.

Cookies are usually set to expire after a predetermined amount of time and are usually saved in memory until the Browser software is closed down, at which time they may be saved to disk if their "expire time" has not been reached.

Cookies **do not** read your hard drive and send your life story to the CIA, but they can be used to gather more information about a user than would be possible without them.

Coordinating Committee for Intercontinental Research Networks (CCIRN)

A committee that provides a forum for North American and European network research organizations to cooperate and plan.

Corporation for Research and Educational Networking (CREN)

An organization formed in October 1989, when **Bitnet** and CSNET were combined. CSNET is no longer around, but CREN still operates Bitnet.

Cracker

Substantially different from **hackers**, crackers are users who try to gain illegal access to computers. They are usually malicious in their intentions.

Cyberspace

The **world of computers and the society that gathers around them**, as referred to by William Gibson in his fantasy novel *Neuromancer*. It now loosely refers to the online world and even more loosely to the **Internet**.

Data Encryption Key (DEK)

Much like an actual key used for locking and re-opening doors, DEKs are used for the encryption and decoding of message text, sometimes in the form of a digital signature.

Data Encryption Standard (DES)

A standardized encryption method widely used on the **Internet**.

Datagram

A block of data that is "smart" enough (actually, which carries enough information) to travel from one **Internet** site to another without having to rely on earlier exchanges between the source and destination computers (not to be confused with a Candygram).

DDN

See **Defense Data Network**.

DECnet

The proprietary network **protocol** designed by Digital Equipment Corporation.

Dedicated Line

A communications line that is used solely for computer connections. If you buy an additional phone line for your modem, that's a dedicated line. There are other types of dedicated lines (such as **T3**s and **T1**s) that are used for larger network entities.

Defense Data Network (DDN)

A global communications network that serves the U.S. Department of Defense. It is made up of a network called MILNET, other portions of the **Internet**, and classified networks that are not part of the Internet. The DDN is used to connect military installations and is managed by the Defense Information Systems Agency. It was originally developed by DARPA.

Dialup

A widely used method of accessing the **Internet**. A dialup connection uses regular phone lines to connect one computer to another via modem.

Distributed Computing Environment (DCE)

An architecture based on standard programming interfaces, conventions, and server functionalities used for distributing applications transparently across networks. The DCE is controlled and promoted by the Open Software Foundation (OSF), a consortium of vendors including DEC, IBM, and Hewlett Packard.

DNS

See **Domain Name Service**.

Domain

A "logical" region of the **Internet**. People sometimes refer to them loosely as "sites." Generally, a domain corresponds to an **IP address** or an area on a **host**.

Domain Name Service (DNS)

The DNS is a static, hierarchical name service used with **TCP/IP** hosts, and is housed on a number of servers on the **Internet**. Basically, it maintains a database for figuring out and finding (or resolving) host names and **IP addresses** on the Internet. This allows users to specify remote computers by **host** names rather than numerical IP addresses (if you've used UNIX, you may have heard the DNS referred to as the BSD UNIX BIND service). For example, go to a DOS prompt in Windows 95, the % prompt in UNIX, or use a ping client for Windows 3.1 or Mac, and type **ping** **www.winfiles.com**. This will check the DNS server you have configured, look up the numerical IP address for **www.winfiles.com**, and then ping that server's IP address. The advantage of the DNS is that you don't have to remember numerical IP addresses for all the Internet sites you want to access.

Dot Address (or Dotted Decimal Notation)

The common notation for **IP addresses** of the form 1.2.3.4, where each number represents one byte in the four-byte IP address.

Electronic Frontier Foundation (EFF)

A foundation that addresses social and legal issues arising from the impact of computers on society.

Electronic Mail (Email)

A method by which computer users can exchange messages with each other over a network. Email is probably the most widely used communications tool on the **Internet**. There are many quirky conventions to Email, but most entail a **To:**, **From:**, and **Subject:** line. One of the advantages of email is its ability to be forwarded and replied to easily. If an email is badly received by a group or user, the sender is likely to get **flamed**.

Email

See **Electronic Mail**.

Email Address

Your **email** address is made up of several parts. By convention, addresses use lowercase letters with no spaces. The first part of the address, the username, identifies a unique user on a **server**. The **@** (pronounced **at**) separates the **username** from the **host** name. The host name uniquely identifies the server computer and is the last part of the **Internet** email address. Large servers, such as those used at universities or large companies sometimes contain multiple parts, called subdomains. Subdomains and the host name are separated by a **period** (but it's pronounced **dot**). The three-letter suffix in the host name identifies the kind of organization operating the server (some locations use a two-letter geographical suffix). The most common suffixes are: **.com** (commercial), **.edu** (educational), **.gov** (government), **.mil** (military), **.net** (networking), and **.org** (non-commercial). More suffixes are under consideration. Addresses outside of the U.S. sometimes use a two-letter suffix that identifies the country in which the server is located. Some examples are: **.jp** (Japan), **.nl** (The Netherlands), **.uk** (United Kingdom), **.ca** (Canada), and **.tw** (Taiwan).

Encryption

The basis of network security. Encryption encodes network packets to prevent anyone except the intended recipient from accessing the data.

Ethernet

A standard and probably the most popular connection type for **Local Area Networks** (LANs). It was first developed by Xerox, and later refined by Digital, Intel, and Xerox. In an Ethernet configuration, computers are connected by coaxial or twisted-pair cable where they contend for network access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) paradigm. Ethernet can transfer information at up to 10 megabit-per-second (Mb/s).

FAQ

Acronym for **Frequently Asked Questions**. FAQs are widely available on the **Internet** and usually take the form of large, instructional text files. They are written on a wide variety of topics, and are usually the most up-to-date source for specialized information.

Federal Networking Council (FNC)

A collection of federal agencies that have heavy interests in federal networks using **TCP/IP** and the **Internet**. Representatives from DOD, DOE, DARPA, NSF, NASA, and HHS are the major members of the FNC.

File Transfer Protocol (FTP)

The most widely used way of downloading and uploading (getting and putting) files across an **Internet** connection. The File Transfer Protocol is a standardized way to connect computers so that files can be shared between them easily. There is a set of commands in FTP for making and changing directories, transferring, copying, moving, and deleting files. Formerly, all

FTP connections were text based, but graphical applications are now available that make FTP commands as easy as dragging and dropping. Numerous FTP **clients** exist for a number of platforms.

Finger

A UNIX command that shows information about a user or group of users on the **Internet**. When executed, the Finger command usually returns the user's real name, whether or not they have unread mail, and the time and date of their last login. Finger also displays two files (if they exist) located in the home directory of the user you fingered. These two files (the .PLAN and the .PROJECT files.) are simply ASCII text files that can be entered by the user to display any information upon being fingered.

Flame

A negative response to an **email** message or **newsgroup** posting. If you post an article or send an email to an audience that deems your message inappropriate, expect to get flamed. The most common recipients of flames are users who post commercial messages in public forums, those who post adult material in non-adult areas of the **Internet**, and users who post or send racial or gender-biased comments. The worst sort of flame is known as a **mail-bomb**, which occurs when the user being flamed opens his or her email and receives a flood of letters with unusually long file attachments that make his or her computer crash.

Follow-up

A reply to an **email** or **newsgroup** posting that continues the conversation or idea, known as a **thread**.

Freenet

A network system made up of community-based **bulletin board systems** with **email**, information services, interactive communications, and conferencing. They are usually funded and operated by individuals or organizations much like public television. Freenet providers are part of the National Public Telecomputing Network (NPTN), a Cleveland-based organization that works to make computer networking services as freely available as public libraries.

FTP

See **File Transfer Protocol**.

Gateway

A kind of "go-between" device or program that passes information between networks that normally couldn't communicate. What used to be called a gateway is now called a **router**. Not to be confused with a **protocol** converter.

Gopher

An information search and retrieval tool used widely for research. Gopher information is stored hierarchically on computers across the **Internet**. It uses a simple protocol that allows a client to access information from a multitude of numerous Gopher servers at one time, creating what's known as **gopher space**. The most common search tools in gopher are **Veronica** and Jughead. Gopher **clients** exist for most platforms.

Hacker

A computer user who works to understand the ins and outs of computers, networks, and the **Internet** in general. Hackers are generally benign, and are not to be confused with the more malicious **crackers**.

Hit

As used in reference to the World Wide Web, "hit" means a single request from a web *browser* for a single item from a web *server;* thus, for a web browser to display a page that contains 3 graphics, 4 "hits" would occur at the server: 1 for the *HTML* page, and one for each of the 3 graphics.

"Hits" are often used as a very rough measure of load on a server, e.g. "Our server has been getting 300,000 hits per month." Because each "hit" can represent anything from a request for a tiny document (or even a request for a missing document) all the way to a request that requires some significant extra processing (such as a complex search request), the actual load on a machine from 1 hit is almost impossible to define.

Host

A computer that is attached to a network or the **Internet**. Hosts allow users on **client** machines to connect and share files or transfer information. Individual users communicate with hosts by using client application programs.

Host Address

The address of a **host** computer on the **Internet**.

Hostname

The name given a **host** computer connected to the **Internet**.

HTML

See **HyperText Markup Language**.

Hypermedia

The combination of **hypertext** and multimedia in an online document.

Hypertext

A type of text that allows embedded **links** to other documents. Clicking on or selecting a hypertext link displays another document or section of a document. Most **World Wide Web** documents contain hypertext.

Hypertext Markup Language (HTML)

The standard way to mark text documents for publishing on the **World Wide Web**. HTML is marked-up using **tags** surrounded by brackets. To see what tagged HTML text looks like, select the View Source feature from the menus in the program you are using to view this document now, and you'll see a display of the HTML text used to create this page.

IMHO

Acronym for **In My Humble Opinion**. Generally seen in **IRC**, **email**, or **Usenet** postings.

Integrated Services Digital Network (ISDN)

A relatively new technology which combines voice and digital network services in a single medium. ISDN makes it possible for communications carriers to offer their customers digital data services as well as voice connections through a single line. **CCITT** defines the standards relating to ISDN.

International Organization for Standardization (ISO)

An organization of 89 member countries (founded in 1946) responsible for setting world standards in many electronics areas. Members of the ISO are the national standards organizations of the member countries.

Internet

A large, uncontrolled, unadministered, anarchic cyber-state that will soon take over the world! Basically, it's just everyone's computers hooked together. It's not a corporation, organization, or entity in itself. When you connect to the Internet, you actually become part of it. Always capitalized, the word Internet can also be referred to colloquially as the "Net."

Internet Assigned Numbers Authority (IANA)

The central registry for various **Internet** protocol parameters, such as port, protocol and enterprise numbers, and options, codes, and types. The currently assigned values are listed in the **Assigned Numbers** document. If you'd like more information or want to request a number assignment, you can **email** IANA at **iana@isi.edu**.

Internet Protocol (IP)

An industry standard, connectionless, best-effort packet switching **protocol** used as the network layer in the **TCP/IP** Protocol Suite.

Internet Protocol Address (IP Address)

The 32-bit address defined by the **Internet Protocol**. Every resource on the **Internet** has a unique numerical IP address, represented in dotted decimal notation. IP addresses are the closest thing the Internet has to phone numbers. When you "call" that number (using any number of connection methods such as **FTP**, HTTP, **Gopher**, etc.) you get connected to the computer to which that IP address is assigned.

Internet Service Provider (ISP)

An ISP is a company that maintains a network that is linked to the **Internet** via a dedicated communication line, usually a high-speed link known as a **T1**. An ISP offers use of its **dedicated communication lines** to companies or individuals (like me) who can't afford $1,300 a month for a direct connection. Using a modem, you can dial up to a service provider whose computers will connect you to the Internet, typically for a fee.

Internet Society (ISOC)

A non-profit, professional organization that supports the technical evolution of the **Internet** and stimulates the interest of members of the scientific and academic communities, industry, and the public regarding technology and the applications of the Internet. The ISOC also promotes the development of new applications for the Internet by publishing a quarterly newsletter, the Internet Society News, and by holding an annual conference, called **INET**.

InterNIC

Meaning **Internet information Center**, InterNIC is the combined name for the providers of registration, information, and database services to the **Internet**. InterNIC is who you contact if you want to register a **domain** name on the Internet.

IP

See **Internet Protocol**.

IP Address

See **Internet Protocol Address**.

IRC

The world-wide **party line** of the '90s. IRC allows multiple users to converse in real time on different **channels**. Channels (which have a # sign preceding their name) vary in traffic and content. Channel operators (or Ops) moderate the conversation, and have the ability to "kick" people from channels, or even ban them if their actions warrant it. IRC **clients** are available for nearly all platforms.

ISDN

See **Integrated Services Digital Network**.

ISO

See **International Organization for Standardization**.

ISOC

See **Internet Society**.

Java

Java is a network-oriented programming language invented by Sun Microsystems that is specifically designed for writing programs that can be safely downloaded to your computer through the Internet and immediately run without fear of viruses or other harm to your computer or files. Using small Java programs (called "*Applets*"), Web pages can include functions such as animations, calculators, and other fancy tricks.

We can expect to see a huge variety of features added to the Web using Java, because you can write a Java program to do almost anything a regular computer program can do, and then include that Java program in a Web page.

See **Applet**.

LAN

Acronym for **Local Area Network**. LANs are now commonplace in most businesses, allowing users to send **email** and share resources such as files, printers, modems, etc. Currently, most larger companies are connecting their LANs to the **Internet**, allowing users to connect to resources within or outside the LAN.

Leased Line

A **dedicated** full-time connection used to link a user or network to an **Internet Service Provider** or another network.

Listserv

An automated mailing list distribution system. Listservs exist for a multitude of professional, educational, and **special interest groups**. Usually, you have to send an **email** to a Listserver with the subject **SUBSCRIBE listname** or something to that effect. You are then **subscribed** to that **mailing list** and (depending on the service) will receive regular mail from a single source or from all members who send email to the Listserver. Listserv was originally designed for the **Bitnet**/EARN network.

Lurking

Non-active participation on the part of a subscriber to a **mailing list**, a **Usenet** newsgroup, an **IRC** channel, a video connection, or any other **Internet** communication device. If you're "lurking," you're generally just listening to the discussion. It's usually best to lurk if you're a beginner or if you are new to a communication group. This allows you to get up to speed on the history or acceptable behavior of the group.

Mailing List

A list of **email** addresses used to forward messages to groups of people. When you subscribe to a mailing list, you receive all mail sent to that list (see also **Listserv**).

Mail Reflector

A program that distributes files or information in response to requests sent via **email**. Many **Listservs** have mail reflectors. You can request documents of a reflector by sending a message with the subject **SEND document name** or a similar command. Mail reflectors are also being used to provide **FTP**-like services for users with limited **Internet** access. **MIME Encoding**
See **Multipurpose Internet Mail Extensions Encoding**.

Mirror Site

Because of the popularity of some **FTP** and **Web** sites, mirror sites came into existence. They are areas on a computer that "mirror" or contain an exact replica of the directory structure of another computer. If you have trouble getting connected to an FTP site, for example, because of the high amount of traffic, you can usually connect to a mirror site that contains the same information on a different computer. Mirror sites are usually updated once a day.

Moderator

The person who manages moderated **mailing lists**, **newsgroups**, or online discussion forums for services such as AOL, CompuServe, or the Microsoft Network.

Mosaic

A graphical browser for the **World Wide Web** that supports **hypermedia**. The NCSA (National SuperComputer Association) invented the Mosaic browser, which quickly became the industry standard. Netscape Communications Corporation later invented the **Netscape Navigator**, which has redefined the content on the Web. Other major companies entered the browser market with little success, until Microsoft launched their **Internet Explorer**, which now contends with Navigator as the browser of choice. The term **Mosaic** is sometimes used incorrectly as a synonym for the World Wide Web.

MUD

Acronym for **Multi-User Dungeon** or **Domain**. MUDs are role-playing games that take place on a computer. Users can **Telnet** to a MUD host, and create a character. MUDs can be action, adventure, or fantasy games, and allow you to save your character for future play. Some MUDs have thousands of registered characters, and most foster a community or culture of their own. These are highly addictive areas of the **Internet**, and users can spend many hours enthralled in this type of activity.

Multipurpose Internet Mail Extensions Encoding (MIME Encoding)

MIME is a standardized method for organizing divergent file formats. The method organizes file formats according to the file's MIME type. When **Internet** (usually **email**) software retrieves a file from a **server**, the server provides the MIME type of the file, and the file is decoded correctly when transferred to your machine.

Netiquette

The combination of the words **Net** and **etiquette**, this refers to the proper behavior on a network, and more generally the **Internet**. The key element in Netiquette is remembering that actual people are on the other end of a computer connection, and offensive comments or actions are just as offensive even if you can't see your recipient.

Network File System (NFS)

A protocol developed by Sun Microsystems. NFS allows a computer to access and use files over a network as if they were local. This protocol has been incorporated into the products of more than 200 companies and is now a de facto **Internet** standard.

Network News Transfer Protocol (NNTP)

An industry standard protocol for the distribution, inquiry, retrieval, and posting of **news** articles.

NFS

See **Network File System**.

NNTP

See **Network News Transfer Protocol**.

Open Systems Interconnection (OSI)

A suite of **protocols**, designed by **ISO** committees to be the international standard computer network architecture.

OSI

See **Open System Interconnection**.

Packet

The common term for the standard unit of data sent across a network.

Packet Internet Gopher (PING)

The simplest way to test or time the response of an **Internet** connection. A **PING** sends a request to an Internet **host** and waits for a reply called (yep, you guessed it), a **PONG**. When you PING an address, you get a response telling you the number of seconds it took to make the connection. PING **clients** exist for a number of platforms, or you can use a UNIX or Windows 95 prompt to issue a PING command directly.

PAP

See **Password Authentication Protocol**.

Password Authentication Protocol (PAP)

One of the many **authentication** methods that can be used when connecting to an **ISP**. PAP allows you to login automatically, without having to use a terminal window to type in your username and password. One warning about PAP: passwords are sent over the connection in text format, which means there is no protection if someone is "listening-in" on your connection.

Plug-in

A piece of software (usually small) that adds features to a larger piece of software. Common examples are plug-ins for the Netscape® *browser* and web *server*. Adobe Photoshop® also uses plug-ins. The idea behind plug-in's is that a small piece of software is loaded into memory by the larger program, adding a new feature, and that users need only install the few plug-ins that they need, out of a much larger pool of possibilities. Plug-ins are usually created by people other than the publishers of the software the plug-in works with.

Point of Presence (POP)

An installation of telecommunications equipment, usually digital **leased lines** and multi-**protocol routers**.

Point-to-Point Protocol (PPP)

A **protocol** that provides a method for transmitting **packets** over serial point-to-point links. PPP is one of the most popular methods for **dialup** connections to the **Internet**, because it allows you to use other standard protocols (such as IPX, **TCP/IP**, and Netbeui) over a standard telephone connection, but it can also be used for **LAN** connections.

POP

See either **Point of Presence** or **Post Office Protocol**.

Posting

The sending of an article to a **Usenet** newsgroup or the placing of a message on a **BBS**.

Post Office Protocol (POP)

A **protocol** designed to allow single users to read mail from a **server**. There are three versions: POP, POP2, and POP3. When **email** is sent to you, it is stored on the server until accessed by you. Once you are **authenticated**, the POP is used to transmit the stored mail from the server to your local mailbox on your **client** machine.

PPP

See **Point-to-Point Protocol**.

Protocol

Simply, the "language" spoken between computers to help them exchange information. More technically, it's a formal description of message formats and the rules that two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces (like the order in which bits and bytes are sent across a wire) or high-level exchanges between allocation programs (the way in which two programs transfer a file across the **Internet**).

Read the Flippin' Manual (RTFM)

An acronym used to respond to a simple or commonly asked question.

Request for Comments (RFC)

A document series, begun in 1969, which describes the **Internet** suite of **protocols** and related experiments. Not all (actually, very few) RFCs describe Internet standards, but all Internet standards are written up as RFCs.

RFC

See **Request for Comments**.

Router

A device that forwards traffic between networks. Forwarding decisions are made based on network layer information and routing tables, often constructed by routing **protocols**.

Serial Line Internet Protocol (SLIP)

Similar to **PPP**, SLIP is another standard **protocol** used to run **TCP/IP** over serial lines, such as telephone circuits or RS-232 cables. Unlike PPP, however, SLIP does not work on **LAN** connections. SLIP used to be the most popular way for **dialup** users to access the **Internet**, but PPP quickly overcame SLIP because of its ease of use and integration into many client operating systems.

Server

Simply, a computer that provides resources, such as files or other information. Common **Internet** servers include file servers and name servers **Domain Name Service**.

Service Provider

See **Internet Service Provider**.

SIG

Acronym for **Special Interest Group**. SIGs sponsor a variety of **Listservs**, **IRC** channels, and **Internet** sites. Also a nickname for a **Signature**.

Signature

An ASCII text file that can be automatically attached to the bottom of a piece of **email** or **newsgroup** posting that identifies the sender. Many signatures (or **sigs**) use symbols and characters to create images or words to make the sig more interesting.

Simple Mail Transfer Protocol (SMTP)

A **protocol** used to transfer **email**. SMTP transfers mail from **server** to server, and the end user must use POP (see also **Post Office Protocol**) to transfer the messages to their machine.

Simple Network Management Protocol (SNMP)

Developed to manage nodes on an **IP** network, SNMP is an **Internet** standard **protocol**. It can be used to manage wiring hubs, video toasters, CD ROM jukeboxes, and many other devices.

SLIP

See **Serial Line Internet Protocol**.

Smiley

The use of punctuation marks and other symbols or characters to portray moods when typing, especially in **email** messages and **IRC**. Here's an example of a simple smiley: **:)**. If you don't see it, tilt your head to the left and look at it. The colon makes the eyes and the parenthesis makes the smiley mouth. The smile means happiness (like if someone says something funny) or it often denotes sarcasm. Other combinations of characters can express many other emotions. You may also hear them referred to as **emoticons.**

SQL

(Structured Query Language)—A specialized programming language for sending queries to databases. Most industrial-strength and many smaller database applications can be addressed using SQL. Each specific application will have its own version of SQL implementing features unique to that application, but all SQL-capable databases support a common subset of SQL.

SRI

A research institute based in California that runs the Network Information Center (NISC).

SSL

(Secure Sockets Layer)—A protocol designed by Netscape Communications to enable encrypted authenticated communications across the Internet. SSL used mostly (but not exclusively) in communications between web *browsers* and web *servers*. *URLs* that begin with "http" indicate that an SSL connection will be used. SSL provides 3 important things: Privacy, Authentication, and Message Integrity. In an SSL connection each side of the connection must have a *Security Certificate*, which each side's software sends to the other. Each side then encrypts what it sends using information from both its own and the other side's Certificate, ensuring that only the intended recipient can de-crypt it and that the other side can be sure the data came from the place it claims to have come from and that the message has not been tampered with.

Subnet Mask

See **Address Mask**.

T1

One of AT&T's terms used to denote the type of connection of a **host** to the **Internet**. A T1 transmits a DS-1 formatted digital signal at **1.544 megabits** per second.

T3

One of AT&T's terms used to denote the type of connection of a **host** to the **Internet**. A T3 transmits a DS-3 formatted digital signal at **44.746 megabits** per second—about 40 times the speed of a T1.

TCP/IP

See **Transmission Control Protocol/Internet Protocol**.

TCP/IP Stack

To properly use the TCP/IP **protocol**, PCs require a **TCP/IP** stack. This consists of TCP/IP software, sockets software (such as **WINSOCK.DLL** for Windows machines), and hardware driver software (known as packet drivers). Windows 95 comes with Microsoft's own built-in TCP/IP stack, including version 1.1 of Microsoft's WINSOCK.DLL and packet drivers.

Telnet

The **Internet** standard **protocol** to connect to remote terminals. Telnet **clients** are available for most platforms. When you Telnet to a UNIX site, for example, you can issue commands at the prompt as if the machine were local.

TN3270

A slight variation of **Telnet** used to connect the user to an IBM mainframe. TN3270 **clients** exist for most platforms.

Token Ring

A type of **LAN** in which networked computers are wired into a **ring**. Each computer (or node) is in constant contact with the next node in the ring. A control message, called a **token**, is passed from one node to another, allowing the node with the token to send a message out to the network. If the ring is "broken" by one computer losing contact, the network can no longer communicate. The IEEE 802.5 token ring standard is the most common.

Topology

The layout of all the computers on a network and the links that join them.

Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP is the standard communications **protocol** required for **Internet** computers. To communicate using TCP/IP, PCs need a set of software components called a **TCP/IP stack**. Macintosh computers typically use a proprietary software package called MacTCP. Most UNIX systems are built with TCP/IP capabilities.

Universal Resource Locator (URL)

More commonly referred to as the **URL**, the Universal Resource Locator refers to the entire address that is recognized "universally" as the address for an Internet resource. Each resource on the Internet has a unique URL. URLs begin with letters that identify the resource type, such as http, ftp, gopher, etc. These types are followed by a colon and two slashes. Next, the computer's name is listed, followed by the directory and filename of the remote resource. For example, the URL for this glossary is **http://www.winfiles.com/glossary.html**.

UNIX-to-UNIX Copy (UUCP)

Originally, UUCP was a program that allowed UNIX systems to transfer files over phone lines. Currently, the term is used to describe the **protocol** that passes **news** and **email** across the **Internet**.

Usenet

Usenet groups are more commonly known as **newsgroups**. There are thousands of groups hosted on hundreds of servers around the world, dealing with various topics. Newsreader software is required to properly download and view **articles** in the groups, but you can usually **post** an article to a group simply by **emailing** to it.

UUCP

See **UNIX-to-UNIX Copy**.

Veronica

A search engine (not unlike **Archie**) that is built into **Gopher**. It allows searches of all gopher sites for files, directories, and other resources.

W3

See **World Wide Web**.

WAIS

See **Wide Area Information Service**.

White Pages

Databases containing **email** addresses, telephone numbers, and postal addresses of **Internet** users. You can search the Internet White Pages to find information about particular users.

WHOIS

An **Internet** program (related to **Finger** and the **White Pages**) that lets you enter an Internet entity (such as **domains**, networks, and **hosts**) and display information such as a person's company name, address, phone number and **email** address.

Wide Area Information Service (WAIS)

A distributed information service and search engine that allows natural language input and indexed searching. Many **Web** search utilities use a WAIS engine.

Winsocks

Stands for **Windows Sockets**. Winsocks is a set of specifications or standards for programmers creating **TCP/IP** applications for use with Windows.

World Wide Web (WWW or W3)

The **Web** is a collection of online documents housed on **Internet** servers around the world. The concept of the Web was created by researchers at CERN in Switzerland. Web documents are written or **coded** in **HTML**. To access these documents, you have to use a **Web browser**. When these browsers access (or hit) a page, the server uses the HyperText Transfer Protocol (HTTP) to send the document to your computer.

Worm

A computer program that replicates itself and is self-propagating. Whereas viruses are designed to cause problems on a local system and are passed through boot sectors of disks and through files, worms are designed to thrive in network environments. Network worms were first defined by Shoch & Hupp of Xerox in ACM Communications (March 1982). The most famous (or infamous) worm was the Internet Worm of November 1988. It successfully propagated itself on over 6,000 systems across the **Internet**.

WWW

See **World Wide Web**.

Common Internet File Formats

Because much of your time will be spent working with files and other forms of electronic data, the following table has been provided to help take away some of the mystery of file formats and their meaning.

File Suffix	Format Description	Type
.aiff	Semi-common sound format	Binary
.au	Most common sound format on the web	Binary
.bin	Mac binary II encoded file	Binary
.doc	May be a DOS/Windows program files or self-extracting archive	Binary
.exe	May be a DOS/Windows program files or self-extracting archive	Binary
.gif	Graphical Interchange Format—most common graphics format on the web, but not the most economical in terms of space.	N/A
.gz	The Gnu version of zip. This is a compression algorithm for Unix	Binary
.hqx	BinHex 4.0—encryption program for Macintosh files	Binary
.html or .htm	Hypertext markup language—the format used on most web-based documents	Text
.image	Macintosh Disk Image file	Binary
.jpg, .jpeg or .jfif	Common graphic format. Very economical in terms of space requirements.	Binary
.mov, .qt, .movie or .moov	Apple's QuickTime Movie formats	Binary
.mpg or .mpeg	The standard movie platform on the Internet	Binary
.pdf	Adobe Acrobat Portable document format. Documents in this format can be used on any platform.	Binary
.ps	Postscript files used for printing. Not readable.	Text
.sea	Macintosh self-extracting archive file	Binary
.sit	Stuffit Archive compression file	Binary
.tar	Unix tar program takes separate files and combines them into one file	Binary
.tiff or .tif	Very large and very high quality image format	Binary
.txt	You guessed it—plain ol' text file	Text
.uu or .uue	Encoded file usually done on a Unix machine. Popular with some older email packages.	Binary
.wav	Windows wage format sound file	Binary
.z	Unix compressed file	Binary
.zip	Pkzip—a common DOS/Windows compression format	Binary

APPENDIX B

Summary of State-by-State Temporary Practice Rules

The following table has been extracted from the AICPA/NASBA Digest of State Laws and State Board Regulations—1998. Practitioners performing an engagement, or portion of an engagement, in a state other than where he or she is licensed should consider how the following information impacts their engagement and consider contacting the state board of accountancy prior to the beginning of the engagement.

State	Temporary Practice
Alabama	The Board may issue an annual temporary permit to an out-of-state CPA to fulfill specific engagements contracted for outside Alabama.
Alaska	General permits for nonresident firms can be obtained on a temporary basis.
Arizona	The jurisdiction does not provide for temporary practice.
Arkansas	An out-of-state accountant may practice temporarily and periodically in Arkansas if he/she is conducting a regular practice outside of the State.
California	Any person who is the holder of a valid and unrevoked license as a certified public accountant under the provisions of Section 5087 may, after application for a license and after providing evidence of qualifying continuing education, engage in the practice of public accountancy in this State as a certified public accountant, until such time as his or her application for a license may be granted or rejected.
Colorado	Temporary practice by an out-of state accountant is permitted on professional business incident to regular out-of-state business.
Connecticut	No mention in Digest
Florida	A temporary license is required for out-of-state practitioners to fulfill specific engagements when they must come into the state to complete the engagement. Temporary licenses are not valid for more than ninety (90) days and will not be granted to practitioners who are residents. To obtain a temporary permit, an application must be completed, a fee paid, and a copy of one audited, one reviewed, and one compiled financial statement must be submitted with the first temporary permit requested each calendar year.
Georgia	Temporary permits are issued to those individuals or firms not residing in Georgia but holding valid permits to practice in another jurisdiction that was issued after the recipient passed an examination equivalent to that required by the Georgia Board. An applicant must meet equivalent educational and experience requirements in effect in Georgia. Ten (10) years of public accounting experience may be accepted in lieu of examination requirement. A reciprocal certificate may be issued to an applicant provided that the state of original issuance grants a similar privilege to Georgia CPAs.
Guam	The jurisdiction makes no provision for the issuance of temporary permits to practice.

State	Temporary Practice
Hawaii	A temporary permit may be issued for a period of three (3) months to out-of-state accountants to fulfill specific engagements that are incidental to their practice out of state. Application must be filed no later than sixty (60) days prior to the engagement. Verification of a current, valid license is required.
Idaho	A CPA or LPA of another state or country holding a valid and unrevoked license may temporarily practice for a period not exceeding thirty (30) days in a calendar year. Individuals must make advance written notification to the Board.
Illinois	Temporary practice by a CPA licensed by another jurisdiction is permitted for professional business incident to regular practice in another jurisdiction.
Indiana	Temporary practice by an out-of-state accountant is permitted on business incident to his/her regular practice out of state, provided that such practice is conducted in conformity with the Board's rules.
Iowa	Temporary practice is permitted if it is temporary in nature and is incident to a regular practice outside of Iowa.
Kansas	Kansas no longer issues temporary permits to practice. All out-of-state CPAs wishing to practice in Kansas, on business not incidental to their practice in another state, must now obtain a Kansas CPA certificate by reciprocity and then a permit to practice. The Board defines what it considers to be incidental to one's regular practice. Permits are required prior to commencing business in Kansas.
Kentucky	Kentucky does not have a temporary practice rule. CPAs of other states are expected to become licenses unless the work in Kentucky is incidental to their practice. "Incidental" is defined as "an engagement that was initiated with a client located outside of the Commonwealth and has extended into the commonwealth due to common ownership or existence of a subsidiary, assets, or other operations located within the Commonwealth."
Louisiana	A temporary permit may be issued to a licensed CPA of another state for a period of ninety (90) days for a specified single engagement. The permit is not renewable. A temporary permit for Practice Monitoring Engagements may be issued to a licensed CPA of another state for a period of one (1) year and may be renewed annually. The permit may only be used to perform quality/peer reviews and is not a license to practice or authorization to engage in the practice of public accounting in Louisiana.
Maine	There is not provision for the issuance of temporary permits to practice.
Maryland	Individuals must secure limited licenses, and corporations or partnerships must secure limited permits. An application must be filed and a fee paid. A limited license/permit shall be good for no more than one (1) year and is for practice on a specified job. An explicit set of requirements must be met to secure a limited license/permit.
Massachusetts	The Board has no provisions for granting temporary permits to practice.
Michigan	An applicant may obtain a temporary permit if certified properly outside the State for a one (1)-year period to work directly under the supervision of a licensed individual.
Minnesota	CPAs who are licensed and in good standing in other states, and who come into Minnesota for engagements that will last more than thirty (30) days in any twelve (12)-month period, must apply for a temporary license. The license expires at the end of twelve (12) calendar months from the date it was granted.
Mississippi	A CPA from another state may practice in Mississippi on a temporary basis if such practice is incident to the practitioner's regular practice out of state. "Temporary" is defined as less than ten (10) days during a year and "regular out-of-state practice" as not including engagements with a Mississippi-domiciled entity.

State	Temporary Practice
Missouri	Out-of-state CPAs who have a Missouri client must be licensed. Such out-of-state accountants may practice temporarily in Missouri on professional business incident to their regular practice for clients outside Missouri. The phrase "temporarily practicing in this state on professional business incident to regular practice outside this state," as used in section 326.012(1) RSMo, means that practice that is a continuation or extension of an engagement for a client located outside Missouri, which engagement began outside Missouri and extends into Missouri through common ownership, existence of a subsidiary, assets, or other operations located within Missouri.
Montana	Not allowed.
Nebraska	No mention in Digest.
Nevada	An out-of-state accounting firm may temporarily practice in Nevada by obtaining a temporary permit that is issued for the period of a specific engagement (not to exceed six [6] months). Permits are issued to the firm. The proprietor, partner, or shareholder responsible for the engagement must meet all current Nevada requirements for licensing.
New Hampshire	A CPA of another state may practice in New Hampshire after acquiring a foreign accountant practice permit. This is required for all engagements however incidental.
New Jersey	The Board does not permit temporary practice. The Board does permit occasional audits in the state by licensees other states as long as a licensee of another state does not open a practice in new Jersey, the out-of-state licensee may conduct business in New Jersey and issue the audit report from his/her home state.
New Mexico	An out-of-state accountant may temporarily practice in New Mexico on professional business upon filing the proper application for reciprocity with the Board office. However, temporary authority to practice shall not prevent the Board from refusing, after complying with the provisions of the Uniform Licensing Act, to issue a certificate or permit if the applicant otherwise fails to qualify for a certificate under the New Mexico Public Accountancy Act.
New York	An out-of-state accountant may perform services in New York that are incidental to such person's practice outside of the State.
North Carolina	A CPA without a North Carolina certificate wishing to perform an engagement in North Carolina must apply for a reciprocal certificate. A CPA can request a temporary certificate for an engagement prior to the issuance of the reciprocal certificate. All CPAs who will be assigned to an engagement must also have reciprocal certificates.
North Dakota	No provisions are made for temporary practice.
Ohio	Temporary practice in Ohio is generally prohibited. Please contact the Board for details.
Oklahoma	An accountant of another state or foreign country may temporarily practice in Oklahoma or engage in professional business, provided such temporary practice must be a continuance of an engagement for a client located outside Oklahoma that extends into Oklahoma through common ownership, existence of a subsidiary, assets, or other operations located within Oklahoma. No permit or registration is required for temporary practice.
Oregon	An out-of-state accountant may temporarily practice in Oregon on professional business, incident to his/her regular practice, without obtaining permission from the Oregon Board. Also, reciprocity applicants who request permission in writing may be allowed to practice accounting in Oregon until their Oregon license is granted or denied. Otherwise, no other circumstance allows any practice of accounting in Oregon without first obtaining an Oregon license.
Pennsylvania	An out-of-state accountant who is engaged in public practice in Pennsylvania on professional business incident to his/her regular practice outside of Pennsylvania, provided such temporary practice is conducted in conformity with Board rules. He/she must apply to the Board and receive written approval.

State	Temporary Practice
Puerto Rico	The Board does not give special permits to out-of-jurisdiction CPAs to work in Puerto Rico. An extra-territorial accountant may temporarily practice in Puerto Rico on professional business incident to his/her regular practice outside Puerto Rico.
Rhode Island	A certified public accountant who holds a permit to practice issued by another state and who practices in Rhode Island must apply for a permit to practice in Rhode Island. From the date of filing the completed application with the Board, the applicant shall be deemed qualified to practice and may practice public accounting in Rhode Island until the Board has acted upon the application. Such application shall constitute the appointment of the Secretary of State as an agent for service of process in any action or proceeding arising out of any transaction or operation connected with, or incidental to, the practice of public accounting in Rhode Island by such applicant.
South Carolina	Temporary practice by a licensed accountant of another state is permitted on business incident to such person's regular practice outside the State, provided that the applicant registers with the Board and complies with its regulations. Registration is not required if services within the State do not exceed a total of ten (10) days in a calendar year.
South Dakota	There is no provision for the issuance of temporary permits to practice. Any individual or firm intending to practice public accountancy in South Dakota, even for one engagement, must apply for a permit to practice. The permit must be renewed or maintained during the fiscal year in which the individual or firm is practicing in the state.
Tennessee	There is no provision for temporary practice in this jurisdiction. Individuals must notify the Board office regarding their intent to practice if they are from a "substantially equivalent" state. Otherwise, applicants must apply for reciprocity.
Texas	For a fee of $100, a licensed accountant from another state or territory may practice temporarily in Texas on professional business incident to his/her regular practice.
Utah	An out-of-state accountant may practice temporarily in Utah if the practice is incidental to his/her regular out-of-state practice, provided that such practice is conducted in conformity with Utah laws and rules.
Vermont	An out-of-state accountant may temporarily or periodically practice in Vermont if he/she is conducting a regular practice outside of Vermont, provided the temporary practice is conducted in conformity with the regulations and rule of professional conduct promulgated by the Board. All nonresident firms licensed or registered in another state or country that desires to practice temporarily in Vermont must register with the Board and pay the required fee. The Board shall adopt rules prescribing the procedure to be followed in carrying out the registrations. Registrations under this section shall expire three (3) months after issuance.
Virginia	Virginia makes no provision for the issuance of temporary permits to practice.
Virgin Islands	An out-of-state accountant may temporarily practice in the U.S. Virgin Islands on professional business incident to his/her regular practice.
Washington	The Board does not issue temporary practice permits to out-of-state CPAs or CPA firms. A CPA from another state may temporarily practice in Washington provided the business is incidental (less that 10% of the firm's total business for the year) to the CPA's regular out-of-state practice, and the CPA holds a valid license to practice public accounting issued by the other state.

State	Temporary Practice
West Virginia	A person holding a certificate or registration issued by the accountancy board of another jurisdiction may temporarily practice in this state on professional business incident to his/her regular practice provided hat he/she shall in the practice be governed by this rule and pay a fee. An application for a nonresident or temporary license must be completed, accompanied by a certifying/verifying letter from the applicant's resident board, a copy of the applicant's current license to practice in his/her resident state, and the required fee. This temporary or nonresident permit/license may be renewed.
Wisconsin	A CPA of another state may temporarily practice in Wisconsin on professional business incident to an engagement with a client of his/her regular practice in the state in which he/she is domiciled, provided that such CPA has neither residence nor office in Wisconsin, and that the client is not located exclusively in Wisconsin.
Wyoming	Available while the individual is in the process of applying for a certificate or permit.

APPENDIX C

Sample Forms

This appendix includes forms for the WebTrust engagement. Please note that they are divided into several categories, as indicated.

GENERAL

- WebTrust Engagement File Index
- Client Self-Assessment Document
- Engagement Letter
- Request of Arbitration Representation Letter
- Management Representation Letter
- EID Number and Documentation from the AICPA
- Supervision, Review, and Approval Form
- Engagement Termination Letter
- Mailing House Request Letter

ENGAGEMENT PLANNING AND EXECUTION

- Engagement Acceptance Worksheet
- Summary WebTrust Work Program Worksheet
- WebTrust Work Program
- Client Information Worksheet
- General Control Environment Worksheet
- Analytical Procedures
- Transaction Walk-Through Worksheet
- Self-Monitoring Worksheet

BUSINESS PRACTICES AND INFORMATION PRIVACY CRITERIA

- Business Practices and Information Privacy Practices Disclosure Worksheet
- Privacy Disclosures and Policies Worksheet
- Dispute Resolution Disclosures
- Legal and Regulatory Issues
- Test of Transactions

Transaction Integrity

- Transaction Integrity Controls Worksheet
- Order Entry Process Worksheet
- Credit Card System Evaluation Worksheet
- Test of Transactions

Information Protection

- Information Protection Controls Worksheet
- Information Protection Controls System Architecture
- Site Security
- Firewall Control Evaluation
- Disaster Recovery and Physical Access
- Information Protection Controls Tests of Transactions

Change Management and Accountant Notification

- CPA Notification of Change

Other Matters

- Other Matters Worksheet

WebTrust Engagement File Index

Client: ______________________________

Closing date: __________________________

WP Reference/Index	Description
	General
	Client Self-Assessment Document (obtain from WebTrust Principles and Criteria for Business-to-Consumer eCommerce, version 2, Appendix B at the AICPA website at: www.aicpa.org/webtrust/index.htm)
	(The self-assessment document for ISP in eCommerce is coming soon.)
	Engagement Letter
	Request of Arbitration Representation Letter
	Management Representation Letter
	EID number and documentation from AICPA (also see Appendix H for enrollment information)
	Supervision, Review, and Approval Form
	Engagement Termination Letter
	Mailing House Request Letter
	Engagement Planning and Execution
	Engagement Acceptance worksheet
	Summary WebTrust Work Program Worksheet
	WebTrust Work Program
	Client Information Worksheet
	General Control Environment Worksheet
	Analytical Procedures
	Transaction Walk-Through Worksheet
	Self-Monitoring Worksheet
	Business Practices and Information Privacy Criteria
	Business Practices and Information Privacy Practices Worksheet
	Privacy Disclosures & Policies Worksheet
	Dispute Resolution Disclosures
	Legal and Other Regulatory Issues
	Test of Transactions

WebTrust Engagement File Index (cont.)

Client: ______________________________

Closing date: _________________________

WP Reference/Index	Description
	Transaction Integrity
	Transaction Integrity Controls Worksheet
	Order-Entry Process Worksheet
	Credit Card Evaluation Worksheet
	Test of Transactions
	Information Protection
	Information Protection Controls Worksheet
	Information Controls System Architecture Worksheet
	Site Security Worksheet
	Firewall Control Evaluation Worksheet
	Disaster Recovery & Physical Access Worksheet
	Test of Transactions
	Change Management and Accountant Notification
	CPA Notification of Change Process
	Other Matters
	Other Matters Worksheet

Client Self-Assessment Document

Note: The self-assessment document for WebTrust-ISP in eCommerce is coming soon and will be available at the AICPA website at www.aicpa.org/webtrust/index.htm.

WEBTRUST $^{SM/TM}$ SELF-ASSESSMENT QUESTIONNAIRE (VERSION 2.0)

This questionnaire is for use by e-commerce service providers in documenting their e-commerce business practices disclosures and related controls and in documenting a basis for their assertion or representation that "on its Web site at www.___.____ during the period __________, 1999 through __________, 2000 the entity—

- Disclosed its business and information privacy practices for e-commerce transactions and executed transactions in accordance with its disclosed practices.
- Maintained effective controls to provide reasonable assurance that customers' transactions processed using e-commerce over the web were completed and billed as agreed.
- Maintained effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce was protected from uses not related to its business.

based on the AICPA/CICA WebTrust $^{SM/TM}$ Criteria."

Entity Name ______________________ Entity Location ______________________

Web Site URL ____________________ Server Location ____________________

Period Covered: From ______________ Through ____________________________

Date Prepared ____________________ Prepared By ________________________

I General Information

A. E-commerce Activities to Be Covered

1. Describe the entity's e-commerce activities that are asserted and represented to meet the WebTrust Principles and Criteria.

   a) What goods and services are being sold or provided?

   b) Who is the typical customer?

   c) What is the typical form of payment?

2. What is the Web site URL?

3. Who is responsible for controlling these activities and what is their reporting relationship to the entity's management?

4. How long has the entity been selling such goods and services through this form of e-commerce?

5. If the e-commerce activities have changed in the last ninety days, describe the nature of such changes and when each change occurred.

B. Information Systems Used to Support E-commerce Activities

1. List the Web Site or other customer interface systems and provide the following information about each.

   a) Provide a description.

   b) Indicate who, in this entity, is responsible.

   c) Describe any portion of these systems that is outsourced to third parties.

   d) Describe the frequency and nature of changes to Web site and customer interface systems.

2. List the telecommunications and network systems, including the following information.

   a) Give a description.

   b) Indicate, who, in this entity, is responsible.

c) Describe any portion of these systems that is outsourced to third parties.

d) Describe the frequency and nature of changes to telecommunications and network systems.

3. List the other supporting systems and technology, including the following information.

a) Provide a description.

b) Indicate who, in this entity, is responsible.

c) Describe any portion of these systems that is outsourced to third parties.

d) Describe the frequency and nature of changes to such systems and technology.

C. Web Site Server Technology

1. Describe the e-commerce server platform(s) in use (description and version).

2. How many e-commerce servers are in use at the primary site? How many are at an alternate or backup site?

3. Is SSL used for some, or all, Internet transactions? If so, describe the kinds of transactions for which SSL is used and the kind of server digital certificate being used.

4. Identify the technical staff (and/or whether the site is hosted by an ISP and the technical staff of the ISP) who are capable of performing the following technical tasks.

a) Generate a Certificate Signing Request (CSR) using the Web server software?

b) Install a Digital Certificate (also known as a Digital ID) on the Web server software?

c) Configure certain pages on your web server to be secure using (SSL)?

d) Install a Java Applet on the appropriate Web page?

5. Identify the WebServer package used.

If the site is running on Netscape 2.0 +, Microsoft IIS 2.0+, C2Net Apache Stronghold, Oracle Server, O'Reilly, WebSite Pro 2.0+, Primehost 2.033+, Advanced Business Link Server, Oracle Server, JavaSoft Server, Open Market Server 2.1+, there should be no technical difficulties using the WebTrust service. If another WebServer software package is being used, VeriSign should be contacted to ensure compatibility. A complete WebTrust test package may be obtained by contacting VeriSign directly. Identify the version of Netscape that your customer base is most likely to be using. Users using Netscape 4.05 will see the message "The Certificate Authority used to sign this certificate has expired. Do you wish to proceed?" If the user agrees, the session proceeds as normal. This is a general problem affecting virtually all commerce sites using VeriSign Digital Certificates, not only WebTrust sites.

D. Control Environment

1. Describe the factors in the entity's organization that contribute to a control environment that is generally conducive to reliable business practice disclosures on its Web site and effective controls over e-commerce transaction integrity and the protection of related private customer information. Such factors might include, but are not limited to the following:

   a) Management's "tone at the top"

   b) Hiring, development, and retention of competent personnel

   c) Emphasizing the importance and responsibilities for sound business practices and effective control

   d) Supervising business activities and control procedures

   e) Employing a suitable internal auditing function that periodically audits matters related to the entity's e-commerce activities

   f) Other factors

II Business and Information Privacy Practices

Principle - ***The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.***

A. Description of Business Practices.

1. Describe the entity's business practices and how such practices are disclosed to customers for each of the following.

   a) Descriptive information about the nature of the goods that will be shipped or the services that will be provided, including the following:

      (1) Condition of goods (meaning, whether they are new, used, or reconditioned).

      (2) Description of services (or service contract).

      (3) Sources of information (meaning, where it was obtained and how it was compiled).

      (4) Other relevant descriptive information.

   b) The terms and conditions by which e-commerce transactions are conducted

      (1) Time frame for completion of transactions (transactions means fulfillment of orders where goods are being sold and delivery of service where a service is being provided).

      (2) Time frame and process for informing customers of exceptions to normal processing of orders or services requests (e.g., backorders or other order exceptions) and available customer options.

      (3) Normal method of delivery, including customer options, where applicable.

      (4) Payment terms, including customer options, if any.

      (5) Electronic settlement practices and related charges to customers.

      (6) How the customer may cancel recurring charges, if any.

      (7) Product return policies and/or limited liability, where applicable.

      (8) Other relevant terms and conditions, if any.

   c) Where on its Web site (and/or in information provided with the product) customers can obtain warranty, service, and support related to the goods and services purchased on the Web site.

   d) Information to enable customers to file claims, ask questions and register complaints, including but not limited to the following:

      (1) Street address (not a post office box or e-mail address).

      (2) Telephone number (a number to reach an employee on a reasonably

timely basis and not only a voice mail system or message machine).

(3) Days and hours of operation.

(4) If there are several offices or branches, the same information for the principal office.

(5) Other relevant information for customers,

e) The entity discloses on its Web site its information privacy practices. These practices include but are not limited to, the following disclosures:

(1) The specific kinds and sources of information being collected and maintained.

(2) The use of that information.

(3) Possible third-party distribution of that information.

(4) Choices regarding how individually identifiable information collected from an individual online may be used and/or distributed.

(5) The consequences, if any, of an individual's refusal to provide information.

(6) How erroneous or incomplete individually identifiable information collected can be reviewed and, if necessary, corrected or removed.

(7) How to resolve complaints related to accuracy, completeness, and distribution of private customer information and the consequences for failure to resolve such complaints.

(8) The address and contact information for any government bodies that receive consumer complaints on privacy matters.

f) The disclosure of the dispute resolution process that should have at a minimum the following attributes:

(1) Management's commitment to use a specified third party dispute resolution service in the event the customer is not satisfied with the entity's proposed resolution of such a complaint.

(2) A commitment from such a service to handle such unresolved complaints.

(3) Procedures to be followed in resolving such complaints, first with the entity.

(4) What use or other action will be taken with respect to the private information, which is the subject of the complaint, until the complaint

is satisfactorily resolved.

g) If the Web site uses cookies, disclose how cookies are used and the consequences, if any of an individual's refusal to accept a cookie.

2. Describe who is responsible for controlling these activities.

3. Has the entity changed its business practices or the related disclosures in the last ninety days? If so, describe the nature of such changes and when each change occurred.

B. Where there are local, national, or other laws or requirements affecting business terms and conditions (for example, consumer protection rights and "lemon laws")?

1. Describe the entity's policies and procedures to provide reasonable assurance that it complies with such laws and requirements.

2. Where required by such laws and requirements, describe how appropriate disclosures provided to the customer.

C. Describe the entity's process for monitoring customer claims and complaints and for identifying patterns of claims and complaints that are not being satisfactorily addressed.

D. Describe the processes management uses to monitor the continuing effectiveness of its disclosure of business practices to provide reasonable assurance that—

1. The e-commerce transactions it executes are in accordance with its disclosed business practices.

2. Its business practice disclosures on its Web site remain current and continue to meet the WebTrust Criteria.

3. Reports of noncompliance are promptly addressed and corrective measures taken.

E. Describe how the foregoing disclosures are presented on the Web site.

III Transaction Integrity Controls

Principle - ***The entity maintains effective controls to provide reasonable assurance that customers' orders placed using e-commerce are completed and billed as agreed.***

A. Steps taken to ensure the integrity of e-commerce transactions

1. Describe the controls maintained by the entity to ensure the integrity of e-commerce transactions by explaining the following:

   a) How the entity provides reasonable assurance that—

   (1) Each request for transaction is checked for accuracy and completeness.

   (2) Positive acknowledgement is received from the customer before the transaction is processed.

   b) How the entity provides reasonable assurance that—

   (1) The correct goods are shipped in the correct quantities in the time frame agreed.

   (2) Services and information are provided to the customer as agreed to in the transaction.

   (3) Transaction exceptions (for example, back orders and other exceptions) are promptly communicated to the customer.

   c) How the entity provides reasonable assurance that—

   (1) Sales prices and all other costs/fees are displayed for the customer before requesting acknowledgment of the transaction.

   (2) Transactions are billed and electronically settled as agreed.

   (3) Billing or settlement errors are promptly corrected.

   d) How the entity maintains controls that allow for subsequent follow-up of transactions.

2. Describe who is responsible for controlling these activities.

3. Has the entity changed its controls over transaction integrity in the last 90 days? If controls over transaction integrity have changed, describe the nature of such changes and when each change occurred

B. Describe the processes management uses to monitor the continuing effectiveness of its controls over transaction integrity to provide reasonable assurance that—

1. Its transaction integrity controls remain effective.

   a) Its transaction integrity controls continue to meet the WebTrust Criteria.

   b) Reports of noncompliance are promptly addressed and corrective measures taken.

IV Information Protection Controls

Principle - ***The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce is protected from uses not related to the entity's business.***

In this context, private customer information includes personal identification information to the customer or his or her family (name, address, telephone number, social security/insurance or other government identification numbers, employer, credit card numbers, etc.), personal or family financial information, personal or family medical information, employment history, history of purchases or other transactions, credit records or similar information.

A. Description of the controls over the collection of data

1. Describe the policies and controls which provide customers with a choice to whether individually identifiable information collected from them online may be used for purposes other than completing the transaction in progress (an internal secondary use or external third party use).

2. Describe the controls allowing the opportunity to opt out of any particular internal secondary or external third party usage of that information except those required by law or regulatory agency

B. Description of steps taken to ensure the protection of private customer information.

1. Describe the controls maintained by the entity to protect transmissions of private customer information over the Internet from unintended recipients.

2. Describe the controls maintained by the entity to protect private customer

information obtained as a result of e-commerce and retained in its system from outsiders, as follows.

a) How systems that retain private customer information obtained as a result of e-commerce are protected from unauthorized outside access.

b) How the entity ensures that customers entering through the Web page cannot access other customers' private information (meaning, they can only perform inquiries, execute transactions, and obtain information about their own transactions).

c) How private customer information obtained as a result of e-commerce is protected from intentional disclosure to parties not related to the entity's business unless one of the following occurs.

(1) Customers are clearly notified prior to their providing such information.

(2) Customer permission is obtained after the customer has provided such information.

d) How the entity ensures that private customer information obtained as a result of e-commerce is used by employees only in ways associated with the entity's business.

3. Describe the controls maintained by the entity to protect against its unauthorized access to customer's computers and its unauthorized modification of customer's computer files, as follows.

a) Describe how the entity ensures that customer permission is obtained before storing, altering or copying information in the customer's computer (including the use of "cookies" stored on the customer's computer system) or that the customer is notified with an option to prevent such activities.

b) Describe how the entity ensures that transmission of malicious computer code (for example, viruses) to customers is prevented.

4. Who is responsible for controlling these activities?

5. Has the entity changed its controls over information protection in the last ninety days? If so, describe the nature of such changes and when each change occurred.

6. Describe the controls the entity maintains to ensure that individually identifiable information collected, created or maintained by it is accurate and complete for its intended use.

7. Describe the controls the entity maintains to determine the integrity and security policies of third party service providers to whom information is transferred as part of an outsource arrangement (if any).

C. Describe the processes management uses to monitor the continuing effectiveness of its controls over information protection to provide reasonable assurance that—

1. Its information protection controls remain effective.

2. Its information protection controls continue to meet the WebTrust Criteria.

3. Reports of noncompliance are promptly addressed and corrective measures taken.

V Change Management and CPA/CA Notification

A. Description of the Change Management Process

1. Describe the entity's controls over changes to its electronic business practices, its transaction integrity controls, its information protection controls, and its e-commerce systems and supporting technology, which are designed to provide reasonable assurance that—

   a) All such changes are approved by management.

   b) Changes in business practices are reflected in modified disclosures of such practices.

   c) Changes in the manner in which e-commerce transactions are executed are reflected in modified business practice disclosures.

   d) Modified business practice disclosures continue to conform to the WebTrust Criteria.

   e) Controls over transaction integrity and information protection continue to function effectively and to conform to the WebTrust Criteria.

B. Description of the Process to be Used to Notify CPA or CA of Changes

1. Describe the entity's policies and procedures to notify the CPA or CA in

advance of making changes to the following:

a) E-commerce activities

b) E-commerce systems and supporting technology

c) Business practices and disclosures of business practices

d) Controls over transaction integrity

e) Controls over information protection

f) Monitoring procedures over the foregoing

g) Control environment

2. Who is responsible for notifying the CPA or CA of such changes?

3. Has the entity changed those controls, procedures, or responsibilities designed to provide reasonable assurance that the CPA or CA is notified of all relevant changes in the last three months? If so, describe such changes and when each was made.

VI Other Matters

A. Describe below any other matters that would be relevant to the CPA or CA in evaluating the Web site's conformity with the WebTrust Criteria. Examples might include the following:

1. Significant changes in the entity's business or its organizational structure

2. Significant problems in meeting demand for its goods and services, meeting its customer commitments or continuing its historical level of customer satisfaction (for example., as might be evidenced by unusual levels of customer complaints).

3. Significant processing or controls problems with the entity's e-commerce systems or supporting infrastructure.

4. Instances of fraud and breaches of transaction integrity, security and information protection controls involving the following:

a) Employees with e-commerce responsibilities

b) Contractors and others who provide services to the entity related to its e-commerce activities

c) Unauthorized third parties

d) Systems and supporting infrastructure used for executing e-commerce transactions.

5. Significant changes in management and other key personnel with e-commerce responsibilities.

6. Significant changes in legal or regulatory requirements affecting the entities business or the operation of its Website

7. Other relevant information.

Engagement Letter

[Date]

To the Board of Directors

[Company]

[Address]

[City, State Zip Code]

This letter is to confirm our understanding of the terms and objectives of the engagement and the nature and limitations of the services we will provide.

We will perform the following services:

We will examine the Web site of ABC Company as and for the period _______, 20XX through _______, 20XX, in accordance with standards established by the American Institute of Certified Public Accountants ("AICPA"). The Purpose of this examination is to examine ABC Company's Web site and determine whether ABC Company's management's assertions related thereto are fairly stated, in all material respects, based on the AICPA/CICA WebTrust Principles and Criteria. This assurance service will consist of inquiries of company personnel and review of company policies and procedures as they relate to electronic commerce. Our procedures will include obtaining an understanding of the company's internal controls and testing these controls to the extent we feel necessary. This engagement cannot be relied upon to disclose errors or illegal acts, including fraud or defalcations, that may exist. In addition, this engagement will result in no warranty or assurances regarding the goods or services you provide. Any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time [such as to accommodate dates in the year 2000], may alter the validity of such conclusions.

Our engagement is to provide assurance on the company's electronic commerce business processes. However, we will inform you of any material errors, fraud, or illegal acts that come to our attention during the course of our work.

This engagement will result in the issuance of our report that management's assertions are fairly stated, in all material respects, based on the WebTrust Principles and Criteria. If the report issued is unqualified, you will be awarded the right to obtain the WebTrust seal for your Web site following your application for and receipt of a Special Class 3 Certificate from the certification authority designated by the AICPA pursuant to a subscriber agreement. You must comply with all the terms of this subscriber agreement. Also, you agree to provide a consumer recourse program as outlined in the current WebTrust Principles and Criteria for eCommerce transactions occurring at your site.

The WebTrust seal is a symbolic representation to viewers of your Web site that your Web site has met the WebTrust Principles and Criteria and has received an unqualified report. This seal is intended solely for the use by the management of ABC Company on the Web site for which the assurance service was performed and may only be displayed on appropriate pages of your Web site as we instruct. This seal may not be copied, reproduced, or distributed. If, for any reason, we are not able successfully to complete our procedures or the criteria are not met, the seal will not be delivered.

In addition to the WebTrust seal and the certification mark included therein, the AICPA/CICA own rights in various trademarks and service marks used in connection with the WebTrust Program, such as WEBTRUST and CPA WEBTRUST. This engagement will not give you any right to use these additional marks or to make any use of the certification mark or WebTrust seal other than as permitted on your Web site.

The WebTrust seal will be displayed on your Web site using a digital certificate provided by a certification authority. The seal will hypertext ("hot") link to our unqualified report and the following other information concerning the WebTrust Program: the WebTrust Principles and Criteria at <http://www.aicpa.org/webtrust/princrit.htm>, Management's disclosures of business practices for electronic commerce; and Management's assertions.

The digital certificate and WebTrust seal delivered by the certification authority will be valid for one year, after which you will need to obtain a new digital certificate. However, your right to display the WebTrust seal will depend on your continued compliance with the WebTrust Principles and Criteria as confirmed by periodic testing resulting in the issuance of new unqualified accountant's reports. For your Web site, periodic testing and issuance of new unqualified reports will be required every ________ (___) months (based on the nature and complexity of your Web site. **[NOTE: in NO event may the periodic testing period exceed three (3) months].**

You will notify us in advance in the event that you make changes to your electronic commerce activities, including: changes to your electronic commerce controls, practices and disclosures or the manner in which you comply with the WebTrust Principles and Criteria; changes in the nature of the products, information, or services you offer through electronic commerce (e.g., new product lines, etc.), or changes in the system used to support your electronic commerce. In such event, we shall have the right to perform additional procedures, at your expense, to determine whether your Web site continues to meet the WebTrust Principles and Criteria and to issue an updated Unqualified Report; if we are unable to perform such additional procedures (for whatever reason), we shall have the option of declaring for this purpose that your Web site no longer meets the WebTrust Principles and Criteria. Your failure to notify us in advance of changes in your electronic commerce activities may result in the revocation of your unqualified accountant's report and your continued right to use the WebTrust seal.

In the event that changes such as those noted above have been made without communication to us, or an examination of the Web site has not been made within _______ (___) months of the issuance of the previous unqualified accountant's report, or we become aware of false or misleading information contained within the Web site, which has not been corrected by management, we may unilaterally revoke our accountant's report and your continued right to use the WebTrust seal. You agree that, upon expiration of our unqualified report and/or the Subscriber Agreement or if the AICPA or we advise you that we have reason to believe your Web site no longer meets the WebTrust Principles and Criteria, you shall immediately remove the WebTrust seal from your Web site. You acknowledge that your failure to remove the WebTrust seal from your Web site upon request from us or the AICPA will irreparably harm the AICPA and give it the right to seek an immediate court order requiring you to remove the seal from your site.

We plan to begin your WebTrust engagement on ______, 20XX, and to complete our work on ______, 20XX. As discussed above, we will begin to update our testing procedures to ensure continued compliance with the WebTrust Principles and Criteria _______ (___) months from the issuance of our initial accountant's report.

We will respect the confidentiality of the information you provide in connection with this engagement; however, by agreeing to this engagement, you also consent to a review of the documents and work papers generated or accumulated in connection with this engagement for quality control purposes by individuals or firms designated by Firm or the owner or licensees of the Certification Mark and Related Marks.

At the conclusion of this engagement and prior to the issuance of our report, ABC management must provide us with a representation letter describing its responsibility for disclosing its business practices for electronic commerce transactions, for executing its electronic commerce transactions in accordance with its disclosed business practices, for maintaining adequate internal control structures as they relate to your Web site and for ensuring that it follows the WebTrust Principles and Criteria. This letter will also attest to the completeness and truthfulness of the representations and disclosures made to us during the course of our work.

Our report is presently expected to read as follows:

Independent Accountants' Report

To the Management of ABC Company, Inc.:

We have examined the assertion by the management of ABC Company, Inc. (ABC) that:

"on its Web site for electronic commerce at <www.abc.com> during the period August 1, 2001 through October 31, 2001, ABC:

- disclosed its business and privacy practices for electronic commerce transactions and executed transactions in accordance with its disclosed business and privacy practices,
- maintained effective controls to provide reasonable assurance that customers' orders placed using electronic commerce were completed and billed as agreed, and
- maintained effective controls to provide reasonable assurance that private customer information was protected from uses not related to ABC's business

in conformity with the AICPA/CICA *WebTrust* Principles and Criteria [hot link]."

ABC's management is responsible for its assertion [hot link to management's assertion]. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was made in accordance with standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance that management's assertion is not materially misstated.

Our examination included (1) obtaining an understanding of ABC's electronic commerce business practices and its controls over the processing of electronic commerce transactions and the protection of related private customer information, (2) selectively testing transactions executed in accordance with disclosed business practices, (3) testing and evaluating the operating effectiveness of the controls, and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Also, projections of any evaluation of controls to future periods are subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, ABC management's assertion for the period August 1, 2001 through October 31, 2001 is fairly stated, in all material respects, based on the AICPA/CICA WebTrust Principles and Criteria.

The CPA WebTrust seal of assurance on ABC's Web site for electronic commerce constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

This report does not include any representation as to the quality of ABC's goods or services nor their suitability for any customer's intended purpose. Furthermore, any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time [such as to accommodate dates in the year 2000], may alter the validity of such conclusions.

[Name of CPA firm]

Certified Public Accountants

[City, State]

[Date of report]

Request of Arbitration Representation

Arbitration Firm is Requested to Furnish Information

[Client Letterhead]

Date

Name/Address of Arbitration Organization

Our accountants, [name and address], are conducting a WebTrust examination as of [date] and for the [period] then ended. Please furnish directly to them the information requested below involving matters as to which you have been engaged and to which you have devoted attention in the form of arbitration or mediation services.

Please prepare a description of all material pending or threatened arbitration claims, and assessments. Materiality for purposes of this letter includes items involving amounts exceeding $___________ individually or in the aggregate. The description of each case should include the following information:

- nature of the arbitration case
- progress of the case to date
- how management of [name of client] is responding or intends to respond

Also, please identify any pending claims or assessments that have not had any case work performed.

Our accountants plan to have completed the WebTrust examination on [date]. And would appreciate receiving your reply by that date with a specified effective date no earlier than [date].

Should you require additional clarification on this matter, please contact our accountants directly at: [address, telephone and contact].

Very truly yours,

[Signature]

[Name of client]

Management Representation Letter

[Date of Accountants' Report]

To [accountant/accounting firm]:

In connection with your examination of the electronic commerce business processes of [name of client] as of [date] for the purpose of expressing reasonable assurance that the principles of WebTrust as published by the American Institute of Certified Public Accountants (CICA) are being followed, we confirm to the best of our knowledge and belief, the following representations made to you during your examination.

1. Specifically, we represent that—

   a) The company's business practices are followed consistently and as disclosed to the accountant.

   b) There have been no changes in the company's business practices during the period of review, or since the last review.

   c) There are no violations or possible violations of laws or regulations whose effects should be considered as to their effect on the transaction of electronic commerce.

   d) The company has complied with all contractual agreements that would have a material effect on the transaction of electronic commerce.

   e) There have been no breeches to the security of the website.

   f) Management subscribes to and follows WebTrust Principles.

   g) We represent that the business practices disclosures for www.abc.com are current, accurate, and complete and have been on our website since July 1, 199X.

   h) We have disclosed to you all organizations to whom we sell our customer data base information

2. In addition we agree to:

   - Permit you to conduct subsequent examinations at such times as you may deem appropriate, but not to exceed three months from the date of this report

   - Maintain our electronic commerce controls, practices and disclosures

- Notify you regarding changes affecting our electronic commerce activities, including:
  - Changes to our electronic commerce controls, practices, and disclosures or the manner in which they achieve the WebTrust Electronic Commerce Principles
  - Changes in the nature of the products, information, or services we offer through electronic commerce
  - Changes in the system(s) we use to support electronic commerce

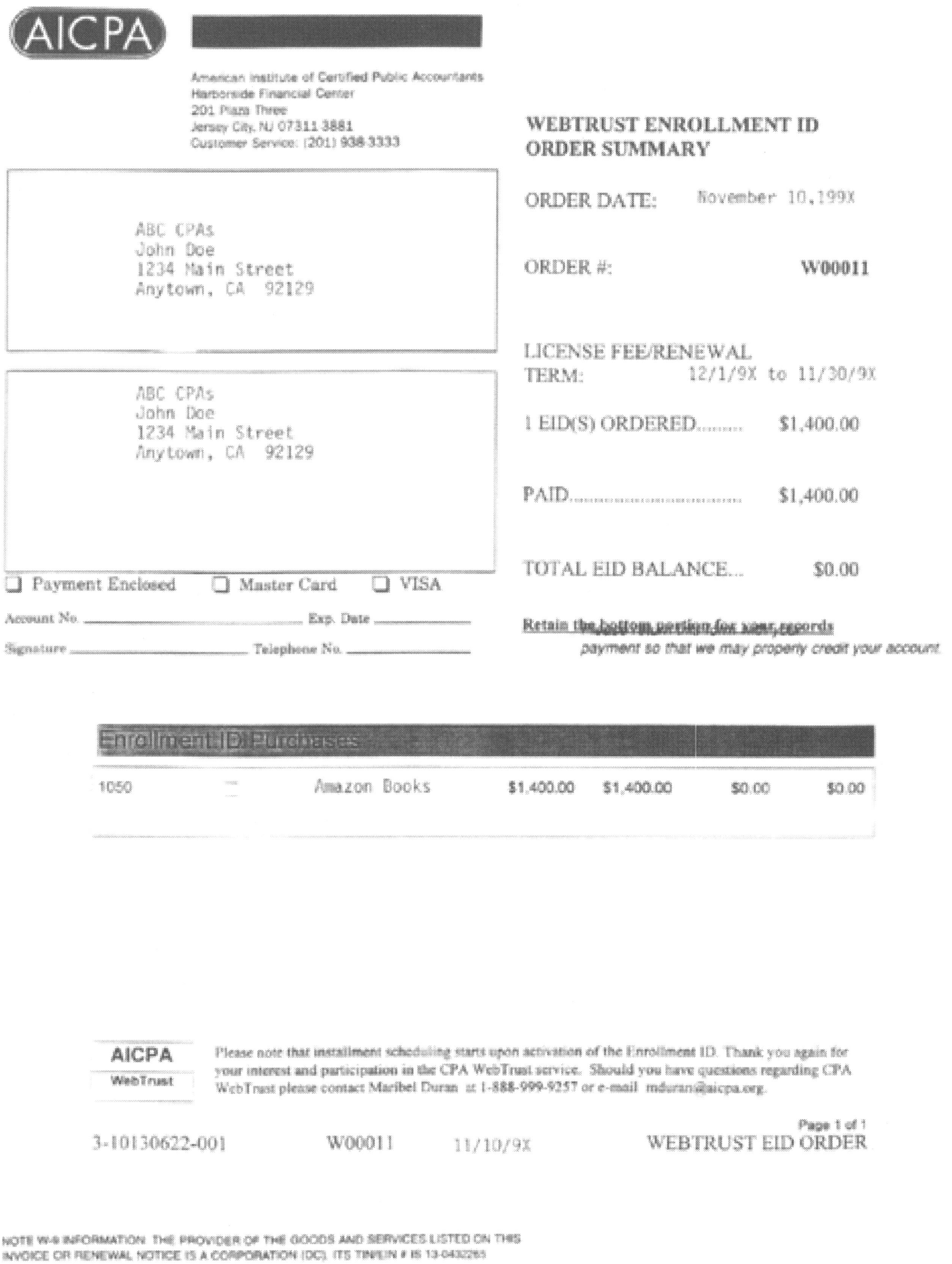
3. We also agree to permit you to unilaterally remove the WebTrust Seal if:
   - You find that changes, such as those above, have been made but not communicated to you by us
   - A subsequent examination has not been made within ____ days for any reason
   - During the course of performing the engagement you discover that changes we have made result in practices that no longer meet the WebTrust Principles

1. We have advised you of all actions taken at meetings of stockholders, board of directors, and committees of the board of directors (or other similar bodies, as applicable) that may affect our transacting business electronically.
2. We have responded fully to all inquiries made to us by you during your examination.
3. We understand that this engagement is not intended to examine our system(s) for the year 2000 problem and that you have provided no assurance on the system(s) in that regard.

Name of owner, CEO or other Officer & title

[Date]

EID Number and Documentations from the AICPA



AICPA

American Institute of Certified Public Accountants
Harborside Financial Center
201 Plaza Three
Jersey City, NJ 07311 3881
Customer Service: (201) 938 3333

WEBTRUST ENROLLMENT ID
ORDER SUMMARY

ABC CPAs
John Doe
1234 Main Street
Anytown, CA 92129

ABC CPAs
John Doe
1234 Main Street
Anytown, CA 92129

ORDER DATE:	November 10,199X
ORDER #:	**W00011**
LICENSE FEE/RENEWAL TERM:	12/1/9X to 11/30/9X
1 EID(S) ORDERED........	$1,400.00
PAID...............................	$1,400.00
TOTAL EID BALANCE...	$0.00

□ Payment Enclosed □ Master Card □ VISA

Account No. ________________ Exp. Date __________

Signature ________________ Telephone No. __________

Retain the bottom portion for your records
payment so that we may properly credit your account

Enrollment ID Purchases

1050	–	Amazon Books	$1,400.00	$1,400.00	$0.00	$0.00

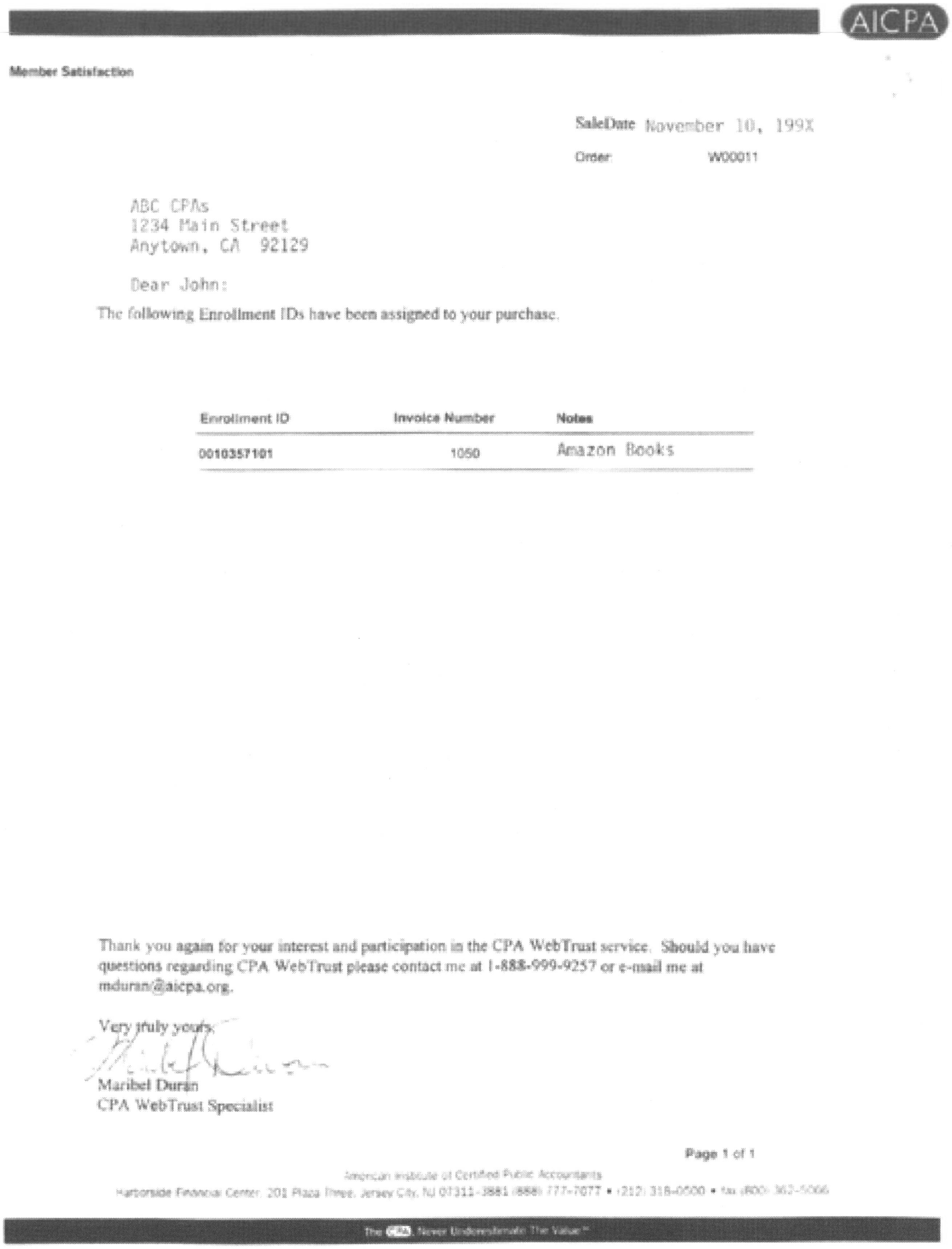
AICPA
WebTrust

Please note that installment scheduling starts upon activation of the Enrollment ID. Thank you again for your interest and participation in the CPA WebTrust service. Should you have questions regarding CPA WebTrust please contact Maribel Duran at 1-888-999-9257 or e-mail mduran@aicpa.org.

Page 1 of 1

3-10130622-001 W00011 11/10/9X WEBTRUST EID ORDER

NOTE W-9 INFORMATION: THE PROVIDER OF THE GOODS AND SERVICES LISTED ON THIS INVOICE OR RENEWAL NOTICE IS A CORPORATION (DC). ITS TIN/EIN # IS 13-0432265



AICPA

Member Satisfaction

SaleDate November 10, 199X

Order: W00011

ABC CPAs
1234 Main Street
Anytown, CA 92129

Dear John:

The following Enrollment IDs have been assigned to your purchase.

Enrollment ID	Invoice Number	Notes
0010357101	1050	Amazon Books

Thank you again for your interest and participation in the CPA WebTrust service. Should you have questions regarding CPA WebTrust please contact me at 1-888-999-9257 or e-mail me at mduran@aicpa.org.

Very truly yours,

Maribel Duran
CPA WebTrust Specialist

Page 1 of 1

American Institute of Certified Public Accountants
Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311-3881 (888) 777-7077 • (212) 318-0500 • fax (800) 362-5066

The CPA. Never Underestimate The Value.™

WebTrust Supervision, Review and Approval

Client: ______________________________

Closing date: ____________________ URL: ____________________

This form should be completed as the last step before issuing a WebTrust report and seal. Any items answered "no" should be fully explained and attached as a part of this form.

	Yes	No	N/A
Detailed Review Performed by the staff in charge of fieldwork			
I have reviewed all work papers prepared by the personnel in my charge on this engagement. Each schedule is complete, properly headed, initialed, indexed, and cross-referenced			
I have reviewed all other files (permanent, general) as necessary. All relevant information has been used or cross-referenced.			
I have compared the work performed as evidenced by our work papers with the procedures indicated in the work program and find that our examination complies with the requirements of the work program.			
I have compared the work papers with management's assertions for WebTrust and find satisfactory attest consideration has been given to all of the WebTrust Principles and Criteria.			
I have reviewed the completed work program and am satisfied that our examination was done in accordance with AICPA/CICA attest standards, and that:			
All conclusions are supported by evidence obtained.			
There are no unresolved points in the work papers.			
I have reviewed the dispute resolution and management's representation letters for consideration of all important representations.			

Completed by: ______________________________

Date: ______________________________

WebTrust Supervision, Review and Approval (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

Partner Review Performed by the Engagement Partner

	Yes	No	N/A
I have reviewed all work papers prepared by the personnel in my charge on this engagement that were not a part of the detailed review process.			
I have also made a review of sufficient additional work papers to be satisfied with the adequacy of our examination and with the detailed review.			
I have reviewed the completed work programs and am satisfied that our examination, as evidenced by the work papers reviewed by me, was conducted in accordance with attest standards and the engagement arrangements with the client. And that:			
All conclusions are supported by evidence obtained.			
There are no unresolved points in the work papers.			
I have reviewed the dispute resolution and management's representation letters for consideration of all important representations.			
A summary memorandum, if necessary, has been prepared to explain any unusual technical issues, examination complications, opinions of specialists, and resolution of disagreements on technical issues between the personnel assigned on this engagement.			
I approve of our report and issuance of the WebTrust Seal			

Completed by: ______________________________

Date: ______________________________

Engagement Termination Letter

[Firm Letterhead]

Date

Name/address of client

As of [date], we will end our services as your accountants for the WebTrust engagement. We have not come to the decision easily, and after substantial discussions and deliberation with you and our firm's management, it is deemed necessary to take this step because:

- [We lack the expertise to continue with this engagement]
- [There have been severe limitations in our ability to obtain the needed information for this examination]
- [Of a lack of payment for services we have performed]
- [Other]

You should take immediate steps to address the reasons for our decision to withdraw from the engagement. If corrective measures are taken, we will consider working on this engagement again.

Should you wish to engage a new accountant we will assist the accountant in addressing any open items, subject to your payment of any outstanding invoices. To assist in this process, please provide to us a letter authorizing us to communicate with the new accountant regarding this engagement.

We look forward to resolving this (these) issue(s) in a professional manner. Should you require additional information or clarification, please feel free to contact us.

Very truly yours,

[Firm]

by [Engagement partner]

Mailing House Request

[Letterhead of Organization]

[Date]

[Mailing House & address]

Our accountants, [Name & Address], are conducting an examination of our website (www.abc.com) as of [date] and for the [period] then ended. Part of this examination is to verify to the accountants that customers from our site who have not given permission for their information to be sold to third parties, such as your company, has not been sold or provided to you. Please furnish directly to them from the information below involving our sale to you of our customer database. **[Note: do not include a street address, because this would give an opportunity to the mailing house to add the customer to their data base if it is not already part of their information. Also be sure to include both types of customers—those who have given permission and those who have not given permission for their private information to be distributed to other parties—in your sample.]**

Customer Name	Street	City	Zip Code	Included in Sample (Y/N)

Our accountants expect to have their examination completed on [date], and would appreciate receiving your reply by that date. If you anticipate any problems, please inform them no later than [date] so other procedures can be worked out.

Very truly yours,

[Signature]

[Title]

Engagement Acceptance

Instructions: Use this form to document acceptance and engagement consideration.

General Information:

Client name:

Address:

Year end:

Telephone:

Fax:

Domain name:

email:

Type of entity:

Description of client business:
(Include any specialized
treatment to be required)

Key company personnel:

If company is a new client, disclose if this engagement is a WebTrust only engagement. Identify the other firm and consider any problems that may have been left unresolved with the prior accountants:

Document any communication with prior or other accounting firm:

Engagement Acceptance (cont.)

Client: ____

Closing date: ________________________

Acceptance criteria:	Yes	No
1 There are no issues with client personnel, management, or officers with regard to integrity.	______	______
2 There are no unresolved issues with regard to independence or conflicts of interest, which may impair our independence.	______	______
3 There are no collection problems with the prior accountant (or our firm if this a new engagement).	______	______
4 The proposed engagement team expertise and capabilities is not beyond the team's capabilities.	______	______
5 There are no unresolved issues with prior accountants.	______	______
6 Will this engagement require additional firm tools or other resources not currently available?	______	______
7 The staffing and timing required by this engagement is not beyond the capabilities of the firm.	______	______
8 The electronic commerce carried on by this client does not place any undue risk to the firm.	______	______
9 There are no concerns regarding the Website's disclosures that do not relate to the WebTrust Principles & Criteria.	______	______
10 This engagement does not appear to cause any undue risk or exposure to the firm.	______	______

Note: A "yes" response does not disqualify the prospective engagement from being accepted. However, additional steps will need to be considered before proceeding with the engagement. Please explain any "yes" responses and consider any additional steps that should be taken to mitigate the situation.

____

____

____

Engagement Acceptance (cont.)

Client: ____________________

Closing date: ____________________

Explain how client was acquired (referral, advertising etc.): ____________________

____

Has a thank you been sent to the referral source? ____________________

Other: List any other items that should be considered in the acceptance of this client/engagement not previously listed: ____________________

____

____

____

____

____

____

____

Conclusion:

Engagement SHOULD ________ or SHOULD NOT ________ be accepted.

Engagement Partner: ____________________ Date: ____________

Review Partner: ____________________ Date: ____________

Summary WebTrust Work Program

Client: ______________________________

Closing date: ________________ URL: ________________

Assigned personnel:	Name	Initials
In charge		
Assistants		
Manager		
Partner		

Timing	Date Planned	Actual Date
Self-assessment document		
Delivered to client		
Discussed with client		
Planning		
Begin field work		
Complete field work		
Complete report and documentation		
Partner approval		
Deliver to client		

Approval:	By	Date
Estimated time		
Actual time		

Summary WebTrust Work Program (cont.)

Client: ____________________

Closing date: ____________________ URL: ____________________

	Reference	Date	Hours	Date	Hours
General					
Self-assessment document					
Engagement acceptance					
Client information worksheet					
General control environment worksheet					
Analytical procedures					
Transaction walk-through					
Self-monitoring worksheet					
Business Practices & Information Privacy					
Business and information privacy practices					
Privacy disclosures & policies					
Dispute resolution disclosures					
Legal & other regulatory issues					
Test of transactions					
Transaction Integrity					
Transaction integrity controls					
Order entry process worksheet					
Credit card evaluation worksheet					
Test of transactions					
Information Protection					
Information protection controls					
System(s) architecture worksheet					
Site security worksheet					
Firewall control evaluation worksheet					
Disaster recovery & physical access					
Test of transactions					
Change Management & Accountant Notification					
CPA notification of change process					

Summary WebTrust Work Program (cont.)

Client: ____

Closing date: ______________________ URL: ______________________

Other Items	Reference	Date	Hours	Date	Hours
Other matters worksheet					
ISP visit					
Report matters					
Client conferences					
Travel time					
Other:					
Cumulative total					

WebTrust Work Program

Client: ______________________________

Closing date: ________________ URL: ________________

Instructions: This checklist should be used for initial WebTrust engagements and the interim evaluations. After each procedure is completed it should be initialed by the in-charge accountant. If the procedure is deemed unnecessary, an "NA" should be placed on the appropriate line. Any additional steps or situations noted should be appended to this document.

Examination Objectives
The objectives in the general program are general in nature and not necessarily related to specific WebTrust assertions

General	N/A Performed by	Work paper Index
The examination has been properly planned.		
Information prepared by the client appears accurate.		
Written representations have been obtained from management.		
Reportable conditions, irregularities or illegal acts, and other matters related to the conduct of the examination have been communicated to the appropriate individuals or parties.		
Staff assistants have been properly supervised.		
Outside experts have had their credentials properly verified and have been properly supervised.		
Work papers have been reviewed in accordance with firm policies.		
Proper considerations have been given to independence, client acceptance and continuation, personnel assignment, consultation, and supervision.		
The self-assessment document has been completed.		
Other		

WebTrust Work Program (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

Planning

Perform the following planning steps before fieldwork begins:

If the entity is a new client:
Obtain assurance that the client meets firm standards, consider using Engagement Acceptance Form.

If this is a continuing client:
Determine whether there is any reason why there should be a reevaluation of continuance. (Consider items such as: changes in management, scope of the engagement, lack of firm expertise, etc.).

Determine whether there is any change in independence. Include a check for unpaid fees.

If specialists outside the firm will be engaged to perform portions of the engagement, obtain assurance in writing of their independence.

Ascertain or acquire the necessary knowledge concerning the client's industry and/or other technical skills required by the engagement.

As a practical consideration, the accountant may wish to request the following items before starting fieldwork:

Organization charts
Minutes of board meetings
Significant agreements or contracts relating to eCommerce
Contracts with outside service providers, specifically ISPs, hosting, etc.

Company's written policies regarding:
Privacy
Warranties and returns
Security
Disaster Recovery
Other

N/A Performed by	Work paper Index

WebTrust Work Program (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

	N/A Performed by	Work paper Index
Obtain an understanding of the client's eCommerce activities, its customers and systems (consider using Client Information Worksheet)		
Obtain an understanding of the client's control environment, hiring policies, and supervisor of company personnel (consider using Control Environment Worksheet)		
Apply preliminary analytical procedures by comparing account balances for the current period to similar amounts in the prior period (consider using Analytical Procedures Worksheet)		
Obtain an understanding of the controls used by the client to monitor its own practices, policies, and procedures (consider using Self-Monitoring Worksheet)		
Obtain an understanding of the client's order process as it relates to electronic commerce transactions (consider using Order Entry Worksheet)		
Execution		
Perform the following as a part of field work:		
Obtain a management representation letter (the letter should be dated as of the end of fieldwork)		
Obtain a sample of transactions for testing (consider using Transaction Walk-Through Worksheet)		
Ascertain whether there are adequate business disclosures from a sample of transactions and consider whether proper compliance with disclosed criteria is met (consider using the Business Practices Worksheet)		

WebTrust Work Program (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

N/A Performed by	Work paper Index

Ascertain whether there are adequate privacy disclosures from a sample of transactions and consider whether proper compliance with disclosed criteria is met (consider using the Privacy Policies Worksheet)

Ascertain whether there are adequate consumer dispute resolution disclosures from a sample of transactions and consider whether proper compliance with disclosed criteria is met (consider using the Dispute Resolution Worksheet)

Ascertain whether legal and other regulatory issues impact the commerce site and whether adequate disclosure has been given (consider using the Legal/Regulatory Worksheet)

Test the site's compliance with its own disclosures against a sample of transactions and consider whether proper compliance with disclosed criteria is met (consider using the Practices Test of Transactions Worksheet)

Obtain sufficient understanding as to the adequacy of the client's credit card processing system and consider its impact on the engagement (consider using Credit Card System Worksheet)

Test the site's compliance with its own controls over and procedures regarding transaction integrity for electronic commerce transactions (consider using Transaction Integrity Test of Transactions Worksheet)

Consider the adequacy of the site's information protection controls (consider using Information Protection Worksheet)

Obtain sufficient understanding of the site's layout and system architecture (consider using Site Security Worksheet)

WebTrust Work Program (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

	N/A Performed by	Work paper Index
Evaluate any weakness in the site's security and consider its impact on the engagement (consider using the Site Security Worksheet)		
Evaluate the site's firewall and corresponding configuration and consider its impact on the engagement (consider using Firewall Worksheet)		
Evaluate the site's overall disaster recovery program for electronic commerce transactions and consider its impact on the engagement (consider using Disaster Recovery Worksheet)		
Test the site's transactions against the disclosed practices and procedures for information protection and consider its impact on the engagement (consider using Information Protection Test of Transactions Worksheet)		
Consider the adequacy of the client's policies and procedures for monitoring changes, updates, and notification of the CPA/CA and evaluate the impact on the engagement (consider using Change Notification Worksheet)		
Consider other matters and their impact on the engagement (consider using Other Matters Worksheet)		
Ascertain that all open work paper items, "to dos" and other items have been completed and that any differences of professional opinion have been resolved		

WebTrust Work Program (cont.)

Client: ____

Closing date: ____________________ URL: ____________________

Seal Issuance

	N/A Performed by	Work paper Index
Obtain a copy of the management's assertions and ascertain if appropriate for seal issuance		
Obtain EID from the AICPA for obtaining the class 3 server certificate from VeriSign. EID Number: ____________________		
Have the Webmaster generate a certificate signing request (CSR) for the specific type of server used.		
Have client apply for a server certificate from VeriSign		
Prepare accountant's report		
Issue accountant's report to client		

Client Information Worksheet

Client: ______________________________

Closing date: ______________ URL: ______________

Describe the industries in which electronic commerce activities are occurring: ______

List any AICPA guides or other publications that are authoritative sources for the industry(s) in which the client operates and any specialized practices unique to this industry(s): ______

What goods, services, or information are being sold at the company website? ______

Who represents a typical customer? ______

What is the typical form of payment? ______

List the main members of management and their title: ______

List the location(s) of the company:

Main office: ______

Other office: ______

Server location: ______

Indicate how long the company has been involved with electronic commerce: ______

Describe any concentrations (major customers, suppliers, or seasonal periods): ______

Client Information Worksheet (cont.)

Client: ______________________________

Closing date: ______________ URL: ______________

Describe the information systems used for the electronic commerce transactions: ______________

Describe any contingency plans the client has in place should the system(s) used become damaged or not accessible: ______________

Describe any functions related to the eCommerce cycle that are outsourced to a third party:

Client Information Worksheet (cont.)

Client: ____________________

Closing date: ____________________ URL: ____________________

Describe any steps the client has taken to address the Year 2000 issue: ____________________

____

____

____

____

____

____

____

____

____

____

Completed by: ____________________ Reviewed by: ____________________

Date: ____________________ Date: ____________________

General Control Environment Worksheet

Client: ____________________

Closing date: ____________________ URL: ____________________

Describe the factors that contribute to a control environment and are generally conducive to reliable business practices and policies:

Managements "tone at the top": ____________________

Hiring, development, and retention of competent personnel: ____________________

Emphasizing the importance and responsibilities of sound business practices and effective control: ____________________

Supervising business activities and control procedures: ____________________

General Control Environment Worksheet (cont.)

Client: ______________________________

Closing date: ______________________ URL: ______________________

Employing a suitable internal auditing or other internal reporting mechanism that periodically audits matters related to eCommerce activities: __________

____
____
____
____
____

Other factors: ______________________________

____
____
____
____
____
____

Completed by: ______________________ Reviewed by: ______________________

Date: ______________________ Date: ______________________

Analytical Procedures

Client: ____________________

Closing date: ____________________ URL: ____________________

Instructions: The following ratios can be used in the evaluation of a client site and should not be computed just for the exercise. Choose the ratios that will provide the most meaningful information under the circumstances and add others where appropriate.

	Period 1	Period 2	Period 3
Trend Analysis			
$\frac{\text{eCommerce Sales}}{\text{Total Sales}}$			
* $\frac{\text{Warranty Expense}}{\text{eCommerce Sales}}$			
* $\frac{\text{Returns}}{\text{eCommerce Sales}}$			
Profitability Inventory turnover			
$\frac{\text{Cost of Sales}}{\text{Average Inventory}}$			
Return on net sales			
$\frac{\text{Net Income}}{\text{Net Sales}}$			
Quick Ratio			
$\frac{\text{Current Assets}}{\text{Current Liabilities}}$			

Completed by: ____________________ Reviewed by: ____________________

Date: ____________________ Date: ____________________

* From eCommerce sales

Transaction Walk-Through

Client: ______________________________

Closing date: ____________________ URL: ______________

Order number	Order date	Customer ack. of order	email confirm to customer	Date Shipped	Agree w/support	Date billed	Agree w/support	Backorder notified

Note: Be sure to include some backorder information in the sample to be tested. Use additional sheets if necessary.

Possible sources of information:

Customer order
Shipping documentation
Billing information

Self-Monitoring Worksheet

Client: ____

Closing date: ______________________ URL: ______________________

Describe the process management uses to monitor the effectiveness of its own business practices and information privacy policies, specifically to provide reasonable assurance that --

> The eCommerce transactions are performed in accordance with disclosed practices.
> Its disclosures at the website remain current and continue to fulfill WebTrust Criteria.
> Reports of noncompliance are promptly addressed and corrected.

____
____
____
____
____
____
____
____
____
____
____
____

Describe the process management uses to monitor the effectiveness of its control for transaction integrity, specifically to provide reasonable assurance that --

> Transaction integrity control continues to meet WebTrust Criteria.
> Reports of noncompliance are promptly addressed and corrected.

____
____
____
____
____
____
____
____
____
____
____
____

Self-Monitoring Worksheet (cont.)

Client: ____________________

Closing date: ____________________ URL: ____________________

Describe the process management uses to monitor the effectiveness of its controls over information protection, specifically to provide reasonable assurance that --

> Information protection controls remain effective/current.
> Information protection controls continue to meet WebTrust Criteria.
> Reports of noncompliance are promptly addressed and corrected.

Business Practices Disclosures & Information Privacy Disclosures

Client: ____________________

Closing date: ____________________ URL: ____________________

Instructions: Describe the disclosures related to the WebTrust Principles and Criteria from the client web site. In the date column, put the date the disclosure was added/changed at the web site.

Descriptive information about the nature of the goods that will be shipped or the services that will be provided.

Date

Condition of the goods -- new, used, or reconditioned: ____________________

Description of the services to be rendered (or service contract):

Source of information sold (where obtained or how compiled):

Other relevant descriptive information: ____________________

Sources for verification of the preceding information:
Supplier invoices
Personal observation of inventory
Customer contract
Engagement letter/service contract

Business Practices Disclosures & Information Privacy Disclosures (cont.)

Client: ______________________________

Closing date: ______________ URL: ______________

Date

Time frame for order fulfillment: ______________

Time frame for informing customer of backorder or other order exceptions:

Normal delivery and any customer options: ______________

Customer payment methods and options: ______________

Procedure to allow customer to cancel any recurring charges:

Return policies: ______________

Business Practices Disclosures & Information Privacy Disclosures (cont.)

Client: ____

Closing date: ______________________ URL: ________________________

Date

Other relevant terms and conditions: ______________________

____

____

____

____

____ ________________

Sources for verification of the preceding information:

Company sales processing policy
Company order processing policy
Warranty policy

Business Practices Disclosures & Information Privacy Disclosures (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

Where (on its web site or in information provided with the product) customers can obtain warranty service and support related to the goods and services purchased on its web site.

Date

Description of warranty disclosure: ____________________

____

____

____

____

______________________________ ____________

Information to enable customers to file claims, ask questions, and register complaints, including the following:

Street address: ____________________

______________________________ ____________

Telephone number (number to reach an employee in a reasonable amount of time -- not only a voice mail system): ____________________ ____________

Days/hours of operation: ____________________

______________________________ ____________

Other relevant information for customers: ____________________

____

____

____

____

______________________________ ____________

Sources for verification of the preceding information:
Direct observation at web site URL

Completed by: ____________________ Reviewed by: ____________________

Date: ____________________ Date: ____________________

Privacy Disclosures & Policies

Client: ______________________________

Closing date: ______________________ URL: ______________________

Descriptive information regarding the site's privacy policies. These practices should include (but not be limited to) the following disclosures:

Disclosure of the specific kinds and sources of information being collected and maintained: ________

Disclosure of the uses of collected information: ______________________

Disclosure of third-party distribution of information (if any): ______________________

Disclosure as to whether any choice is available to the customer regarding how information collected may be used or distributed: ______________________

Privacy Disclosures & Policies (cont.)

Client: ______________________________

Closing date: ____________________ URL: ______________________________

Disclosure of the consequences of an individual's refusal to provide specific information (if any): ______

Disclosure of how erroneous or incomplete information can be reviewed, changed, or removed: ______

Disclosure of how to resolve complaints related to accuracy, completeness, and distribution of customer information: ______________________________

Disclosure of the site's cookie policy including customer's refusal to accept a cookie: ____________

Sources for verification of the preceding information:
Direct observation at web site

Completed by: ____________________ Reviewed by: ____________

Date: ____________________ Date: ____________

Dispute Resolution

Client: ______________________________

Closing date: ____________________ URL: ____________________

Disclosure of the management's commitment to use a third-party dispute resolution service: ______

Identification of the third-party dispute resolution service: ______

Disclosure of the dispute resolution process (starting with the entity): ______

Disclosure of the action to be taken with regard to private customer information (if subject of the complaint) until the dispute is resolved: ______

Completed by: ______________ Reviewed by: ______________

Date: ______________ Date: ______________

Legal & Regulatory Issues

Client: ______________________________

Closing date: ____________________ URL: ____________________

Describe the local, national, or other laws or requirements affecting business terms and conditions (customer rights, and "lemon laws"):

Describe the entity's policies and procedures to provide reasonable assurance that it complies with such laws and requirements:

Describe the disclosures regarding such laws and requirements made to customers and visitors to the web site:

Completed by: ____________________ Reviewed by: ____________________

Date: ____________________ Date: ____________________

Business Practices Disclosures
Test of Transactions

Client: ______________________________

Closing date: ______________________ URL: ______________________

Instructions: From the information obtained in the "Transaction Walk-Through" evaluate the client's disclosures with the actual results.

Tested by Date

Time frame for order fulfillment

Exceptions noted ______________________

______________________ ______

Time frame for informing customer of backorder or other order exceptions:

Exceptions noted ______________________

______________________ ______

Normal delivery and any customer options:

Exceptions noted ______________________

______________________ ______

Customer payment methods and options:

Exceptions noted ______________________

______________________ ______

Procedure to allow customer to cancel any recurring charges:

Exceptions noted ______________________

______________________ ______

Business Practices Disclosures
Test of Transactions (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

Tested by ____________ Date ______

Return policies:

Exceptions noted ____________________

____

____

____

____________ ______

Other relevant terms and conditions:

Exceptions noted ____________________

____

____

____

____________ ______

Completed by: ____________________ Reviewed by: ____________

Date: ____________________ Date: ____________

Transaction Integrity Controls

Client: ______________________________

Closing date: ______________ URL: ______________

Instructions: Describe the controls related to the WebTrust Principles and Criteria from the client web site.

Describe the controls maintained by the entity to ensure the integrity of electronic commerce transactions

Order entry stage

Describe the client controls in place to provide assurance that:

Each order is checked for accuracy and completeness ______________

Sale prices and all other costs are displayed for the customer before processing ______

Customer gives a positive acknowledgement BEFORE order is processed ______

Transaction Integrity Controls (cont.)

Client: ____

Closing date: ____________________ URL: ____________________

Shipping stage

Describe the client's controls in place to provide assurance that:

The correct goods are shipped in the correct quantities in the time frame agreed

Services and information are provided to the customer as agreed on the order

Backorder and other exceptions are communicated to the customer as disclosed

Transaction Integrity Controls (cont.)

Client: ______________________________

Closing date: ______________ URL: ______________

Billing and Accounting Stage

Describe the client's controls in place to provide assurance that:

Orders are billed and settled as disclosed/agreed ______________

Billing or settlement errors are (or can be) quickly corrected ______________

Follow-up on prior orders can be performed ______________

Completed by: ______________ Reviewed by: ______________

Date: ______________ Date: ______________

Order Entry Process

Client: ______________________________

Closing date: ____________________ URL: ____________________

The purpose of this form is to assist the accountant in documenting the order entry process.

Describe how customer identifies him/herself on the web site ____________________

____

____

____

Describe the process by which a customer places an order. Items included (but not limited to): CGI scripts, encryption, shopping cart utilization. ____________________

____

____

____

____

____

____

____

Describe interface between the web site and the company order-processing system (e.g., manual, etc.)

____

____

____

____

____

____

____

Describe the company process for customer notification/confirmation of an order ____________

____

____

____

Completed by: ____________________ Reviewed by: ____________________

Date: ____________________ Date: ____________________

Credit Card System Evaluation

Client: ____

Closing date: ______________________ URL: ______________________

Credit card processing system used by client:

Merchant bank used by client and history with system:

Describe the credit card processing procedure:

Credit Card System Evaluation (cont.)

Client: ______________________________

Closing date: __________________ URL: __________________

	Yes/No
The web site does not store credit card information on the customer computer -- or if it does the information is encrypted.	________
The web site does not store credit card information on the company's computer -- or if it does the information is encrypted or is not displayed to those without proper access.	________
Credit card information is purged at the conclusion of the specific transaction -- BEST PRACTICES.	________
Customer credit card numbers are validated either online with a merchant bank or by using the check-digit test.	________
The system allows for credits to be posted.	________
When a credit is posted special access or other control is used to assure that credits are being processed for the correct accounts and transactions.	________
The credit card system allows for customer charge backs that follow similar procedures and controls for customer credit posting.	________

Explain any "no" answers and evaluate the materiality of a "no" on the integrity of the system:

____

____

____

____

____

Completed by: __________________ Reviewed by: __________________

Date: __________________ Date: __________________

Transaction Integrity Controls
Test of Transactions

Client: ______________________________

Closing date: ____________________ URL: ____________________

Instructions: From the information obtained in the "Transaction Walk-Through" evaluate the client's disclosures with the actual results.

Tested by Date

Each order is checked for accuracy and completeness

Exceptions noted ____________________

____

____

____

____

Sales prices and all other costs are displayed for the customer before processing

Exceptions noted ____________________

____

____

____

____

Customer gives a positive acknowledgement BEFORE order is processed

Exceptions noted ____________________

____

____

____

____

The correct goods are shipped in the correct quantities in the time frame agreed

Exceptions noted ____________________

____

____

____

____

Transaction Integrity Controls
Test of Transactions (cont.)

Client: ____________________

Closing date: ____________________ URL: ____________________

Tested by Date

Services and information are provided to the customer as agreed on the order

Exceptions noted ____________________

Backorder and other exceptions are communicated to the customer as disclosed

Exceptions noted ____________________

Orders are billed and settled as disclosed/agreed

Exceptions noted ____________________

Billing or settlement errors are (or can be) quickly corrected

Exceptions noted ____________________

Follow-up on prior orders can be performed

Exceptions noted ____________________

Completed by: ____________________ Reviewed by: ____________________

Date: ____________________ Date: ____________________

Information Protection Controls

Client: ____

Closing date: ____________________ URL: ____________________

Instructions: Describe the controls related to the WebTrust Principles and Criteria from the client web site.

Describe the steps taken to ensure the protection of private customer information:

Transmission over the Internet
Describe the controls maintained by the entity to protect transmission of private customer information:

Information Protection Controls (cont.)

Client: ______________________________

Closing date: ________________ URL: ________________

Retained information

Describe how information obtained is protected from outside access: ________________

Describe the controls that ensure that customers entering the web site can only perform inquiries, execute transactions, and obtain other information about the customers' transaction:

Describe the controls that protect private customer information from intentional disclosure to the entity's private customer information: ________________

Information Protection Controls (cont.)

Client: ______________________________

Closing date: ______________ URL: ______________

Describe the controls maintained by the entity to protect private customer information from misuse by employees: ______________________________

Computer Access

Describe the controls maintained to protect against unauthorized access to the customers' computer and unauthorized access modification of customers' computer files: ______________

Information Protection Controls (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

Describe the controls the client has in place to ensure that permission is obtained before storing, altering, or copying information from the customer's computer (including "cookies"):

Describe the controls the client has in place to ensure that transmission of viruses TO the customer is prevented:

Describe the controls the client has in place to ensure that transmission of viruses FROM the customer is prevented:

Completed by: ____________________ Reviewed by: ____________________

Date: ____________________ Date: ____________________

Information Protection Controls
System Architecture

Client: ____

Closing date: ____________________ URL: ____________________

Instructions: This document will assist the accountant in understanding the client's system, software, and other peripherals as it relates to the overall security of the site.

Describe the server hardware (include CPU, memory, and peripherals): ____________________

Describe the router and firewalls used (include brand name, model, and version): ____________________

Describe the configuration of the server in relation to the firewall (e.g., Judas, Sacrificial Lamb, DMZ, etc.): __________

Information Protection Controls
System Architecture (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

Describe the software components of the system:

Operating system ____________________ Version ____________
Commerce software ____________________ ____________
HTML generator ____________________ ____________
Encryption ____________________ ____________
Firewall ____________________ ____________
Virus ____________________ ____________
Other ____________________ ____________
____________________ ____________
____________________ ____________

Yes/No

Are current versions of all software installed? ____________

Are current patches of all software installed? ____________

Is logging used on:
Web server ____________
Commerce server ____________
Firewall ____________
Error ____________
System ____________
Other ____________
____
____

Explain any "No" answer from above: ______________________________
____
____
____
____
____
____
____
____
____

Information Protection Controls
System Architecture (cont.)

Client: ____

Closing date: ______________________ URL: ______________________

Does the site use/have: ______________

SSL ______________

Digital certificates ______________

Credit card processing ______________

CGI scripting ______________

Perl scripting ______________

Active X ______________

Java ______________

Other applets (Describe) ______________

______________________ ______________

______________________ ______________

______________________ ______________

Completed by: ______________________ Reviewed by: ______________

Date: ______________________ Date: ______________

Site Security

Client: ______________________________

Closing date: ____________________ URL: ____________________

	Yes/No
Issues:	
Client has an established security policy	________
Transmission of plain text passwords over the network is prohibited	________
Security tools (COPS, Tripwire, etc.) are used regularly	________
Client has a policy to acquire/develop software that is free of bugs and security holes	________
Client has a policy to track current software for security holes, bugs and has applied all patches	________
Client has adequate system, firewall, and other logs	________
Client has adequate system and network monitoring	________

Policies:

Who is allowed access and their access level? ____________________

____

____

____

____

____

Who is accountable for security, upgrades, backups, and maintenance? ________

____

____

____

____

____

____

Site Security (cont.)

Client: ______________________________

Closing date: ______________ URL: ______________

What kind of material is allowed on server pages? ______________

Who has access to pages and data? ______________

What testing/evaluation is done on software, pages, scripts, etc., before they go "live"?

What is the policy to address complaints and requests concerning server and page content?

Site Security (cont.)

Client: ______________________________

Closing date: ________________ URL: ________________

What is the procedure for handling security incidents?

What is the process used to monitor, evaluate, and update the security policy?

Passwords:

What is the structure (length and character composition) of the password?

What is the life span of the password?

Site Security (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

Who is responsible for password setup? ____________________

What is the policy on passwords if the employee is terminated? ____________________

Monitoring Tools:

	Name/Version	Frequency Run
Snapshot tools (COPS, Tiger)		
Network tools (Tripwire, SATAN)		
Real time (Stalker, NetRanger)		

Site Security (cont.)

Client: ______________________________

Closing date: ______________ URL: ______________

Examine log files for connections from unusual locations or unusual activity.
Findings: ______________________________

Look for setuid and setgid files (UNIX only) everywhere on the system and delete unneeded copies.
Findings: ______________________________

Check system binaries to make sure they haven't been altered.
Findings: ______________________________

Check for unauthorized copies of network monitoring programs or packet sniffers and delete if found.
Findings: ______________________________

Check for unauthorized server services.
Findings: ______________________________

Site Security (cont.)

Client: ____

Closing date: ____________________ URL: ____________________

Check for unnecessary server services and eliminate.
Findings: ____

Examine the password file for unauthorized changes or modifications.
Findings: ____

Examine the system configuration files for unauthorized changes or modifications.
Findings: ____

Examine the entire system for hidden or unusual files and delete if necessary.
Findings: ____

Examine machines on the LAN when searching for signs of intrusion.
Findings: ____

Site Security (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

Consider the findings on the engagement and note any concerns for follow-up with the client.

Completed by: ____________________ Reviewed by: ____________________

Date: ____________________ Date: ____________________

Firewall Control Evaluation

Client: ______________________________

Closing date: ____________________ URL: ____________________

	Yes/No
IP packets are not passed between the two networks unless packets have the firewall system as their destination or origin	________
Firewall hides structure of internal network from outside network	________
Firewall provides for static routing only (no dynamic routing permitted)	________
Only OUTBOUND FTP, Mosaic, and Gopher on protected systems	________
User authentication does not rely solely on user ID/passwords	________
External FTP is prohibited	________
Services not required (rlogin, rwho, etc.) are turned off	________
External users are prohibited from logging in as root	________
The firewall rejects ALL unknown protocols	________
The firewall provides DNS services to outside network systems in the protected network	________
The firewall distinguishes between internal users (those coming from the internal network) and external users	________
The firewall is configured to exercise tighter control on functions that originate from external systems than those that originate from internal systems	________
The Telnet "open" command has been eliminated	________
The firewall is configured so that outgoing mail appears to come from the firewall	________
Only users who need access to/from the internal network have access controlled by user ID and passwords	________

Firewall Control Evaluation (cont.)

Client: ______________________________

Closing date: ________________ URL: ________________

	Yes/No
All nonrequired services have been deactivated	______
Firewall logs are configured to capture successful and unsuccessful attempts to use the system	______
The firewall is configured to verify that the Trusted Computing Base has not been modified	______
The firewall provides high levels of performance -- speed is limited by the LAN, not the firewall	______
Other	
______________________________	______
______________________________	______
______________________________	______

Explain any "no" answers and evaluate the materiality of a "no" on the integrity of the firewall

____

____

____

____

____

____

____

____

____

____

____

____

Completed by: ________________ Reviewed by: ________________

Date: ________________ Date: ________________

Disaster Recovery & Physical Access

Client: ______________________________

Closing date: ____________________ URL: ____________________

Note: This document is NOT intended to provide a comprehensive disaster recovery program. It is intended to provide guidance to the accountant. It is recommended that the accountant assist the client in developing a comprehensive disaster recovery program that includes eCommerce components.

Yes/No **Completed By**

Does the entity have a disaster recovery program? ____________________

Does the entity have a tape back-up system? ____________________

Is the entire system backed up daily? ____________________

Is the tape back-up done on a single tape? ____________________

Is there a tape rotation policy? ____________________

Are tape back-ups stored off-site? ____________________

Are tape back-ups tested (both read and write) monthly? ____________________

Are work stations logged out before the tape back-up routine? ____________________

Is there a complete listing of all critical hardware including configurations? ____________________

Are copies of all software stored in a protected cabinet? ____________________

Does the entity have a contingency plan in place to obtain needed hardware or infrastructure in case of emergency? ____________________

Does the entity have a current virus-scanning software? ____________________

Is the virus-scanning software updated at least monthly? ____________________

Are all work stations using a virus-scanning software? ____________________

Is all incoming media scanned for viruses before use? ____________________

Does the entity have an incident response policy? ____________________

Is physical access to critical hardware controlled? ____________________

Have off-site resources been identified? ____________________

Does the entity have a UPS system? ____________________

Does the entity have any equipment to protect against surges and spikes? ____________________

Does the entity have any redundant storage on its server(s)? ____________________

Disaster Recovery & Physical Access (cont.)

Client: ______________________________

Closing date: ______________________ URL: ______________________

Explain any "no" answers and evaluate its materiality on the engagement

Completed by: ______________________ Reviewed by: ______________________

Date: ______________________ Date: ______________________

Information Protection Controls
Test of Transactions

Client: ______________________________

Closing date: ______________ URL: ______________

Instructions: From the information obtained in the "Transaction Walk-Through" evaluate the client's disclosures with the actual results.

Tested by Date

Transmission over the Internet protects private customer information

Encryption or other method tested

Exceptions noted ______________

____

____

____

____

Site domain name and IP address verified

Exceptions noted ______________

____

____

____

____

Site's digital certificate verified

Exceptions noted ______________

____

____

____

____

Protection of information obtained

Packet filters are implemented Internet Gateway Routers using Access Control Lists (ACLs)

Exceptions noted ______________

____

____

____

____

Information Protection Controls
Test of Transactions (cont.)

Client: ________________________________

Closing date: ________________ URL: ________________

Tested by Date

Anti-spoof filters are used on the routers to prevent spoofing of trusted sources

Exceptions noted ________________

Commercial firewall properly configured and tested for possible security weakness

Exceptions noted ________________

Shared user IDs are prohibited

Exceptions noted ________________

All system level access to all production systems is provided via a strong identification and authentication mechanism

Exceptions noted ________________

User passwords on UNIX systems use a shadow file

Exceptions noted ________________

Information Protection Controls
Test of Transactions (cont.)

Client: ______________________________

Closing date: ______________________ URL: ______________________

Tested by Date

Protection from disclosure to third parties

Customers who decline permission to have information passed on to third parties are removed from the database before database is shared with third parties

Exceptions noted ______________________

____

____

____

____

Customer database is restricted to employees who have job functions that require access to the database

Exceptions noted ______________________

____

____

____

____

Employees are assigned only the privileges necessary to accomplish their tasks

Exceptions noted ______________________

____

____

____

____

Audit trails contain sufficient data for intrusion detection, after the fact investigations, and supports management response

Exceptions noted ______________________

____

____

____

____

Information Protection Controls
Test of Transactions (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

Tested by ________ Date ________

The identification and authentication audit trail identifies login time and logoff time

Exceptions noted ____________________

____

____

____

____________ ____________

System logon IDs are reviewed periodically for business need

Exceptions noted ____________________

____

____

____

____________ ____________

Suspicious activity is reported to system security officer (this could be an automated process)

Exceptions noted ____________________

____

____

____

____________ ____________

Access to/from customer's computer is controlled

Site requests the customer's permission before accessing the customer computer

Exceptions noted ____________________

____

____

____

____________ ____________

Information Protection Controls
Test of Transactions (cont.)

Client: ____

Closing date: ______________________ URL: ______________________

Tested by Date

Site has a "cookie policy" that it follows

Exceptions noted ______________________

____

____

____

____

All systems have current virus-scanning software installed that runs in active memory

Exceptions noted ______________________

____

____

____

____

Detected computer viruses are reported to the I Incident Response database.

Exceptions noted ______________________

____

____

____

____

All system software versions and patches are current

Exceptions noted ______________________

____

____

____

____

Hardware performance and capacity is performed to ensure optimal operation

Exceptions noted ______________________

____

____

____

____

Information Protection Controls
Test of Transactions (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

Tested by Date

Monitoring statistics for performance measures are analyzed in a timely manner

Exceptions noted ____________________

____

____

____

____

Monitoring software is used to detect system degradation and service availability

Exceptions noted ____________________

____

____

____

____

Completed by: ____________________ Reviewed by: ____________________

Date: ____________________ Date: ____________________

CPA Notification of Change

Client: ______________________________

Closing date: ____________________ URL: ____________________

Describe and document the client's policies and procedures regarding notification in advance of its:

Electronic commerce activities ____________________

Business practices and related disclosures of business practices ____________________

Controls over transaction integrity ____________________

Controls over information protection ____________________

CPA Notification of Change (cont.)

Client: ____

Closing date: ____________________ URL: ____________________

Describe and document the client's policies and procedures regarding notification in advance of its:

Monitoring procedures over aforementioned ____________________

Overall control environment ____________________

Completed by: ____________________ Reviewed by: ________________

Date: ____________________ Date: ________________

Other Matters

Client: ____

Closing date: ______________________ URL: ______________________

Consider the impact of any other matters (such as those listed below), which would be relevant in evaluating a web site's conformity with the WebTrust criteria

Changes to the organizational structure
Problems in meeting customer orders or commitments
High number of customer complaints or returns
Instances of fraud and/or breaches of controls involving:
  employees with electronic commerce responsibility
  contractors and others who provide service and support to the website
  unauthorized third parties
  systems and other electronic commerce infrastructure
Significant changes in management or other high turnover of employees
Other

Other Matters (cont.)

Client: ______________________________

Closing date: ____________________ URL: ____________________

Describe here any issues that need to be followed up with management

List here any items that will need additional attention during the next seal update examination

Completed by: ____________________ Reviewed by: ____________________

Date: ____________________ Date: ____________________

APPENDIX D

Favorite Websites

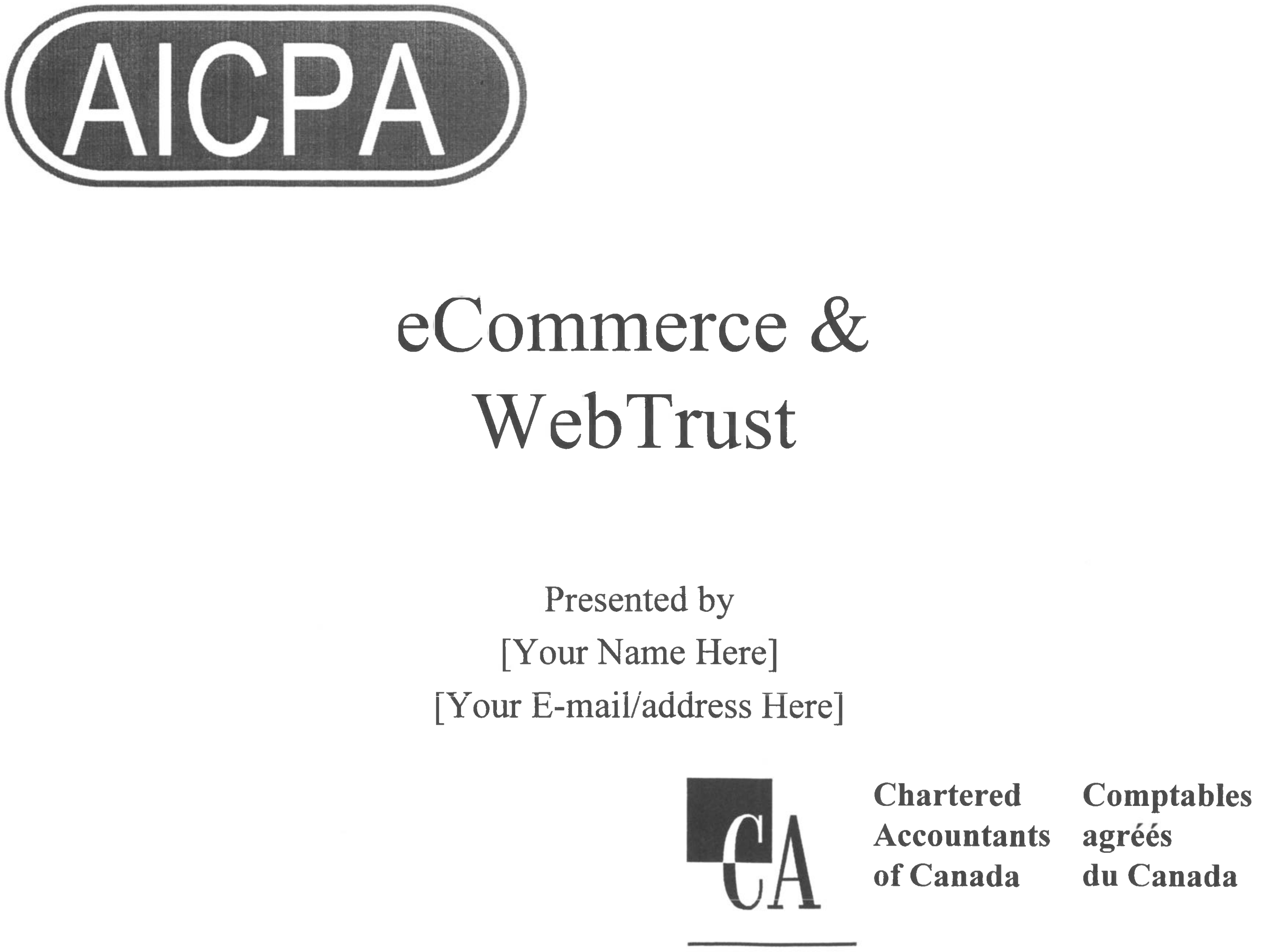
The following websites provide a sample of the good information you can use in a WebTrust engagement. This list is not all-inclusive, and there are new sites being formed every day. We also have made every attempt to verify the links to these sites; however, as is the case with the Internet, the site may become unavailable at a future date.

www.aicpa.org	AICPA home page
www.aicpa.org/webtrust/index.htm	The AICPA site for WebTrust. From here you can find further links to the Principles and Criteria and the Yankolovich study
http://ciac.llnl.gov/ciac/CIACWelcome.html	Computer Incident Advisory Capability—provides information regarding computer security incidents, hoaxes, and viruses
http://www.obscure.org/~jaws/security.html	Computer security and privacy site with links to other sites
http://kumite.com/myths	Computer Virus Myths
www.forrester.com	Forrester Research
http://www.verisign.com/webtrust/siteindex.html	Versign's index of all WebTrusted sites (be sure to visit Verisign's home page for other good information
www.icsa.net	International Computer Security Association—a great site to visit. They have a couple of good downloads of information (firewall buyers guide and others)
www.bbb.com	Better Business Bureau—learn a little about the competition
www.rsa.com	RSA Data Security—good site to learn about cryptography
www.cookiecentral.com	Helpful information on cookies
www.internic.net	Internic home page—go here to verify domain names and IP address. Lots of other helpful information here too.

www.cert.org	CERT Coordination Center studies Internet security vulnerabilities
http://csrc.ncsl.nist.gov	National Institute of Standards and Technology—source for security information and resources
www.lsli.com	Livermore Software Laboratories—has a tutorial for firewalls and the supporting technology
www.truste.org	Trustee's site and information about privacy on the Internet
www.dnb.com/dunsno/dunsno.htm	Dun & Bradstreet's site to obtain and update company duns number—important in setting up a WebTrust seal

APPENDIX E

WebTrust Power Point Presentation Information



AICPA

eCommerce & WebTrust

Presented by

[Your Name Here]

[Your E-mail/address Here]

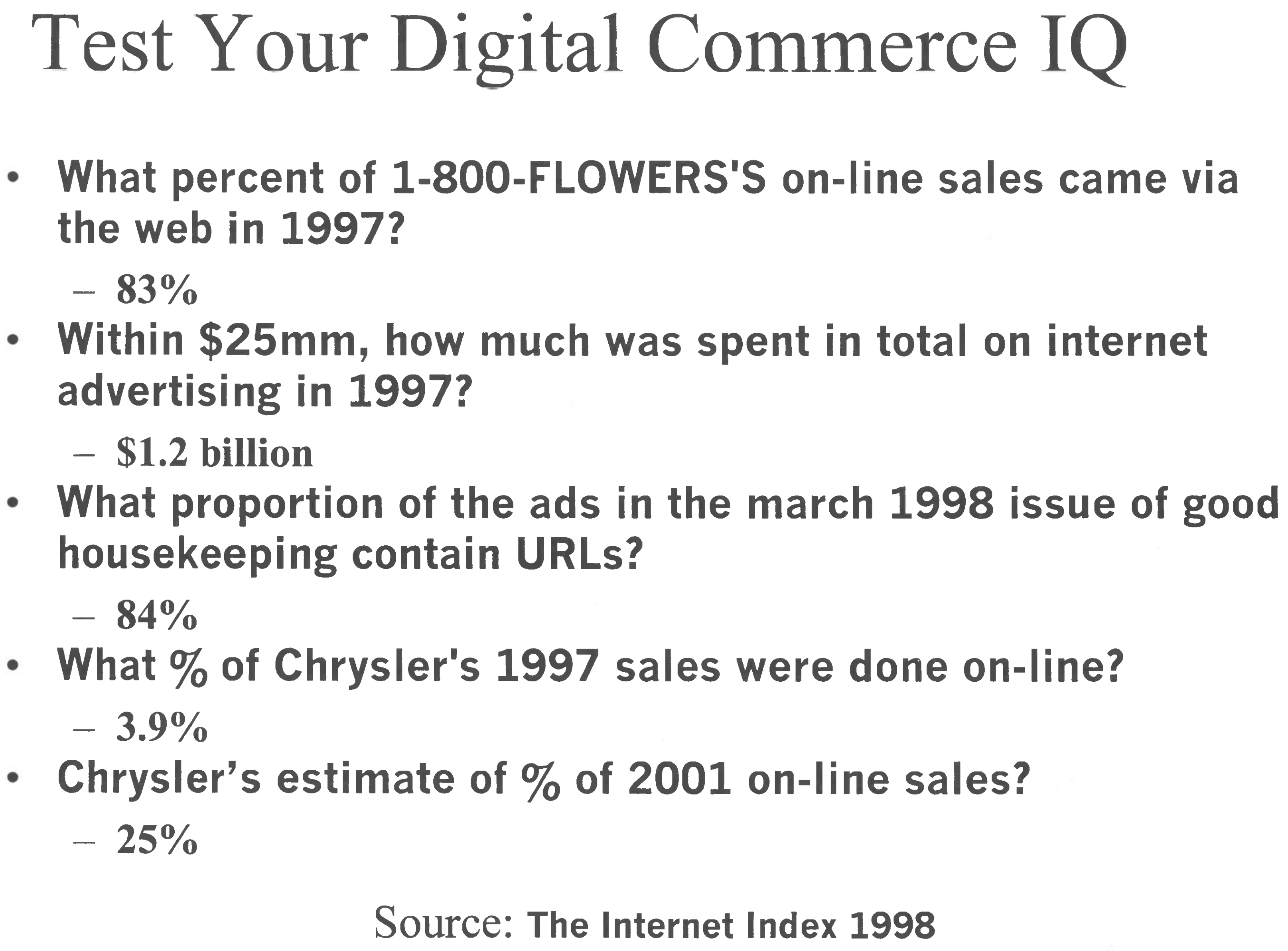
Chartered Accountants of Canada

Comptables agréés du Canada

Our Objectives

- Background of eCommerce
- Introduction to CPA WebTrust
  - Principles
  - Criteria
- Looking at how the seal works

On-line retailers sold $2.4 billion worth of goods in 1997. Yet only one-fifth of on-line adults -- 5% of North Americans -- have made a purchase on-line (see March 1998 Consumers & Technologies^{TM} Report. “Consumer eCommerce Readiness”.



Test Your Digital Commerce IQ

- What percent of 1-800-FLOWERS'S on-line sales came via the web in 1997?
  - 83%
- Within $25mm, how much was spent in total on internet advertising in 1997?
  - $1.2 billion
- What proportion of the ads in the march 1998 issue of good housekeeping contain URLs?
  - 84%
- What % of Chrysler's 1997 sales were done on-line?
  - 3.9%
- Chrysler's estimate of % of 2001 on-line sales?
  - 25%

Source: The Internet Index 1998

Test Your Digital Commerce IQ

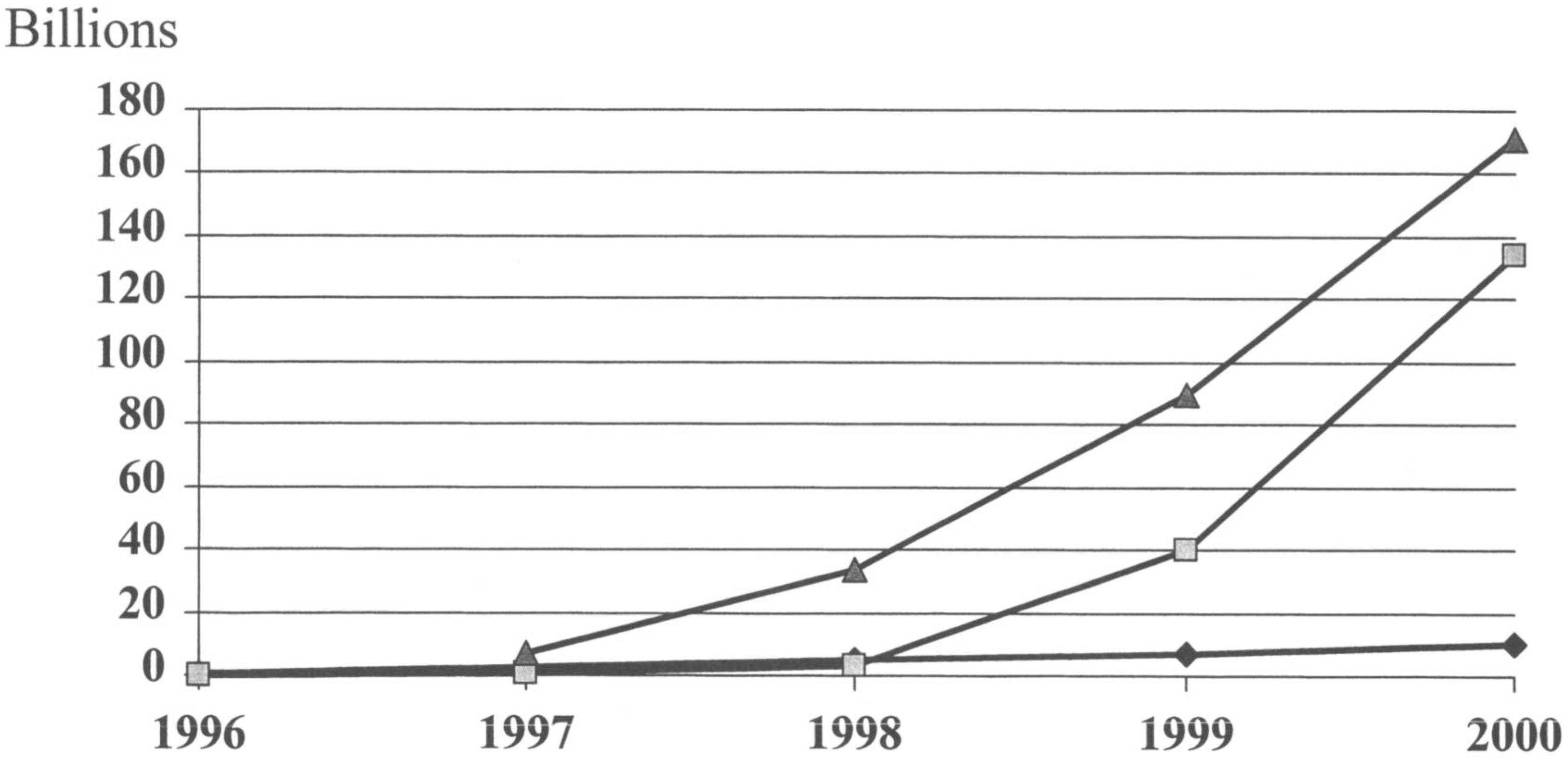
- What percentage of online users have made actual financial transactions on line?
  - 24%
- What is the #1 concern of on-line users?
  - Security & privacy (60%)
- Of on-line shoppers, what is average dollar amount spent monthly on-line?
  - $212
- What is the #1 product purchased on-line
  - Computer hardware/software
- What is the satisfaction level on on-line purchases
  - 84% satisfied
  - 8% not satisfied
  - 8 % don't know

Source: Yankelovich Partners AICPA Study 8/97

The total value of goods and services traded between companies over the Internet will reach $8 billion this year and $327 billion in the year 2002. The rapid growth of intercompany commerce will cause businesses to adopt dynamic trading processes.

Forrester July 1997

Internet Commerce Market



Source: The Yankee Group, 1996 and 1997

Reasons for Not Shopping On-line

- I am worried about security
- I am not sure of who I am doing business with
- I don’t like the traceability
- I am afraid I will get scammed

WebTrust Principles and Criteria

CPA WebTrust

WebTrust Principles

- Business Practices & Information Privacy.

  The entity discloses its business and information privacy practices for electronic commerce transactions and executes transactions in accordance with its disclosed business and information privacy practices.

- Transaction Integrity.

  The entity maintains effective controls to provide reasonable assurance that customers' transactions using electronic commerce are completed and billed as agreed.

- Information Protection.

  The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce is protected from uses not related to the entity's business.

Criteria Structure

- General Assertion
  - Business Practices & Information Privacy Principle
    - Disclosure Criteria
  - Transaction Integrity Principle
    - Controls and Practices Criteria
  - Information Protection Principle
    - Controls and Practices Criteria

Business Practices Criteria

Disclosure

- Terms & conditions by which it does business
  - time frame for fulfillment
  - time for backorder notification
  - normal method of delivery & options
  - payment terms & options
  - electronic settlement practices
  - canceling recurring charges
  - return practices, if any

Business Practices Criteria

Disclosure

- Nature of the goods, information, or services
- Where customers can obtain warranty and other service
- Information to allow customers to file claims & complaints

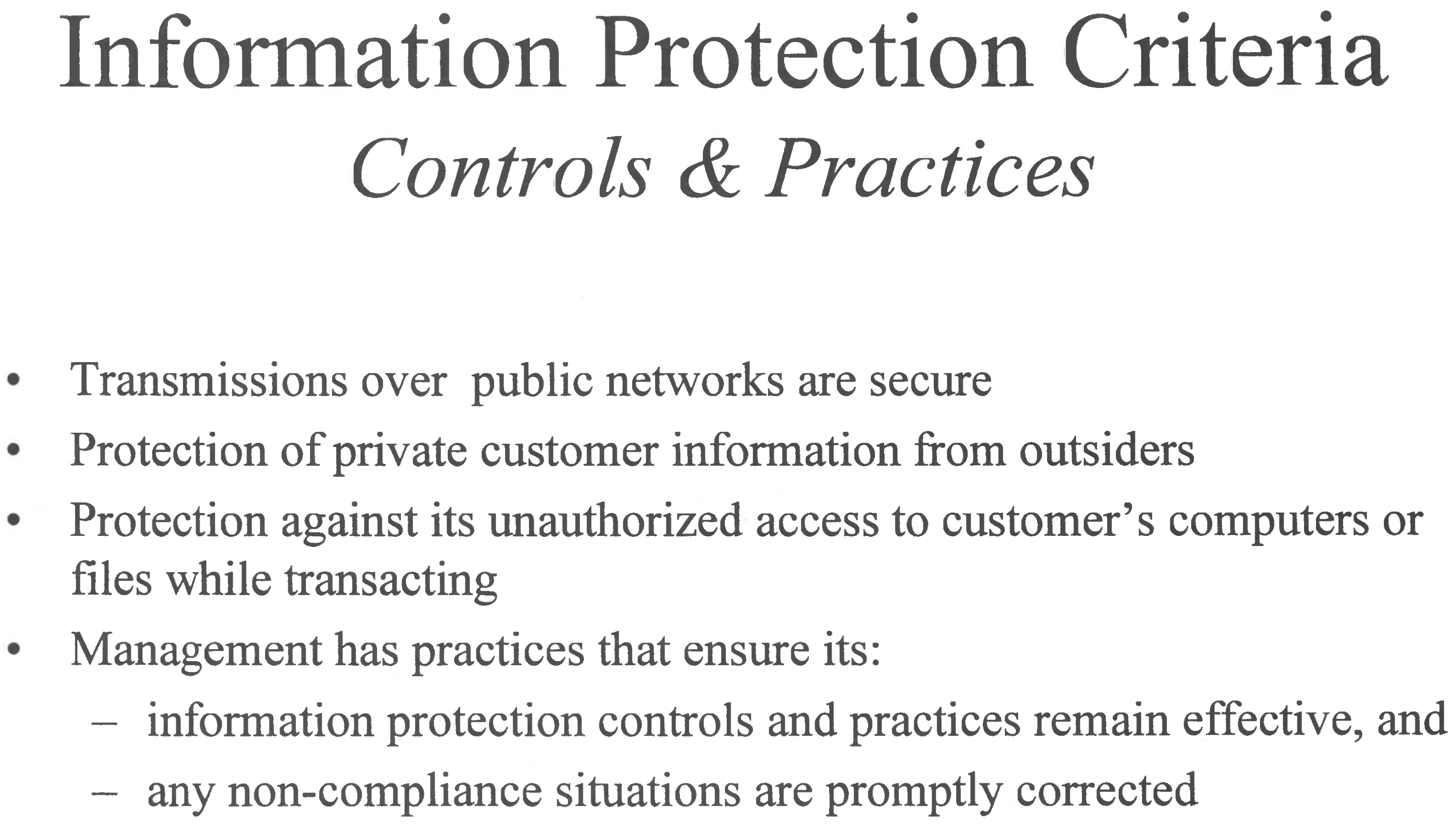
Information Privacy

- Disclosures regarding –
  - Specific types of information collected
  - Distribution of information to 3rd parties
  - Customer choices regarding what information to provide or an “opt out” feature
  - How customers may correct, update or delete collected information
  - Procedure to resolve disputes over the accuracy of collected information
  - Site’s cookie policy

Transaction Integrity Criteria

Controls & Practices

- All information needed to process & bill the order accurately is recorded
- Proper goods or services are provided
- Billing & settlement is done properly
- Documentation permits subsequent follow-up
- Management has practices that ensure its:
  - business practice disclosures are current,
  - transaction integrity controls and practices remain effective, and
  - non-compliance situations are promptly corrected

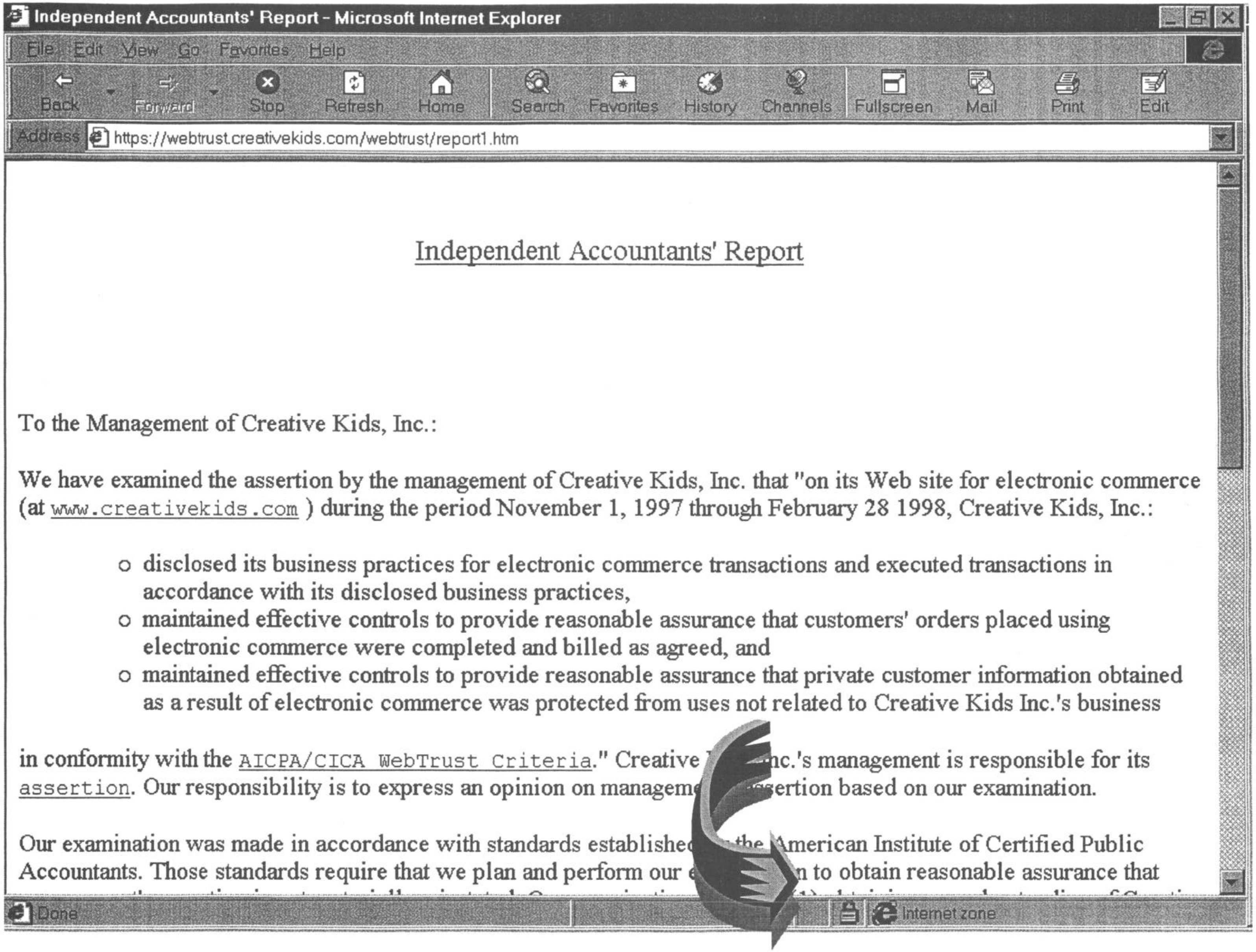


Information Protection Criteria

Controls & Practices

- Transmissions over public networks are secure
- Protection of private customer information from outsiders
- Protection against its unauthorized access to customer's computers or files while transacting
- Management has practices that ensure its:
  - information protection controls and practices remain effective, and
  - any non-compliance situations are promptly corrected

Let's Look at How the Seal Works


Independent Accountants' Report - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print Edit
Address https://webtrust.creativekids.com/webtrust/report1.htm
Done
Internet zone

Independent Accountants' Report

To the Management of Creative Kids, Inc.:

We have examined the assertion by the management of Creative Kids, Inc. that "on its Web site for electronic commerce (at www.creativekids.com) during the period November 1, 1997 through February 28 1998, Creative Kids, Inc.:

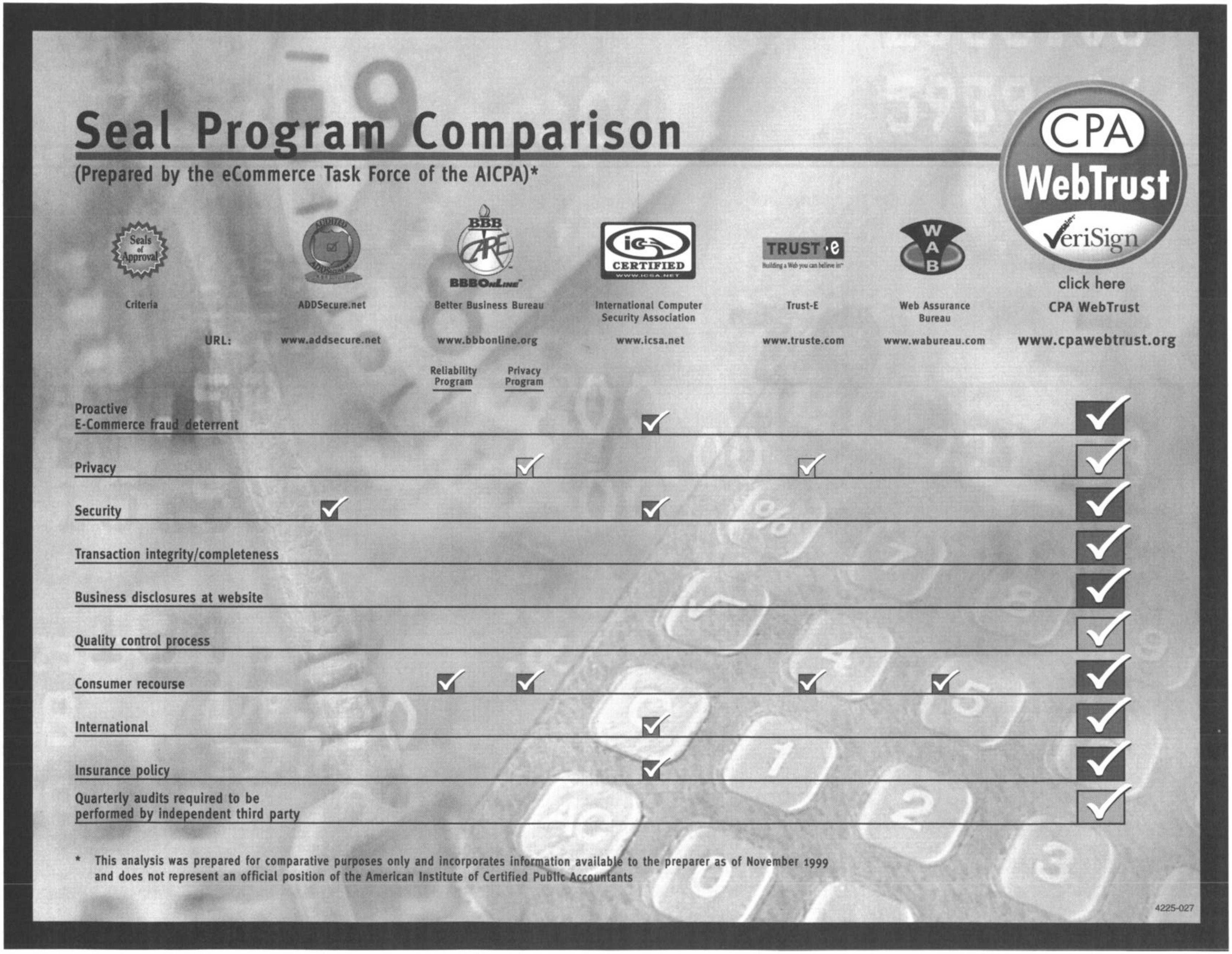
- disclosed its business practices for electronic commerce transactions and executed transactions in accordance with its disclosed business practices,
- maintained effective controls to provide reasonable assurance that customers' orders placed using electronic commerce were completed and billed as agreed, and
- maintained effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce was protected from uses not related to Creative Kids Inc.'s business

in conformity with the AICPA/CICA WebTrust Criteria." Creative [illegible]nc.'s management is responsible for its assertion. Our responsibility is to express an opinion on manageme[illegible]ssertion based on our examination.

Our examination was made in accordance with standards establishe[illegible] the American Institute of Certified Public Accountants. Those standards require that we plan and perform our e[illegible]n to obtain reasonable assurance that

Why WebTrust Is a Better Seal Program

- Proactive fraud deterrent
- Privacy and security features
- Quality control process
- Consumer recourse
- International in scope



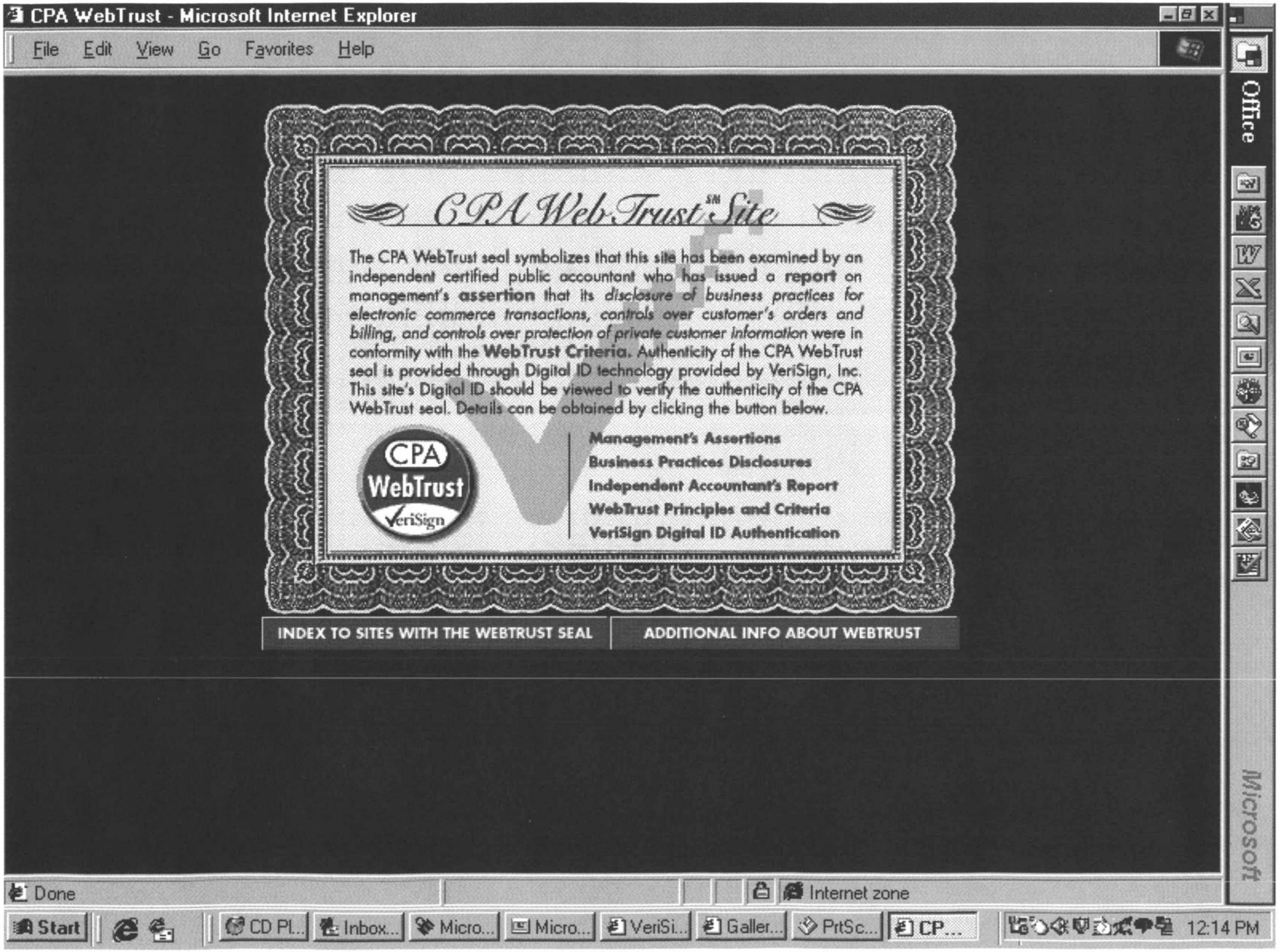
Seal Program Comparison

(Prepared by the eCommerce Task Force of the AICPA)*

Criteria	ADDSecure.net	Better Business Bureau		International Computer Security Association	Trust-E	Web Assurance Bureau	click here CPA WebTrust
URL:	www.addsecure.net	www.bbbonline.org		www.icsa.net	www.truste.com	www.wabureau.com	www.cpawebtrust.org
		Reliability Program	Privacy Program				
Proactive E-Commerce fraud deterrent				✓			✓
Privacy			✓		✓		✓
Security	✓			✓			✓
Transaction integrity/completeness							✓
Business disclosures at website							✓
Quality control process							✓
Consumer recourse		✓	✓		✓	✓	✓
International				✓			✓
Insurance policy				✓			✓
Quarterly audits required to be performed by independent third party							✓

* This analysis was prepared for comparative purposes only and incorporates information available to the preparer as of November 1999 and does not represent an official position of the American Institute of Certified Public Accountants

4225-027



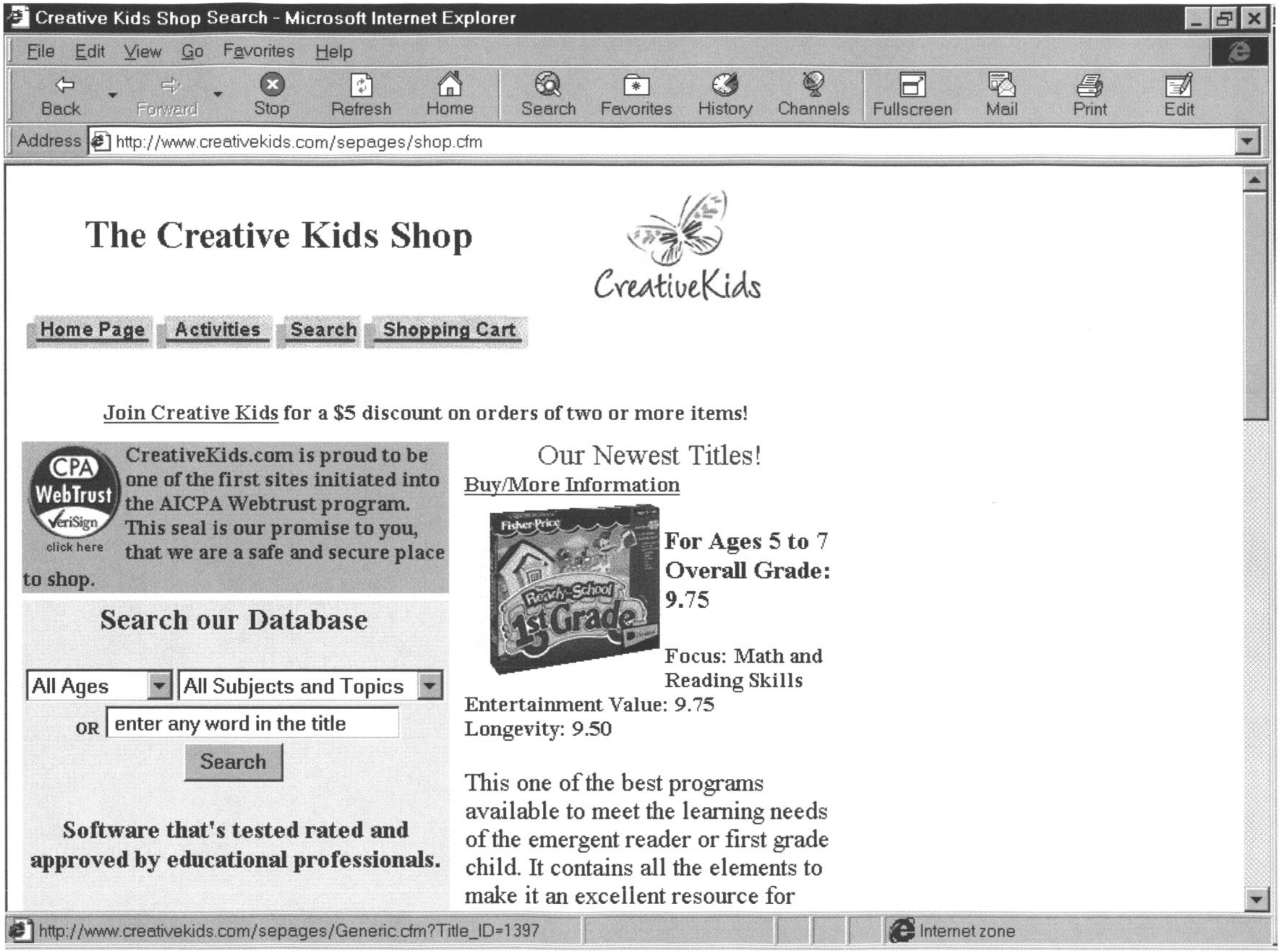
CPA WebTrust℠ Site

The CPA WebTrust seal symbolizes that this site has been examined by an independent certified public accountant who has issued a **report** on management's **assertion** that its *disclosure of business practices for electronic commerce transactions, controls over customer's orders and billing, and controls over protection of private customer information* were in conformity with the **WebTrust Criteria.** Authenticity of the CPA WebTrust seal is provided through Digital ID technology provided by VeriSign, Inc. This site's Digital ID should be viewed to verify the authenticity of the CPA WebTrust seal. Details can be obtained by clicking the button below.

Management's Assertions
Business Practices Disclosures
Independent Accountant's Report
WebTrust Principles and Criteria
VeriSign Digital ID Authentication

INDEX TO SITES WITH THE WEBTRUST SEAL

ADDITIONAL INFO ABOUT WEBTRUST



http://www.creativekids.com/sepages/shop.cfm

The Creative Kids Shop

Join Creative Kids for a $5 discount on orders of two or more items!

CreativeKids.com is proud to be one of the first sites initiated into the AICPA Webtrust program. This seal is our promise to you, that we are a safe and secure place to shop.

Search our Database

OR

Software that's tested rated and approved by educational professionals.

Our Newest Titles!

Buy/More Information

For Ages 5 to 7
Overall Grade: 9.75

Focus: Math and Reading Skills
Entertainment Value: 9.75
Longevity: 9.50

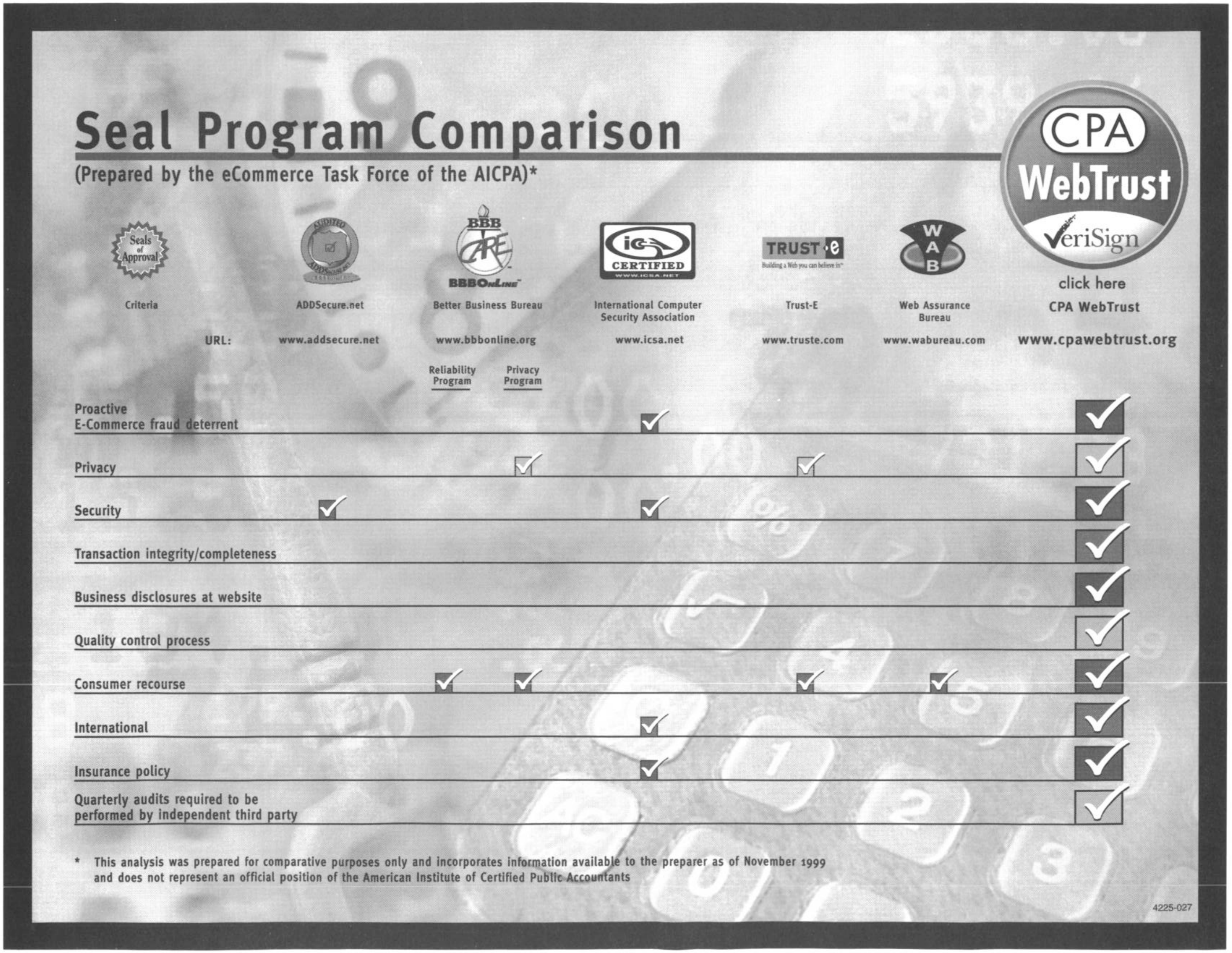
This one of the best programs available to meet the learning needs of the emergent reader or first grade child. It contains all the elements to make it an excellent resource for

http://www.creativekids.com/sepages/Generic.cfm?Title_ID=1397

APPENDIX F

Seal Program Comparison

You, as practitioners, might find it useful to review the Seal Program Comparison, a grid presenting features of the respective seal programs, which we have included on the next page for you. The grid highlights the competitive and technical differences between WebTrust and other seal programs.



Seal Program Comparison

(Prepared by the eCommerce Task Force of the AICPA)*

Criteria	ADDSecure.net	Better Business Bureau Reliability Program	Better Business Bureau Privacy Program	International Computer Security Association	Trust-E	Web Assurance Bureau	click here CPA WebTrust
URL:	www.addsecure.net	www.bbbonline.org		www.icsa.net	www.truste.com	www.wabureau.com	www.cpawebtrust.org
Proactive E-Commerce fraud deterrent				✓			✓
Privacy			✓		✓		✓
Security	✓			✓			✓
Transaction integrity/completeness							✓
Business disclosures at website							✓
Quality control process							✓
Consumer recourse		✓	✓		✓	✓	✓
International				✓			✓
Insurance policy				✓			✓
Quarterly audits required to be performed by independent third party							✓

* This analysis was prepared for comparative purposes only and incorporates information available to the preparer as of November 1999 and does not represent an official position of the American Institute of Certified Public Accountants

4225-027

APPENDIX G

Standard Port Numbers

Port Number	TCP Use	UDP Use
0	Reserved	Reserved
25	Any private mail system	Any private mail system
35	Any private printer	Any private printer
37	Time	Time
42	N/A	Host name server
47	FTP	FTP
50	Remote mail checking	Remote mail checking
53	Domain name server (DNS)	Domain name server (DNS)
71–74	Remote job service	Remote job service
80	WWW	WWW
92	Network printing protocol	Network printing protocol
107	Remote telnet service	N/A
115	Simple file transfer protocol (SFTP)	Simple file transfer protocol (SFTP)
169	Send	Send
190	Gateway Access Control Protocol (GACP)	Gateway Access Control Protocol (GACP)
193	Spider Remote Monitoring Protocol	Spider Remote Monitoring Protocol
201–208	Apple Talk	Apple Talk
221	Berkley rlogind with SPX auth	Berkley rlogind with SPX auth
406	Interactive Mail Support Protocol	Interactive Mail Support Protocol
531	Chat	Chat
532	Readnews	Readnews
533	Emergency Broadcasts	N/A
541	rlogin	rlogin
565	whoami	whoami
758	nlogin	nlogin
773	submit	notify
774	rpasswd	N/A

For a more complete listing visit http://www.con.wesleyan.edu/~triemer/network/docservs.html.

APPENDIX H

VeriSign's Digital ID Enrollment Process

DRAFT

Licensees should be familiar with the following steps to expedite the seal process. We recommend that licensees not only become familiar but serve as a technical resource to clients and work closely with the web master/Technical personnel who will be completing these steps

Obtaining an Enrollment ID number

☞ Licensee has successfully completed this first step.

Examination of site has successfully been completed

☞ Licensee is to confirm that the web master is qualified and has a full understanding of web servers as well as how digital IDs function.

Prior to Enrollment---Web master/ Technical Contact

♦ Note: Web master will apply for the digital Id. Before beginning, the web master should assemble the following information:

☞ Accountant's name, address, phone number and AICPA firm member number (ex. 3-10000000-001).

☞ Technical contact information- First Name, last name, title, Company, Address, City, State/Province, Zip or Postal Code (11220-0433), Country (ex. US), Work Phone, Fax, E-mail Address (check for accuracy).

☞ Domain Name - If not available, see Step 1 (Confirm Domain Name)

☞ Dun and Bradstreet number – If not available, see step 2 (Getting a D-U-N-S number)

☞ Certificate Signing Request (CSR) – If not available, see step 3 (Generating a CSR)

☞ Server software platform

Platforms known to work include:

- Netscape Enterprise Server 2.0 and later version
- Microsoft IIS Server 2.0 and later
- C2 Net Stronghold Apache Servers
- Oracle Web Servers (later versions only)
- 00- Lotus Domino (after 4.6.2)

♦ Servers known not to work include:

- Lotus Domino prior to 4.6.2
- Earlier versions of the Oracle Web Server

Final Preparation before Enrollment

☞ Before starting to enroll, the web master / technical contact should :

- Install Web Server Software
- Ensure that the Proxy Setting enables the site to create a secure connection outside of the firewall
- Have the Enrollment ID number easily accessible
- Review Legal Agreement, a copy of this document can be found at:
  type in: http://digitalid.verisign.com/server/WebTrust/trustintro.htm

ENROLLMENT (To be completed by the Web master/technical contact)

☞ Step 1: Confirm Domain Name

If the Web master needs to find the Domain Name:

Start by typing in:
http://digitalid.verisign.com/server/WebTrust/trustStep1.htm

Note: Your InterNIC domain must be registered to the organization enrolling for the ID (ex. aicpa.org must be registered as AICPA-DOM).

■ This information can also be found by visiting:
Type in: http://www.networksolutions.com

Enter the domain name. If the organization's website is at www.nice.com, the organization's domain name is nice.com

■ Your Who is Query Result will give you the following information:
Example:
Nice, Inc. Nice-Dom
1234 Apple Ave.
Ocean Spray, NY 11001

Domain Name: Nice.Com

☞ Step 2: Proof of Right

Type in:
http://digital.id.verisign.com/server/WebTrust/trustStep2.htm

In this step, the Web master/technical contact confirms that the organization has the legal right to conduct business under the name specified in the enrollment request. The company must submit "Proof of Right" at the time of enrollment. The following are valid methods:

- Entering the organization's Dun & Bradstreet D-U-N-S number at the time of enrollment.

  (This will be the most effective way and VeriSign will also issue the WebTrust Server ID several days sooner.)

- Searching for the organization's D-U-N-S number or applying for one online if the organization does not have one.

- To search or to get a D-U-N-S number (free) go to:
  http://digitalid.verisign.com/server/dnb_query.htm

If obtaining a D-U-N-S number is not possible at the time, you can alternately fax a copy of the following documents to VeriSign.

- Articles of Incorporation
- Business License
- Fictitious Business License
- Official Filing with the Security & Exchange Commission

If the WebTrust Server ID is for a government organization or an agency, fax the following:

- The Act or Charter (or specific page within) that establishes the organization within the government.

If the WebTrust Server ID is for a University, fax the following:

- Articles of incorporation (many domestic Universities are incorporated).

Write the Domain name on the document and fax it to VeriSign at 650-961-8870.

NOTE: Faxing any of the above documents instead of providing a D-U-N-S number may **delay the WebTrust Server ID application up to one week**. It is therefore suggested that a D-U-N-S number be used instead.

Step 3: Certificate Signing Request (CSR)

Type in:
http://digitalid.verisign.com/server/WebTrust/trustStep3.htm

The CSR is an encrypted file that contains the organization's public key, name, locality and URL. The CSR must be submitted at the time the request is made for the WebTrust ID.

When generating a CSR, a Web Server software must be used. The Web Server will create two files when generating a CSR: a Private Key and the CSR.

Instructions on generating a Key Pair and CSR is available, please see below.

If the server type is:

Microsoft IIS 4.0 go to:
http: digitalid.verisign.com/server/help/insMicrosoftCSR_4.htm

Microsoft IIS 3.0 and 2.0 go to:
http: digitalid.verisign.com/server/help/insMicrosoftCSR_2_3.htm

If the server type is:
Netscape Enterprise Server 2.0 go to:
http: digitalid.verisign.com/server/help/insNetscapeCSR.htm

☞ Detailed installation instruction is available for other server types such as:

- Apache Freeware
- IBM
- Lotus Notes Server 4.1 or Lotus Domino Server 4.5
- Microsoft IIS
- Netscape
- OpenMarket
- O'Reilly
- StarNine
- Stronghold

For instructions, type in:
http://www.verisign.com/server/support/install/secure/did.html

Note: If the server you are using is not listed, please refer to the documentation that came with the server or contact your server vendor.

Recommendation

Due to known vulnerabilities of key length up to 512-bits, use a CSR with a key length longer than 512 bits (1024 bits is highly recommended).

Note: older web servers are not capable of generating a longer key.

Trouble Shooting

☞ **Microsoft IIS Software platform**

Due to a slight misconfiguration in the IIS Key Manager Software some customers are encountering the error "Invalid Password". If you encounter this message, follow the appropriate steps below

Web server type Microsoft IIS 4.0 go to:
http: digitalid.verisign.com/server/help/insMicrosoftCSR_4.htm

Web server type Microsoft IIS 3.0 and 2.0 go to:
http: digitalid.verisign.com/server/help/insMicrosoftCSR_2_3.htm

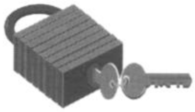
Following these steps will prevent you from getting this error message. There is a possibility that not following these steps will lead to the certificate not working properly, and your installation will be delayed.

☞ If after following these steps, the Web master/technical contact finds that the certificate will not install, verify the following:

- That the certificate is not being created and installed through a remote Key Manager, it must be created and installed through a local server.
- The computer you are logged on to must have an administrator level account.
- If neither of the above appears to be the problem then you can create a test request using Keygen.exe and install the certificate using Setkey.exe. Go to http://digitalid.verisign.com/server/help/insMicrosoftCSR_4.htm for detailed instructions.

If you are unable to use Keygen.exe or Setkey.exe, call Microsoft Technical Support at 1-800-936-3500. If an error message appears when using Keygen and Setkey this may be due to configuration issues. Please contact Microsoft Technical Support at 1-800-936-5900. Please be aware that this is a paid support.

■ Key Manager



Remember the password you enter. You will need this key to perform actions that access your private key material.

***Every web site that has a distinct DNS name must also have an encryption Key installed. However, each website for SSL (secured sockets layer) must have a distinct IP address as well.

***Before closing the Key Manager you must commit the changes. If you accidentally close without committing the changes you delete the partial key in Key Manager and recreate the request.

☞ Remote Server: Generating a Key Pair and CSR

To generate a key pair and a Secure Server ID on a remote server use the Key Manager Tool (keyring.exe) with IIS 2.0.

Note:

- Key Pairs are not encrypted when sent across the network.
- Since the private key is at risk, so is the sites SSL identification (stated in the certificate).
- Due to the vulnerability of the key pair the possibility of future interception and decryption of all communications to and from that computer will be at risk.

Protection
In order to protect the private key, paramount to SSL you should either:

A) Generate the key locally on the computer where is to be installed.
B) Transfer the key via diskette. Save the key from the remote machine and hand deliver for instillation. Installation will be done from the diskette.
C) If you are in a secure environment and it is a trusted network then you can transfer the private key via the network.

☞ Netscape Enterprise Server

For detailed step by step instructions go to:

http://digitalid.verisign.com/server/help/insNetscapeCSR.htm

Note: Key Pair File
It is important to create a back up pair file. The information should be stored in a secured place. It is recommended for it to be copied on to a floppy disk and stored in a safe or safe-deposit box.

☞ Once the CSR has been generated the software server will either e-mail the CSR or save it on to your hard disk (created a request file).

Step 4: Submitting the CSR

Type in:
http://digitalid.verisign.com/server/WebTrust/trustStep4.htm

An ASCII text editor (such as NotePad) will be needed in order to open the file. Word processors such as Word that will insert formatting or control characters are not to be used for this file.

Copy the entire CSR file including the lines containing the beginning and end into the field on the right.

Step 5: Completing the Application

Type in:
http://digitalid.verisign.com/server/WebTrust/trustStep5.htm

The following information will be reflect the information supplied with the CSR, this information must be checked for accuracy. If any of the information is not correct you must submit a new CSR with the correct information.

Common Name-The name of the website that will be secured.

Organization-This must be the same as the registered owner of the domain name.

Organizational Unit- (Optional) Used to differentiate organizational divisions and DBA names.

City/Location- The city or locality in which the organization does business

State/Province- The state or province where the organization does business. Abbreviations will not be accepted, the name must be typed in full (required for all organizations outside the US and Canada).

Country-The two-character ISO country code (ex US for United States). Required for all organizations outside of the US or Canada.

☞ **Enrollment Information**

Enrollment ID#

NOTE: The input screen is case sensitive. Please ensure that you enter the first four letters of your EID in lower case.

CPA/CA's Firm Number:

Seal Type:
- CPA WebTrust Seal
- CA WebTrust Seal

Server Software Vendor:
- Select your server software

Challenge Phrase:

Enter a word that would be easy for you to remember but difficult for any one to figure out.

This field will be needed when submitting a renewal or revocation for the WebTrust ID. The word may also be requested when speaking to a VeriSign support staff. It is important that you remember this word and if needed write it down and store it in a safe location.

Technical Contact Information

Enter the information of the person whom the WebTrust ID should be sent to. The person must have administrative access to the web server. The person could be a web master or technical support representative at your Internet Service Provider (ISP).

The person listed as the Technical Contact will also be responsible for notifying VeriSign if the WebTrust ID is compromised.

Renewals will also be sent to the Technical Contact as well as the Organizational Contact.

The following information will be required:
First Name, last name, title, Company, Address, City, State/Province, Zip or Postal Code (11220-0433), Country (ex. US), Work Phone, Fax, E-mail Address (check for accuracy).

Organizational Contact Information

This must be the person in the organization responsible for the WebTrust ID. The organizational contact should be able to provide organizational information on request. This should be someone with a high-level status within the organization. The Organizational Contact will also be contacted by phone prior to issuance of the WebTrust ID.

The organization's contact should be someone other than the Technical contact. The organizations contact will also receive a renewal notice.

Certified Accountant Contact

Enter the information form the person responsible for certifying the company's web site.

The following information is required:
First name, last name, title, company, address, city, State/ Province, Zip or Postal Code, Country, Work Phone, E-mail Address. The information you have entered must be checked for accuracy.

WebTrust Index

The following information will be listed on the WebTrust index.

Keywords

Enter up to five words that best describes the organization

Category

You will be given a choice (pull down menu) of categories, choose one that best describes the business.

Web Site description

Enter 20 words describing the site. The Web master may want to consult the marketing department.

D-U-N-S Number

Enter the organization's D-U-N-S number (go back to step 2 to of this document if not available)

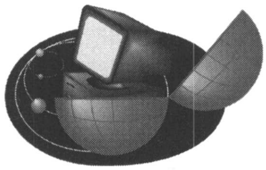
The application will be delayed if submitted without this number.

☞ Subscriber Agreement

Please read the subscriber agreement if you have not done so.

If the terms and conditions are accepted, click on the accept button to submit your request for the WebTrust Server ID.

Step 6: Processing



This is the final step before the organization obtains their WebTrust ID.

VeriSign will do the following:

All the information provided would be checked for accuracy.

Proof of Right: Checks with the company and a reputable third party (such as Dun & Bradstreet) to confirm that the organization has the right to the requested WebTrustGlobal Server ID and meets the US Commerce Dept. Requirements for use of strong encryption.

EID: Confirms that the Enrollment ID was given to you by the CPA or CA is valid.

WebTrust ID: It takes 3 to 5 business days to issue.

Problems that may cause delays are:

- Inaccurate of incomplete information:
- No D-U-N-S number(see step 2 of this document for full details)
- Wrong EID

VeriSign will e-mail the technical contact an email confirming receipt of your application.
The e-mail will contain a PIN number that can be used to check the status, go to:

If a confirmation is not received, please e-mail VeriSign at ca_support@verisign.com or call VeriSign's Technical Support line at 650-429-3338.