2001

Effects of a Third-Party Service provider in a Webtrust or Similar Engagement, Version 3.0, November 2001

American Institute of Certified Public Accountants (AICPA)

Canadian Institute of Chartered Accountants

Chartered Accountants of Canada

Comptables agréés du Canada

EFFECTS OF A THIRD-PARTY SERVICE PROVIDER IN A WEBTRUST$^{SM/TM}$ OR SIMILAR ENGAGEMENT

Version 3.0

November 2001

FOREWORD

It is becoming increasingly common for Web clients (both in business-to-consumer and business-to-business relationships) to rely upon a third-party service provider (TPSP), such as an Internet service provider (ISP) or another third-party Web-hosting service, to perform processing of key and other applications and to administer security relating to the Web client's site. It is not uncommon for a TPSP to host a number of Web client sites on servers it manages.

This situation can cause difficulties for a Web client that wants to obtain a WebTrust report on its site. There may be certain controls that are needed to satisfy the AICPA/CICA WebTrust Criteria that are the primary responsibility of the TPSP or that may be a shared responsibility between the TPSP and the client. Issues arising as a result of this shared responsibility are not covered in the existing AICPA/CICA WebTrust Criteria for the various WebTrust 3.0 Principles.

As a result, in situations where specific services and/or activities of relevance in a WebTrust engagement for a WebTrust client are outsourced or otherwise performed by a TPSP, additional guidance to the WebTrust auditor is required.

Although the guidance contained in this Guide was developed specifically for a WebTrust engagement, the practitioner may encounter a TPSP when engaged to perform a SysTrust examination using the SysTrust Principles and Criteria for Systems Reliability. Accordingly, the practitioner is encouraged to follow the guidance contained in this Guide. The AICPA/CICA Electronic Commerce Assurance Services and Systems Reliability Task Forces were consolidated during the summer of 2001 and will be responsible for preparing this guidance.

This first section of this Guide provides guidance to those performing examinations at the TPSP level, where the examination is being performed for the stated purpose of providing assurance to WebTrust clients (that is, the organization engaging in electronic commerce (e-commerce) activities) and their practitioners with respect to controls at the TPSP. It addresses a number of issues, including the following:

- Objectives of the report

- Users of the report
- Standards and other considerations
- Independence, professional qualifications
- Engagement letters, planning, and representation letters
- Period of coverage
- Basis for TPSP report qualifications

The second section of this Guide provides the WebTrust practitioner with guidance on the professional judgments that need to be made in deciding:

- Whether to accept an engagement when controls relevant to meeting such criteria are provided by a TPSP.
- Whether to rely on the work of another practitioner.
- The form and content of the WebTrust practitioner's report in these circumstances.
- The nature and extent of procedures to be performed when relying on the work of another practitioner.

This is Version 3.0 of the Guide. It is based on Version 3.0 of the WebTrust Principles and Criteria. The principal changes in Version 3.0 of the WebTrust Program, as compared to version 2.0 and earlier, include but are not limited to the following:

1. The introduction of new principles, increasing the number to seven, as follows:
    - Privacy
    - Security
    - Business Practices/Transaction Integrity
    - Availability
    - Confidentiality
    - Non-Repudiation (not yet issued)
    - Customized Assertions (not yet issued)

2. Modularization of the principles to allow for the WebTrust practitioner to issue an opinion and corresponding seal on individual principles or combinations of principles.

3. Expansion of the WebTrust Program to include transactions in the business-to-business marketplace by adding new principles that can be applied to this market.

4. Expansion of the WebTrust Program to include service providers (for example, application service providers) in addition to ISPs.

This Guide has been prepared by a sub-task force of the former AICPA/CICA Electronic Commerce Assurance Services Task Force, chaired by Everett C. Johnson. This Guide was completed under the chairmanship of Donald E Sheehy. We thank the members of the sub-task force, Bruce R. Barrick, Joseph G. Griffin, Christian R. Stormer, and Alfred F. Van Ranst for their significant efforts in completing this update. We thank the other members of the Electronic Commerce Assurance Services Task Force for their timely review and comment.

Anthony J. Pugliese
Vice-President Member Innovations
AICPA

Gregory P. Shields
Director—Assurance Services Development
CICA

AICPA / CICA Electronic Commerce
Assurance Services Task Force

Everett C. Johnson, Jr., Chair

Gary S. Baker

Bruce R. Barrick

Joseph G. Griffin

Christopher Leach (Vice Chair)

Emil J. Ragones

Kerry L. Shackelford

Donald E. Sheehy

Christian R. Stormer

Alfred F. Van Ranst

Staff

Bryan C. Walker

Karyn Waller

TABLE OF CONTENTS

DESCRIPTION

PAGE

Introduction To Guide

BACKGROUND

It is becoming increasingly common for Web clients (for example, Web catalog stores, stores in virtual electronic malls, or auction Web sites that have outsourced their auction processes) to rely on a third-party service provider (TPSP), such as an Internet service provider (ISP) or another third-party Web-hosting service, to perform key and other processing and administer security relating to the Web site. In this situation, certain services, such as Web hosting, fulfillment, and settlement, are outsourced to the TPSP. It is not uncommon for a TPSP to host a number of Web client sites on servers it manages.

This situation can cause difficulties for a Web client that wants to obtain a WebTrust report covering its retail site. There may be certain controls that are needed to satisfy the AICPA/CICA WebTrust Criteria that are the primary responsibility of the TPSP or that may be a shared responsibility between the TPSP and the client. Table 1 below sets out general guidance for what WebTrust principles would be most influenced by TPSP activity.[1]

TPSP Activity	WebTrust Principles Affected
Hosting	Security, Privacy, Confidentiality and Availability
Connectivity	Availability
Web content management	All principles (disclosure affects all principles)
Settlement	Security, Privacy, Confidentiality and Transaction Integrity

[1] The Customized Assertions Principle is not discussed in this table although it could be affected by any TPSP service.

Fulfillment	Transaction Integrity, Security, Privacy and Confidentiality
Application provisioning	Transaction Integrity, Privacy, Security, Availability and Confidentiality (all principles)

In situations where specific services and/or activities of relevance in a WebTrust engagement for a WebTrust client are outsourced or otherwise performed by a TPSP, additional guidance to the WebTrust practitioner is provided in this Guide.

To determine that the organization seeking a WebTrust examination meets the WebTrust Criteria, the WebTrust practitioner would be required to gain assurance about relevant controls at the TPSP. Such assurance would be required on those controls performed by the TPSP, on behalf of the WebTrust client, that contribute to meeting the particular WebTrust Criteria.

In the absence of being able to rely on a practitioner's report for the TPSP, the practitioner for each client using the TPSP's services would likely be required to visit the TPSP to perform an assessment and test controls performed by the TPSP for its Web clients. Such a visit would be needed to perform testing of the relevant controls at the TPSP as needed to satisfy the WebTrust Criteria for the Web client.

This is unlikely to be satisfactory to the TPSP.

As a result, it would be preferable for a WebTrust practitioner to be able to obtain and rely on a report on controls of a TPSP to be able to render a WebTrust report.

The purpose of this Guide is to provide guidance to both a TPSP practitioner for preparing a report that could be used by a WebTrust practitioner (Part I) and to the WebTrust practitioner for relying on the work of the TPSP practitioner (Part II).

Although the guidance contained in this Guide was developed specifically for a WebTrust engagement, the practitioner may encounter a TPSP when engaged to perform a SysTrust examination using the SysTrust Principles and Criteria for Systems Reliability. In such situations, the practitioner is encouraged to follow the guidance contained in this Guide.

DEFINITIONS

For purposes of this Guide, the following definitions are used to identify the various organizations and entities that may enter into discussions regarding e-commerce-related activities that are the subject of WebTrust services:

- *WebTrust practitioner* is the certified public accountant (CPA) or chartered accountant (CA) who has been licensed by the AICPA or CICA or another authorized national institute to perform WebTrust services.

- *WebTrust client* is an organization engaging in e-commerce activities that wishes to be examined by a WebTrust practitioner. The WebTrust client is responsible for the establishment, implementation, and maintenance of business and technical practices and procedures to meet the appropriate WebTrust Criteria.

- *WebTrust customer* is a customer of the WebTrust client. The WebTrust customer is a purchaser of the WebTrust clients' goods, services, or financial products through the e-commerce facilities provided by, or on behalf of, the WebTrust client.

- *Third-party service provider* (TPSP) is an organization contracted by the WebTrust client to perform specific services and/or activities, the consistent performance of which (in accordance with documented expectations) are required for the WebTrust client's business and technical practices and procedures to meet the relevant WebTrust Criteria. A common example of this form of service relationship would be in the form of a TPSP providing Web server hosting and other technical services to a number of potential WebTrust clients.

- *TPSP practitioner*[2] is the CPA or CA or other licensed public accountant who has been engaged to perform an examination (audit) of controls at the TPSP.

STANDARDS CONSIDERATION AND OTHER ASSUMPTIONS

The engagements described herein are performed in the United States under the attestation standards (Chapter 1 of Statement on Standards for Attestation Engagements No. 10, *Attestation Standards: Revision and Recodification* [AICPA, *Professional Standards*, vol. 1, AT sec. 101]). In Canada, the engagements are performed under the assurance standards (Canadian Institute of Chartered Accountants [CICA] section 5025, *Standards for Assurance Engagements*). This guidance addresses a number of differences that exist between these standards.

AICPA Standards and Issues

AICPA guidance has been developed using AT section 101, incorporating certain concepts of Statement on Auditing Standards (SAS) No. 70, *Reports on the Processing of Transactions by Service Organizations* (AICPA, *Professional Standards*, vol. 1, AU sec. 324), as amended[3], into TPSP reporting. These include the concepts of including the description of the examination procedures performed (optionally) and, from SAS No. 1, *Codification of Auditing Standards and Procedures* (AICPA, *Professional Standards*, vol. 1, AU sec. 543, "Part of Audit Performed by Other Independent Auditors"), the ability of a WebTrust practitioner to make specific reference to a TPSP report as part of a WebTrust engagement.

[2] Under the Canadian assurance standards, the highest level of assurance about a subject matter is obtained in an audit engagement and the professional providing the service is referred to as the *auditor*. Under the U.S. attestation standards, the highest level of assurance about a subject matter is obtained in an examination engagement and the professional providing the service is referred to as the *practitioner*. In this document, the term *examination* refers to both audit engagements and examination engagements, and the term *practitioner* refers to both practitioner and auditor.

[3] The term, "SAS No. 70, as amended", includes amendments from SAS No. 78 and SAS No. 88.

CICA Standards and Issues

CICA guidance has been developed using CICA *Handbook* Section 5025 (as either an attest or direct reporting at a high [audit] level of assurance) for the provision of WebTrust services, including the provision of TPSP reports to support WebTrust services.

The CICA has incorporated certain concepts of *Handbook* Section 5900 in relation to TPSP reporting that *do not require* reporting of audit procedures performed and *preclude* the ability of a WebTrust practitioner to make specific reference to a TPSP report.

ASSUMPTIONS

The following assumptions are fundamental to the development of this guidance:

- A WebTrust practitioner needs to decide whether or not a specific engagement can be accepted. There may be situations in which the processing activities and controls at the TPSP are so significant to the entire control structure or to the set of WebTrust Criteria that it is unlikely that the WebTrust practitioner would be willing to rely so extensively on the work of the TPSP practitioner. In such situations, the WebTrust practitioner either needs to directly perform the examination of the TPSP controls (or perform sufficient tests of the work of the TPSP practitioner) or not accept the WebTrust engagement.

- The TPSP examination report should be issued pursuant to the standards set out in AT Section 101 or in CICA *Handbook* Section 5025 in Canada.

- The use of a TPSP examination report is typically restricted to its intended audience (customers and user auditors) to reduce the potential for misinterpretation of the report by a third party.

- Because a WebTrust engagement is conducted at an examination level, the TPSP engagement needs to be performed at an examination level.

- A "user auditor" (WebTrust practitioner) and a WebTrust client both need to know the specific processes that are employed to achieve compliance with the applicable criteria, and therefore a description of each procedure must be provided as a part of the report on a TPSP.

- When reporting on a WebTrust client, the WebTrust practitioner should make no reference to the work performed by the TPSP practitioner:

- In some instances a WebTrust practitioner may determine that access to a TPSP practitioner's working papers is desired based upon the extent of the services outsourced and professional judgment. The need for such WebTrust Practitioner access to TPSP practitioner working papers is contemplated in the professional standards. It is expected that over time, the client expectations and requirements (of both TPSP and WebTrust clients and practitioners) may require disclosure of procedures performed as a portion of engagement and reporting requirements. As a result, although inclusion of details of testing under TPSP examinations is optional, such disclosure may be helpful.

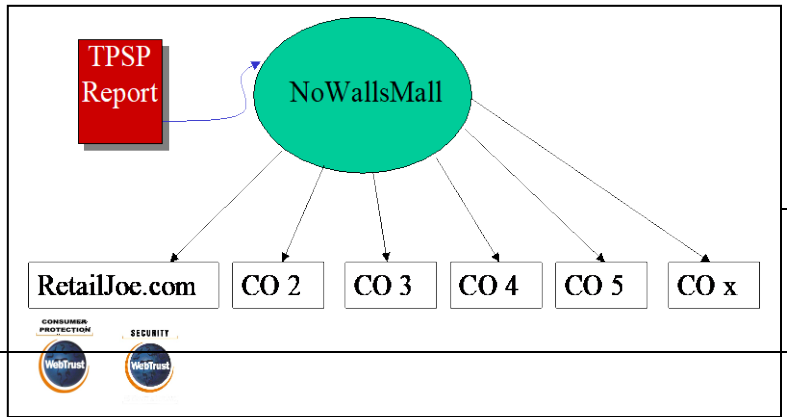
.

ILLUSTRATIVE CASE STUDIES

Two case studies are used throughout this document for illustration. They form the basis for the "Sample TPSP Practitioner Reports" section included as Appendix Two.

Business-to-Consumer Illustrative Case Study

The first case study is a business-to-consumer example using a virtual mall. RetailJoe.com is a high-end specialty electronics business. RetailJoe.com has approached the firm WebTrust Auditors LLP to conduct a WebTrust examination to enable it to receive a WebTrust Consumer Protection seal (i.e., meeting the WebTrust Privacy and WebTrust Disclosure/Transaction Integrity Principles) as well as a WebTrust



seal for Security. RetailJoe.com is hosted by a TPSP, NoWallsMall.net, that performs most of the electronic commerce services on behalf of its clients, including facilitation of product delivery. RetailJoe.com is responsible for its product information and pricing only; the remainder of its operations, including Web page management, is handled through the back-end systems of NoWallsMall.net. NoWallsMall.net is audited by TPSP Auditor LLP. The service contract signed by the two entities states that any audit evidence required by RetailJoe.com with respect to the controls and operations exercised by NoWallsMall.net is to be normally provided by its auditor, TPSP Auditor LLP. The TPSP examination endeavors to cover the needs of most of the organizations serviced by NoWallsMall.net if they also desire a particular WebTrust examination.

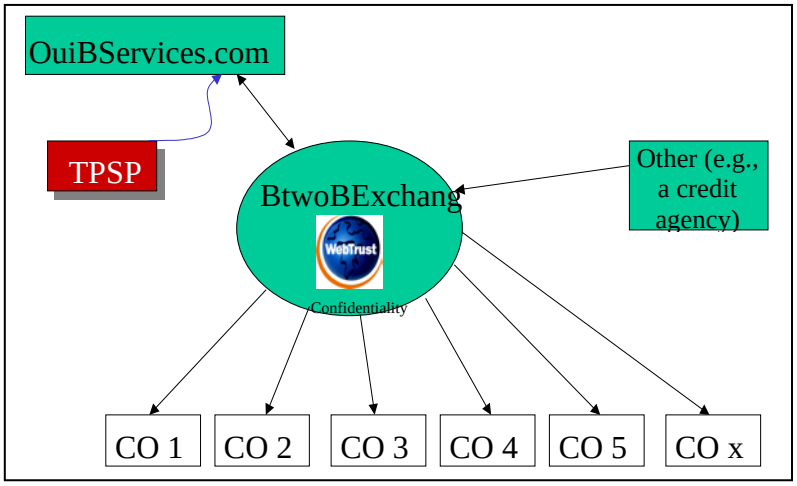
In this example, the WebTrust client believes that Privacy, Transaction Integrity, and Security are the most significant concerns that could be alleviated by a WebTrust examination. NoWallsMall.net is providing similar services for many of its hosted companies. The work by TPSP Auditor LLP with regard to Privacy, Transaction Integrity, and Security would contribute to the ability for those hosted businesses to each obtain of the related WebTrust reports and the related WebTrust seals.

The work performed by TPSP Auditor LLP will not be sufficient to, in itself, render a WebTrust opinion on RetailJoe.com. Additional procedures will need to be undertaken at the RetailJoe.com web site. There will be some question about which firm should be providing the WebTrust seal for security. Most of the controls and procedures relevant to security for RetailJoe.com are undertaken by NoWallsMall.net (see Exhibit 2 in part 2, “Guidance for the WebTrust Practitioner”). As a result, according to the service agreement in this example, the majority of the audit evidence would be obtained by TPSP Auditor LLP, with only minimal audit work being performed at the host level. This illustrative case study is discussed more fully in Part II “Accepting a WebTrust Engagement”.

Business-to-Business Illustrative Case Study

The second case study involves an electronic components exchange, BtwoBExchange.org that facilitates business-to-business transactions among a number of electronic component suppliers and customers.

BtwoBExchange.org has approached WebTrust Auditors LLP to conduct a WebTrust examination to enable it to receive a WebTrust seal for Confidentiality. BtwoBExchange.org is hosted by a TPSP, OuiBServices.com, that handles the exchange transactions and related settlement through its back-end systems. BtwoBExchange.org is responsible for Web site management and for other aspects of exchange commerce, including maintaining relevant credit information for transaction participants prior to the transaction being consummated by the trading partners. OuiBServices.com is audited by TPSP Auditor LLP. The service contract signed by the two entities states that audit evidence required by BtwoBExchange.org with respect to the controls and operations exercised by OuiBServices.com is to be normally provided by its auditor, TPSP Auditor LLP. The TPSP examination endeavors to cover the needs of most of the organizations serviced by OuiBServices.com if they also desire a particular WebTrust examination for Confidentiality.



In this example, the client believes that Confidentiality is the most significant concern that could be alleviated by a WebTrust examination. OuiBServices.com is providing similar services for many of its hosted companies. The work by TPSP Auditor LLP with regard to Confidentiality may be sufficient for those hosted businesses to obtain the related WebTrust report and the related WebTrust seal.

Part 1 - Guidance for the TPSP Practitioner

PURPOSE

The purpose of this section is to provide guidance to those performing examinations at the third-party service provider (TPSP), where the examination is being performed for the stated purpose of providing assurance to WebTrust clients and their practitioners with respect to controls at the TPSP.

OBJECTIVES OF A PRACTITIONER'S REPORT ON A TPSP

The primary objective of a practitioner's TPSP report is to provide independent assurance to users and practitioners that management has properly described the controls at the TPSP that affect a WebTrust client and that the controls tested were, in all material respects, operating effectively during the period specified based on the WebTrust Criteria. Another objective is to provide audit evidence that can be used by a client's WebTrust practitioner for assisting in an assessment of the client's controls when performing a WebTrust examination. The TPSP practitioner should assume that the report will be used for both purposes and accordingly, should determine that the description of the controls addressed in the scope of the examination is clear, complete, and not misleading to users of the TPSP report.

USERS OF TPSP REPORTS

The following summary highlights the primary needs of the users of TPSP reports.

User	Primary Need
• WebTrust client management (RetailJoe.com and BtwoBExchange.org)	An independent assessment of the reliability of controls over the contracted TPSP services to be used as a basis for management's assertion regarding the complete control environment

• WebTrust practitioner (WebTrust Auditors LLP)	Audit evidence to assist in the WebTrust client examination
• TPSP management (NoWallsMall.net and OuiBServices.com)	An independent assessment using an accepted set of criteria results in observations and recommendations for improvement of internal controls.

UNDERLYING ASSUMPTIONS

Based on the purpose of the TPSP report as previously discussed—

- WebTrust Criteria for various WebTrust Principles need to be incorporated into the guidance established for TPSP examinations and reporting.
- Unlike either Statement on Auditing Standards (SAS) No. 70, *Reports on the Processing of Transactions by Service Organizations* (AICPA, *Professional Standards,* vol. 1, AU sec. 324), or Canadian Institute of Chartered Accountants (CICA) Handbook section 5900, the reporting will constitute an opinion on the operating effectiveness of control activities as opposed to an opinion on whether specified control objectives have been achieved.

OTHER FORMS OF REPORTING

Situations may arise in which TPSP organizations already provide some form of third-party reporting to a specified class of customers. Such reporting includes SAS No. 70, CICA section 5900, WebTrust reports, or SysTrust reports related to various principles for the service provider or other general assurance (such as Chapter 1 of Statement on Standards for Attestation Engagements No. 10, *Attestation Standards: Revision and Recodification* [AICPA, *Professional Standards,* vol. 1, AT sec. 101] or CICA Section 5025). These existing reports are not expected to meet all the needs for TPSP reporting in support of WebTrust services without modification and directly addressing the needs of individual WebTrust practitioners and clients. The existence of such reports should not be ignored, however.

In situations in which the TPSP auditor has performed work that resulted in the generation of other assurance or controls reporting, or both, as described in the first paragraph of this section, the TPSP auditor should consider such performance in assessing the extent of the audit effort needed to complete the TPSP examination.

In situations in which *another* auditor has performed work that resulted in the generation of assurance or controls reporting, or both, as described in the first paragraph of this section, the TPSP auditor may consider such performance in assessing the extent of the audit effort needed to complete the TPSP examination, provided that the professional standards for relying on the work of another auditor are met (as described in this Guide).

In situations in which another auditor has performed consulting or similar work that resulted in the generation of a consulting report, but did not result in the generation of an assurance or controls report, the TPSP auditor should review the other auditor's efforts as part of the client control structure assessment. Because no assurance report was issued, there can be no reliance on the work of such consultant.

ENGAGEMENT GUIDANCE

Independence

The TPSP practitioner should be independent of the TPSP in the same way that WebTrust practitioners are required to be independent of the WebTrust client. It is generally not practical, however, nor should it be necessary for the TPSP practitioner to be independent with respect to each Web site that is hosted by the TPSP. Independence should be as defined by the standards set out in the country of the TPSP practitioner (for example, as prescribed by AICPA in its Rules of Professional Conduct or as prescribed by the Provincial Institutes of Chartered Accountants in Canada).

The TPSP practitioner should be prepared to provide the WebTrust practitioner with a representation concerning independence of the TPSP practitioner relative to the TPSP.

Professional Qualifications and Competence

By definition, the TPSP practitioner should be the certified public accountant (CPA) or chartered accountant (CA) or other licensed public accountant who has been engaged to perform the examination of controls at the TPSP. Before undertaking the engagement, the TPSP practitioner should be satisfied that the subject matter is or will be within the collective professional expertise of the practitioner and other persons performing the assurance engagement. Ideally, the TPSP practitioner should be licensed to perform WebTrust examinations. In any event, the TPSP practitioner needs to be familiar with the WebTrust Criteria and the policies and procedures that would be sufficient to achieve compliance with such criteria.

With this familiarity, the TPSP practitioner should be in a position to consider the nature and extent of the services provided by the TPSP and how the TPSP's controls could interrelate with those of the WebTrust client.

Engagement Letters

The TPSP practitioner should establish an understanding with the client regarding the services to be performed for each engagement. Such an understanding reduces the risk that either the TPSP practitioner or the TPSP may misinterpret the needs or expectations of the other party. For example, it reduces the risk that the TPSP may inappropriately rely on the TPSP practitioner to protect the entity against certain risks or to perform certain functions that are the client's responsibility. The understanding should include the objectives of the engagement, management's responsibilities, the TPSP practitioner's responsibilities, and limitations of the engagement. If the TPSP practitioner believes an understanding with the TPSP has not been established, the practitioner should decline to accept or perform the engagement.

An understanding of the terms and objectives of the engagement and the nature of the services provided should be communicated to the client, preferably in writing.

The TPSP practitioner should refer to the attestation or assurance standards, as applicable, to determine the required elements of the engagement understanding. The following elements are ordinarily included:

- The nature of the engagement (for example, an examination)
- An identification of the WebTrust Criteria and any other management assertions being reported on
- A reference to the professional standards governing the engagement
- A description of management's responsibilities
- A description of the TPSP practitioner's responsibilities and the limitations, if any, on the engagement
- The form of report anticipated
- A general description of the nature and scope of the work to be performed, fee, billing, and payment arrangements
- The expectation of receiving a representation letter
- The anticipated timetable for completion of the TPSP practitioner's work
- The expected commitment of client personnel
- Limitations of the engagement
- A request for confirmation that the terms of the engagement have been understood and accepted

Planning

Planning a TPSP engagement involves developing an overall strategy and identifying procedures to be performed. The procedures may vary depending upon the unique management assertions associated with the engagement. Once the procedures to be performed have been defined, other aspects of planning can be formulated. The strategy for the engagement should be included in the planning documentation.

Matters to be addressed by the TPSP practitioner in planning the engagement include the following:

- Scope and frequency of the engagement

- Engagement approach
- Technical competence of assigned personnel
- Timing of the work to meet user's needs
- Staffing considerations
- Use of specialists
- Engagement budgeting and monitoring
- Supervisory review and sign-off

A work program should be prepared and be approved by appropriate supervisory personnel. The amount of detail included in the program depends on both the complexities of the engagement and the nature of the report to be issued.

An engagement budget should be developed in appropriate detail that will vary with the size of the engagement. Arrangements for monitoring the budget by the engagement team and with the client should be established.

Representation Letters

A representation letter from management to the TPSP practitioner:

- Requires management to focus on specific declarations.
- Formalizes oral representations made to the TPSP practitioner in the course of the examination.
- Reduces the possibility of misunderstandings between the TPSP practitioner and the client.

Ordinarily a representation letter would be obtained for each TPSP engagement. The representations appropriate for the client vary depending on the nature of the management's assertions, if applicable, and the nature of the engagement. At a minimum, the letter should contain the following representations that:

- Management has complied with its written assertion.

- Management has made available to the TPSP practitioner all significant information that it believes is relevant to the WebTrust Criteria and assertions, if applicable.
- Management recognizes that it is responsible for the presentation of the assertions and to maintain the effectiveness of its control activities.
- Management has disclosed all events subsequent to the period being examined that would have a material effect on compliance with the criteria.

Management representations should be made as of the date on which fieldwork is substantially completed. The TPSP practitioner's report should be dated concurrently.

The management representation letter should be signed by persons responsible for and knowledgeable about the matters covered by the representations.

OTHER CONSIDERATIONS

Inclusion of Details of Testing Under TPSP Examinations

Although optional, this disclosure may be helpful. Generally, TPSP practitioner working papers are not made available to the WebTrust practitioner for review. As a result, it is expected that over time, the client expectations and requirements (for both TPSP and WebTrust clients and practitioners) may necessitate disclosure of examination procedures performed as a portion of the engagement and reporting requirements.

Coverage of Client-Specific Activities vs. Overall Procedures and Control Environment

TPSP organizations may provide a range of WebTrust-related services to WebTrust clients based on individual client needs and preferences. When this occurs, the TPSP practitioner should endeavor to perform the examination and report at a high enough level to eliminate such differences. When this is not possible, the TPSP practitioner may need to vary the examination and reporting to accommodate significant individual client differences.

As addressed earlier, in the business-to-consumer (RetailJoe.com) example, it is believed that Privacy, Transaction Integrity, and Security would be the most likely concerns that could be

alleviated by a WebTrust examination. Because NoWallsMall.net is providing similar services for many of its hosted companies, the work by TPSP Auditor LLP should be sufficient to assist hosted businesses to obtain such seals (although additional audit work will need to be conducted at the RetailJoe.com site).

As also addressed earlier, in the business-to-business (BtwoBExchange.org) example, it is believed that Confidentiality is the most significant concern that could be alleviated by a WebTrust examination. OuiBServices.com is providing similar services for many of its hosted companies; as a result, the work by TPSP Auditor LLP with regard to Confidentiality may be sufficient for those hosted businesses to obtain the same seal if required.

Relate Procedures Examined to WebTrust Client Requirements

The level of detail to which stated controls are described could present difficulties for WebTrust practitioners in assessing the relevance of a TPSP practitioner's report. The controls examined under the TPSP engagement and the related report issued should be structured for ease of integration into the work being performed by the TPSP's individual WebTrust client's WebTrust practitioner. To the extent possible, the controls examined should be disclosed in a format consistent with the principles and criteria being reported upon at the client level (in this case RetailJoe.com and BtwoBExchange.org). Where possible, consultation should be made with a number of TPSP clients desiring (or potentially desiring) WebTrust services. This may be possible through a TPSP client's user group.

Period of Coverage of TPSP Examinations and Reporting

The frequency of TPSP reporting needs to correlate to the timing requirements of the TPSP's WebTrust clients. The maximum interval between WebTrust update examinations is six months, so the timing of the TPSP reporting will have to coincide with the frequency established by the individual WebTrust clients. It is likely that WebTrust clients would be encouraged to adopt examination cycles that would support optimal TPSP reporting (likely semi-annually).

- The TPSP report cannot be a report only on the design and existence of control procedures (point in time). This would not meet the need of the continuous coverage criterion of the WebTrust practitioner.

- The time period covered by the TPSP practitioner's examination is critical to the WebTrust practitioner in assessing the TPSP's report's relevance. The period of coverage of the TPSP reporting should ideally coincide with the frequency established by the individual WebTrust clients. As the interval from the period covered by the TPSP practitioner's report and the period covered by the WebTrust practitioner's report lengthens, there would be more risk to the WebTrust practitioner that there could be changes in the controls at the TPSP that could impact on the WebTrust client. This additional risk would have to be either accepted or reduced to an acceptable level by the WebTrust practitioner. The period of coverage of the TPSP report should cover a substantial portion[4] of the reporting period provided at the WebTrust client level. This period will have to take into account the time needed by the TPSP practitioner to complete the examination and render the TPSP report.

Inclusion of List of Clients for Whom Procedures Were Examined

There will be an expectation by the individual WebTrust practitioner that testing of the individual WebTrust client in question was included in the TPSP practitioner's examination. This is not viewed to be a significant issue because the TPSP control testing would be repeated with sufficient frequency. There is also the expectation that there would be similar sets of controls over similar types of services and transactions that would be examined by the practitioner.

This reporting issue could be handled by disclosure that the procedures should be presumed to apply to all customers or by specifying what customers or classes of customers were or were not included.

4 More than 50% of the reporting period should be covered.

Need to Specify What Services Are Provided by TPSP

It is important that users of the report understand the services that are provided by the TPSP and that the scope of the audit that is communicated to them. To assist, the TPSP report may include, in an attachment, a description of the services provided to WebTrust clients or classes of WebTrust clients. To the extent possible, the services could be categorized into areas defined by the WebTrust Principles (for example, Business Disclosures/Transaction Integrity, Privacy, Security, Confidentiality and Availability).

Multi-Level Control Issues

There may be situations in which the TPSP, in turn, outsources a particular part/portion of the operations it performs for others. Therefore, it is possible that some of the controls that would support a WebTrust client in obtaining a WebTrust report, would in fact be located at another TPSP. This situation could present difficulty for the WebTrust auditor.

When the controls exercised by this additional third party are significant to the WebTrust client, the WebTrust auditor needs to obtain evidence that they exist and were operating effectively throughout the appropriate engagement time frame. Exhibit One illustrates three example scenarios. In situation one, the WebTrust auditor would need to obtain evidence for the TPSP and third party 2. In two, the WebTrust auditor would need to obtain evidence for the TPSP only. In situation three, the WebTrust auditor would need to obtain evidence for the TPSP and third parties 2 and 3.

Exhibit 1

Examples of Multi-Level Situations

Significance to Client—Controls Exercised by Third Parties

Situation	TPSP	Third Party 2	Third Party 3	Third Party 4
1	Significant	Significant	Not significant	Not significant
2	Significant	Not significant	Not significant	Not significant
3	Significant	Significant	Significant	Not significant

This evidence could be obtained in either of two ways:

- Each additional third party's auditor (or other appropriately qualified practitioner) could also prepare a TPSP auditor's report for use by all entities using that third party.

- The WebTrust auditor or the TPSP auditor could perform the appropriate assurance procedures at this additional third party.

Because it is unlikely that the third party would want a number of assurance examinations conducted at its operations, it is likely more appropriate to obtain a TPSP auditor's report.

In the situation in which the WebTrust auditor is unable to obtain evidence of the existence and effective operation of controls at the additional third-party site, a limitation in the scope of the examination would likely be present. In such a case, the WebTrust client would not be able to obtain a WebTrust seal.

Basis for TPSP Report Qualifications

The following conditions that may lead to a TPSP report qualification are not specifically unique to TPSP reporting:

- Not all relevant controls have been included (completeness).
- The relevant controls are not in place (existence).
- Controls were not found to be operating effectively.

When faced with a TPSP report qualification, the WebTrust practitioner should follow the guidance outlined within this material. This is set out at the end of the WebTrust practitioner guidance that follows this section.

Restrictions on Use

Although the practitioner cannot control the distribution of a TPSP report, the practitioner can restrict its use. Although there is no requirement that the TPSP practitioner's report be restricted

in its use, it is the preference of the Task Force that use be limited to the management of the TPSP, its customers, and their WebTrust practitioners. As a result, there is a restricted use paragraph included in the illustrative report examples. The report itself covers only the part of the WebTrust control structure that is performed by the TPSP. By limiting use, the practitioner potentially limits misinterpretation by unsophisticated users.[5]

Documentation Requirements

Documentation requirements for this type of engagement do not differ significantly from other types of assurance engagements. The documentation should be sufficient to support the opinion expressed in the report and provide evidence that the examination was performed in accordance with accepted standards. The following aspects of a TPSP examination engagement should be considered for documentation:

- Engagement understanding
- Planning activities
- Risk assessment
- Description of the system
- Evidence of understanding of the system and preliminary evaluation of the design of controls
- Testing and other examination procedures undertaken
- Written management representation regarding the controls and management's responsibilities in relation thereto
- Evaluation of audit evidence to support the opinion rendered

[5] In making a decision whether to restrict the permitted uses of the report, the TPSP practitioner should consider the likelihood that WebTrust practitioners may refer to the TPSP practitioner's report and the related likelihood that users of the WebTrust practitioner's reports will need access to the TPSP practitioner's report.

SAMPLE TPSP PRACTITIONER REPORTS

Appendix One illustrates the suggested formats for reporting under AICPA standards and under CICA standards. Illustrations No. 1 and No. 3 are prepared in accordance with the AICPA's attestation standards. Illustrations No. 2 and No. 4 are prepared in accordance with the CICA's assurance standards. In Appendix Two, these illustrations are applied to two case study situations. Illustrations No. 1 and No. 2 are prepared for the business-to-consumer example (the TPSP report is prepared for NoWallsMall.net) with respect to the WebTrust Business Disclosure/Transaction Integrity and Privacy Principles. Illustrations No. 3 and No. 4 are prepared for the business-to-business example (the TPSP report is prepared for OuiBServices.com) for the WebTrust Confidentiality Principle.

Under the United States attestation standards, there are two ways to report, either a report on management's assertion or a direct report on the subject matter. When reporting on management's assertion, the first paragraph of the practitioner's report states that the practitioner has performed an examination of management's assertion about compliance with the WebTrust criteria. Illustration No. 1 is a report in which the practitioner opines on management's assertion. Illustration No. 2 is a report in which the practitioner opines directly on the subject matter.

Both attest and direct engagements and reporting are supported in Canada. The practitioner's communication varies depending on whether the assurance engagement is an attest engagement or a direct reporting engagement. In an attest engagement, the practitioner's conclusion will be on a written assertion prepared by the accountable party. Using suitable criteria, the assertion relates to the subject matter for which the accountable party is responsible. In a direct reporting engagement, using suitable criteria, the practitioner's conclusion relates directly the subject matter for which the accountable party is responsible. Illustration No. 3 is a report in which the practitioner opines directly on the subject matter, and Illustration No. 4 is a report in which the practitioner opines on management's assertion.

In all reporting situations, TPSP management's description of controls, that supports compliance by a WebTrust client with the criteria related to the selected WebTrust Principles, should accompany the TPSP Auditor's report.

Based on the above, either reporting approach could be used in a specific situation. Because the description of controls attached to the report is management's representation, the attest report is believed to be more suitable in this circumstance. Samples of both reports are provided, however. The reports presented are for illustrative purposes and should be modified in accordance with the applicable professional standards as the specific engagement facts and circumstances warrant.

Part II - Guidance for the WebTrust Practitioner

INTRODUCTION TO PART II

This section is based primarily on chapter 1 of Statement on Standards for Attestation Engagements No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), and Statement on Auditing Standards No. 1, *Codification of Auditing Standards and Procedures* (AICPA, *Professional Standards*, vol. 1, AU sec. 543, "Part of Audit Performed by Other Independent Auditors") in the United States, and *Handbook* sections 5025, 5310 and 6930 in Canada, as well as international standards. This section provides the WebTrust practitioner with guidance on the professional judgments that need to be made in deciding—

- Whether a WebTrust practitioner can accept an engagement when controls relevant to meeting such criteria are provided by a TPSP.
- The nature and extent of procedures to be performed by the WebTrust practitioner in order to be able to use the work of another practitioner.
- The form and content of the WebTrust practitioner's report in these circumstances.

There is a difference in standards that should be acknowledged as background for this section. In the United States, in a situation where there is a "division of responsibility," a practitioner may have an option of making reference to the work of another practitioner or not making any such reference. That decision is based on a number of factors, including the significance of the controls exercised by the TPSP. The level of work varies, with the level required for a reference situation being usually less than that where no reference is made. In Canada, there is no such option. The practitioner cannot make reference to the work of another practitioner under generally accepted auditing standards.

In the opinion of the Task Force, there should be no reference to the work of the TPSP auditor. This will avoid various problems including:

- Seal presentation issues. Normally just the issuing firm's name is located on the bottom of the seal. This could be complicated if there is a noted division in responsibility.
- Reporting issues when the TPSP limits distribution of the TPSP auditor's report or has carved out part of the engagement that is in turn performed by another TPSP auditor.

As a result, the discussion in this section is based on the auditor taking responsibility for the work of the TPSP auditor.

ACCEPTING A WEBTRUST ENGAGEMENT

The first decision that a WebTrust practitioner needs to make is whether the engagement can be accepted. There may be situations in which the processing activities and controls at the TPSP are so significant to the entire control structure or set of WebTrust Criteria that it is unlikely that the WebTrust practitioner would be willing to rely so extensively on the work of the TPSP practitioner. In that situation, the WebTrust practitioner needs to either personally perform the examination of the TPSP controls (or perform sufficient tests of the work of the TPSP practitioner) or not accept the WebTrust engagement.

For purposes of this decision, *significance* represents the relative value or importance of the specific set of principles in which the WebTrust practitioner is performing an overall WebTrust engagement. This relationship and weighting may change depending on the WebTrust practitioner's own professional judgment about the risk and the value, criticality, or degree of importance that users place on the assurances being provided in the particular environment in which the engagement is taking place. For example, the controls at a TPSP that manages many applications on behalf of its customers may be believed to be more important and more significant than the controls exercised by a TPSP that simply provides Web hosting and some physical security services for a customer.

In the first case study, readers should refer to the attachment to the TPSP auditor report and to Illustrations No. 9 and 10 (set out in Appendix Two) to assess the extent of controls and procedures exercised by NoWallsMall.net. Regarding both the Business Disclosure/Transaction

Integrity and Privacy criteria, there appears to be sufficient controls exercised at the retail Web site level that the WebTrust auditor can accept the engagement (subject to all other risk management factors being appropriately managed). Regarding security (see Illustration No. 11 in Appendix Two), however, it appears that almost all the controls are exercised by NoWallsMall.net and would be dealt with by the TPSP auditor. In order to assess whether WebTrust auditor could accept such an engagement, the following would need to be considered:

- The ability to audit certain aspects of the TPSP (NoWallsMall.net) directly (In this situation, the service agreement states that all audit evidence with respect to NoWallsMall.net must be obtained by its auditor.);
- Whether the work papers of TPSP Auditor LLP are available to WebTrust auditor to review;
- The significant monitoring controls over the activities of NoWallsMall.net that are exercised by the WebTrust client, RetailJoe.com, and that the WebTrust auditor can audit.

— It would be the decision of the WebTrust auditor to assess whether sufficient evidence exists in order to perform the audit. In this instance if TPSP Auditor LLP is the only firm that is permitted to audit the controls of TPSP, and TPSP Auditor LLP, as a matter of policy, will not make its work papers available for review by other practitioners, the WebTrust auditor may decide that the engagement cannot be accepted. As a result, in this example, if RetailJoe.com wished to have a WebTrust seal for Security, the examination may likely need to be undertaken by TPSP Auditor LLP.

Once the engagement is accepted, the second key decision that a practitioner (in the United States) will need to make is whether to make reference to the other practitioner in the WebTrust report. As mentioned above, this option is not available to WebTrust practitioners in Canada. This decision, as well as the decision of the TPSP practitioner, to set out the procedures performed, and the results thereof, will influence the extent of work that will need to be performed by the WebTrust practitioner.

ASSESSING THE IMPACT OF OTHER FORMS OF REPORTING FOR TPSP REPORT

Situations may arise in which TPSP organizations already may provide some form of third-party reporting to a broader class of customers. Such reporting includes SAS No. 70, CICA section 5900, WebTrust reports, or SysTrust reports related to various principles for the service provider or other general assurance (such as Chapter 1 of Statement on Standards for Attestation Engagements No. 10, *Attestation Standards: Revision and Recodification* [AICPA, *Professional Standards,* vol. 1, AT sec. 101] or CICA Section 5025). These existing reports are not expected to meet all the needs for TPSP reporting in support of WebTrust services without modifying and directly addressing the needs of individual WebTrust practitioners and clients.

The WebTrust auditor should obtain copies of such reports and assess whether the controls required to satisfy some of the appropriate WebTrust criteria have been audited and that the controls have been found to be operating effectively. This could be taken into account in assessing the coverage required by the TPSP report. Professional standards relating to the reliance on the work of other auditors would need to be satisfied.

PROCEDURES TO BE PERFORMED BY WEBTRUST AUDITOR

There are a number of procedures that the WebTrust practitioner should perform in any engagement where the client is being hosted by a TPSP. The WebTrust practitioner should make inquiries concerning the professional reputation and independence of the TPSP practitioner. The WebTrust practitioner should also adopt appropriate measures to assure the coordination of audit activities with those of the TPSP practitioner in order to achieve a proper review of matters affecting the overall WebTrust engagement.

Understanding Division of Controls

First of all, it is important that the practitioner consider the nature and extent of the services provided by the TPSP and how the TPSP's controls interrelate with those of the WebTrust client to meet the WebTrust Criteria. This will be important in assessing the relevance of the TPSP

practitioner's report. (As discussed earlier, this will also be a consideration in whether or not the WebTrust practitioner is in a position to accept the engagement.)

Professional Qualifications

When the qualifications of the TPSP practitioner are not known to the user of the report, inquiries may be made of any of a number of parties concerning the reputation of the TPSP practitioner. In circumstances for which the professional qualifications of the TPSP practitioner cannot be substantiated, consideration should be given to other available evidence (if such exists) and the effect this may have in assessing the usefulness of the report.

Inquiries about the professional reputation and standing of the TPSP practitioner can be made to one or more of the following:

- In the United States, with the American Institute of Certified Public Accountants, the appropriate state society of certified public accountants, the local chapter, or a combination
- In Canada, the Canadian Institute of Chartered Accountants, the appropriate Provincial Institute of Chartered Accountants, or both
- In the case of a foreign practitioner, with the corresponding professional organization
- Other practitioners
- Bankers and other credit grantors
- Other appropriate sources

Inquiries may be unnecessary if the WebTrust practitioner already knows the professional reputation and standing of the TPSP practitioner. The AICPA or CICA can confirm whether the TPSP practitioner is licensed to provide WebTrust services, which is a consideration when assessing professional qualifications.

Competence and Integrity

Before undertaking an assurance engagement, the WebTrust practitioner should be satisfied that the subject matter is or will be within the collective professional expertise of the practitioner and

other persons performing the assurance engagement. The reputation of the TPSP practitioner's competence and integrity may be well known. For example, if the TPSP practitioner is licensed to perform WebTrust examinations, no additional inquiry may be needed. There is no requirement that the TPSP practitioner be specifically licensed to perform a WebTrust examination, but the practitioner needs to be able to demonstrate appropriate knowledge of WebTrust Principles and Criteria as it pertains to this type of engagement.

In instances in which the TPSP practitioner's reputation is not known, inquiries may be made of other professional colleagues, business associates (for example, bankers), or other knowledgeable parties. Furthermore, it may be appropriate to inquire about the qualifications of the TPSP practitioner in terms of his or her knowledge of the business, knowledge of WebTrust Principles and Criteria, and the use of specialists in technical situations (for example, data processing). When there is doubt about the reputation, competence, and integrity of the TPSP practitioner, the impact on the usefulness of the report should be considered.

Professional Standards of the TPSP Practitioner's Jurisdiction

When the TPSP practitioner practices in a foreign jurisdiction, the WebTrust practitioner should consider the effect of any differences between the local country standards and the foreign country's generally accepted auditing standards relating to the conduct of the examination. This may prove to be a difficult task since, at the present time, few foreign professional bodies have adopted standards for these types of examinations. Accordingly, each report should be examined on a case-by-case basis to determine its reliability while considering the independence requirements of the TPSP practitioner.

Independence

The TPSP practitioner should be independent of the TPSP in the same way that WebTrust practitioners are required to be independent of the WebTrust client. It is generally impractical, however, and unnecessary for the TPSP practitioner to be independent with respect to each Web site that is hosted by the TPSP.

Representation should be obtained from the TPSP practitioner that the practitioner is independent of the TPSP as defined by the standards set out in the country of the engagement (for example, as prescribed by AICPA or the Rules of Professional Conduct, as prescribed by the Provincial Institutes of Chartered Accountants in Canada).

ABILITY NOT TO MAKE REFERENCE (UNITED STATES ONLY)

If the WebTrust practitioner is able to obtain satisfaction about the independence and professional reputation of the TPSP practitioner as discussed above, and takes steps appropriate to obtain satisfaction about the examination performed by the TPSP practitioner, the WebTrust practitioner may be able to prepare the WebTrust report without making reference in the report to the procedures performed by the TPSP practitioner. If this position is taken, the WebTrust practitioner should not state in the report that part of the WebTrust engagement was performed by another practitioner because to do so may cause a reader to misinterpret the degree of responsibility being assumed (this is the preferred position of the Task Force).

Ordinarily, the WebTrust practitioner would be able to adopt this position (not to make reference) when one of the following is true:

- The TPSP practitioner is an associated or correspondent firm whose work is acceptable to the WebTrust practitioner based on the WebTrust practitioner's knowledge of the professional standards and competence of that firm.

- The TPSP practitioner was retained by the WebTrust practitioner and the work was performed under the WebTrust practitioner's guidance and control.

- The WebTrust practitioner takes steps that are considered necessary to obtain satisfaction that the controls being tested are appropriate to support the WebTrust report, whether or not the WebTrust practitioner was selected by the TPSP practitioner.

Additional Procedures to be Undertaken

The amount of work depends on the type of information that the TPSP practitioner provides in the practitioner's report. In a situation in which the TPSP practitioner provides a list of the procedures performed, the results thereof, and the description of the controls with the practitioner's report, the WebTrust practitioner would first review the report and the procedures to assess whether the procedures performed were adequate and the results acceptable.

In situations in which only the controls are provided, or the WebTrust practitioner is unsure about whether the procedures performed were adequate, the WebTrust practitioner may need additional assurance. The practitioner could consider performing one or more of the following procedures:

- Visit the TPSP practitioner and discuss the procedures performed and results thereof.
- Review the examination programs of the TPSP practitioner and the work papers if so permitted. In some cases, it may be appropriate to issue instructions to the TPSP practitioner about the scope of the examination procedures to be undertaken.

In some circumstances, the WebTrust practitioner may consider it appropriate to participate in discussions regarding the controls to be tested with the TPSP management personnel and to make supplemental tests of such controls. The determination of the extent of additional procedures, if any, to be applied rests with the WebTrust practitioner alone in the exercise of professional judgment and in no way constitutes a reflection on the adequacy of the TPSP practitioner's work. Because the WebTrust practitioner in this case assumes responsibility for the WebTrust opinion without making reference to the examination performed by the TPSP practitioner, the WebTrust's practitioner's judgment should govern concerning the extent of procedures to be undertaken.

USING THE REPORT

To consider whether the objectives are being achieved, the WebTrust Practitioner needs to assess the relevance and reliability of the TPSP practitioner's report.

Relevance

In assessing the relevance of the TPSP practitioner's examination, the focus should be directed toward the scope of the examination. For the purposes of this discussion, the reporting package also includes the appendices that cover management's assertions (when an attest report is used). Factors to be considered include the following:

- The boundaries of the services covered in the report and the description of the controls
- The appropriateness and the scope of the description of controls
- The time period covered
- The controls in place at the WebTrust client

These factors should be considered independently when assessing the relevance of a TPSP report. Where the findings from the assessment of any one factor indicate that the user's objectives will not be achieved, the relevance of the report should be questioned and consideration given to the degree of reliance to be placed on the report.

Boundary of Services Covered

Because of the range of services that a TPSP might perform, there is no guarantee that a TPSP practitioner's report will cover all the controls associated with a particular service, or systems that interface with that service. The WebTrust practitioner should be aware of this when considering the relevance of the TPSP practitioner's report.

Accordingly, the WebTrust practitioner should review the description of controls to ensure that it completely and adequately addresses the systems or services relevant to particular needs of that WebTrust engagement.

Appropriateness and Scope of the Description of Controls

The level of detail to which stated controls are described could present difficulties for WebTrust practitioners in assessing the relevance of a TPSP practitioner's report. A concern is that the controls may not be described in sufficient detail for a WebTrust practitioner to ascertain

whether a specific control has been examined. This should not ordinarily occur as it is the responsibility of the TPSP auditor to assess whether the description is sufficient and perform appropriate test procedures. In such cases, it may be necessary to obtain further details from the TPSP, discuss the issue with TPSP management, or, as a last resort, contact the TPSP practitioner, because the assumption cannot be made that the specific control is, in fact, included within the scope of the TPSP report.

If it is determined by a WebTrust practitioner that evidence relating to a particular control is crucial to the examination of the WebTrust client, and that the control is not addressed by the TPSP practitioner's report, the options of the WebTrust practitioner are limited. Consideration should be given to a request, through the TPSP, that the TPSP practitioner extend the scope of the examination to include the important control. Failing this, the WebTrust client may request that the TPSP grant the necessary access to enable the WebTrust practitioner to evaluate and directly test the critical control. If either alternative is not feasible, the WebTrust practitioner needs to consider whether other sources of evidence are available. If none is available, the practitioner needs to consider whether a scope limitation exists, in which case a WebTrust seal would not be issued.

Time Period Covered

The time period covered by the TPSP practitioner's examination is critical to the WebTrust practitioner in assessing the report's relevance. Ideally, the period of coverage of the TPSP reporting should coincide with the frequency established by the individual WebTrust clients. As the interval from the period covered by the TPSP practitioner's report and the period covered by the WebTrust practitioner's report lengthens, there would be more risk to the WebTrust practitioner that there could be changes in the controls at the TPSP that could affect the WebTrust client. This additional risk would have to be either accepted or reduced to an acceptable level by the WebTrust practitioner.

One of the factors that need to be considered in making this assessment is the client's process for identifying changes. It is important that the WebTrust client have a suitable process in place to

identify changes in controls at the TPSP and their impact on the client. Nevertheless, it is the AICPA/CICA Electronic Commerce Assurance Services Task Force's opinion that the period of coverage of the TPSP report should cover a substantial portion of the reporting period provided at the WebTrust client level. Ideally, the time periods would coincide. This period will have to take into account the time needed by the TPSP practitioner to complete the examination and render the TPSP audit report.

The Controls in Place at the WebTrust Client

In many situations in which services are provided by a TPSP, a combination of WebTrust client controls and TPSP controls is required to achieve compliance with the WebTrust Criteria.

The TPSP practitioner's report is prepared from the perspective of a "closed" control structure; it addresses the controls over the services provided within the boundaries of the TPSP only. These types of reports place the onus on the WebTrust practitioner to properly identify the controls that should have been implemented at the WebTrust client to ensure that a comprehensive system of control is examined. In these circumstances, the WebTrust practitioner should first understand the systems and the related controls within the WebTrust client. This understanding should then be supplemented by a review of the contract between the TPSP and the WebTrust client and other documentation (for example, a user manual), as appropriate, prepared by the TPSP. Discussions should be held with WebTrust client management about their control responsibilities (either perceived or contracted). The combination of these three procedures and review of the TPSP report should generally be sufficient to gain a proper understanding of the control structure. Caution should nevertheless be exercised concerning the completeness and accuracy of the documentation provided by the TPSP. Consideration should be given to having the TPSP practitioner report in this regard, particularly where the design, implementation and ongoing effectiveness of WebTrust client controls depends on this documentation highly.

WebTrust client controls may be needed to compensate for design weaknesses in the control structure at the TPSP. Such weaknesses may be knowingly accepted by the TPSP and intended to be mitigated by the implementation of specific WebTrust client controls. This situation may

arise where certain controls can be more cost-effectively implemented by WebTrust client than by the TPSP. In these cases, it is the responsibility of the WebTrust practitioner to ensure that the WebTrust client controls are in place and operating effectively to complement the evidence provided in the TPSP practitioner's report.

Reliability

In assessing the reliability of the examination, the focus should be directed toward the TPSP practitioner's capability to conduct the examination. Qualities or characteristics used to make this assessment include the following:

- The professional qualifications of the TPSP practitioner
- The competence and integrity of the TPSP practitioner
- The adequacy of the standards of the jurisdiction in which the TPSP practitioner practices
- The nature and extent of tests of controls performed by the TPSP practitioner

The first three of these were addressed previously.

The Nature and Extent of Tests of Controls Performed by the TPSP Practitioner

It is not necessary for the WebTrust practitioner to understand, in detail, the nature and extent of procedures performed, because these determinations are the responsibility of the TPSP practitioner in forming an opinion based on professional judgment. Circumstances may arise, however, where the WebTrust practitioner has reason to believe that the work performed by the TPSP practitioner is not sufficient for issuing a WebTrust report at the WebTrust client and additional evidence may be needed. In these circumstances, inquiry of the TPSP and, when necessary, the TPSP practitioner may be appropriate to resolve the WebTrust practitioner's concern. Although, the working papers of the TPSP practitioner may not generally be available for review by the WebTrust practitioner, such review may be required to clarify the extent of procedures performed, or to provide to the WebTrust practitioner the basis for accepting responsibility for the audit work performed by the TPSP practitioner, and therefore, not referring to the work of such TPSP practitioner in the WebTrust practitioner's report.

TPSP PRACTITIONER'S REPORT DEPARTS FROM STANDARD REPORT

If the TPSP practitioner's report is other than a standard report, the WebTrust practitioner should decide whether the reason for the departure from the standard report is of such nature and significance in relation to the overall WebTrust engagement that it would require recognition in the WebTrust practitioner's report. If the reason for the departure is not material in relation to the overall WebTrust engagement, the WebTrust practitioner need not make reference in the report to such departure.

If the results of inquiries and procedures by the WebTrust practitioner about matters described in this section lead to the conclusion that the WebTrust practitioner can neither assume responsibility for the work of the TPSP practitioner insofar as that work relates to the WebTrust practitioner's report, nor report in the manner set forth previously, the WebTrust practitioner should qualify the report or issue a disclaimer (pursuant to AT section 101 in the United States and *Handbook* section 5025 in Canada). As a practical matter, most clients would not want a qualified report to be issued because it would preclude obtaining a WebTrust seal.

Appendix One- Illustrative Audit Reports

This appendix illustrates the suggested formats for reporting under AICPA standards and under CICA standards. Illustrations No. 1 and No. 3 are prepared in accordance with the AICPA's attestation standards. Illustrations No. 2 and No. 4 are prepared in accordance with the CICA's assurance standards.

Under the United States attestation standards, there are two ways to report, either a report on management's assertion or a direct report on the subject matter. When reporting on management's assertion, the first paragraph of the practitioner's report states that the practitioner has performed an examination of management's assertion about compliance with the WebTrust criteria. Illustration No. 1 is a report in which the practitioner opines on management's assertion. Illustration No. 2 is a report in which the practitioner opines directly on the subject matter.

Both attest and direct engagements and reporting are supported in Canada. The practitioner's communication varies depending on whether the assurance engagement is an attest engagement or a direct reporting engagement. In an attest engagement, the practitioner's conclusion will be on a written assertion prepared by the accountable party. Using suitable criteria, the assertion evaluates the subject matter for which the accountable party is responsible. In a direct reporting engagement, using suitable criteria, the practitioner's conclusion evaluates directly the subject matter for which the accountable party is responsible. Illustration No. 3 is a report in which the practitioner opines directly on the subject matter, and Illustration No. 4 is a report in which the practitioner opines on management's assertion.

In all reporting situations, TPSP management's description of controls, that supports compliance by a WebTrust client with the criteria related to the selected WebTrust Principles, should accompany the TPSP Auditor's report.

Based on the above, either reporting approach could be used in a specific situation. Because the description of controls attached to the report is management's representation, the attest report is believed to be more suitable in this circumstance. Samples of both reports are provided, however. The reports presented are for illustrative purposes and should be modified in accordance with the applicable professional standards as the specific engagement facts and circumstances warrant.

Illustration No. 1, for Use in the United States

Independent Accountant's Report

To the Management of TPSP:

We have examined the following [accompanying] assertion by the management of TPSP that, with respect to services provided to customers—

- The description of controls presented in Attachment 1 are controls for which TPSP is responsible; and
- The controls presented in Attachment 1 operated effectively, in all material respects, during the period _____ through _____

and contribute to compliance with the AICPA/CICA WebTrust™ Criteria.

The description of controls, and the effectiveness of those controls, are the responsibility of TPSP's management. Our responsibility is to express an opinion 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 TPSP's services provided to its customers, who have or desire to have, a CPA WebTrust examination related to customer's electronic commerce (e-commerce) business and privacy practices for e-commerce transactions and the related controls over privacy and the processing of such transactions, (2) selectively testing transactions executed in accordance with disclosed business and privacy 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.

In our opinion, TPSP's management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA/CICA WebTrust Criteria.

Because of inherent limitations in controls, error 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 the validity of such conclusions may be altered because of (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) a deterioration in the degree of compliance with the policies or procedures.

This information has been provided to customers of TPSP and to their practitioners to be taken into consideration, along with the information about controls at customers, when evaluating the customer's controls in relation to the AICPA/CICA WebTrust Business Practices/Transaction Integrity Criteria and the WebTrust Privacy Criteria. The relative effectiveness and significance of specific controls at TPSP and their effect on assessments of controls at customers depend on their interaction with the controls and other factors present at individual customer organizations. We have performed no procedures to evaluate the effectiveness of controls at individual customers.

This report is intended solely for the information and use of the management of TPSP, its customers, and their independent WebTrust practitioners and is not intended to be, and should not be, used by anyone other than those specified parties.

This report does not include any representations as to the quality of services beyond those covered by the accompanying description of controls, nor to the suitability of any of TPSP's services for any customer's intended purposes.

TPSP Auditor LLP
Certified Public Accountants
City, State
Date of Report

Illustration No. 2, for Use in Canada

Auditor's Report

To the Management of TPSP:

We have audited the following [accompanying] assertion by the management of TPSP that, with respect to services provided to Web site customers—

- The accompanying description of controls presented in Attachment One are controls for which TPSP is responsible that, when combined with a customer's procedures, contribute to compliance with AICPA/CICA WebTrust™ criteria; and
- The controls presented in Attachment One operated effectively during the period from _____ to _____.

TPSP's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our audit.

Our audit was made in accordance with standards for assurance engagements established by the Canadian Institute of Chartered Accountants. Those standards require that we plan and perform our audit to obtain reasonable assurance that management's assertion is not materially misstated. Our audit included (1) obtaining an understanding of TPSP's services provided to its customers who have, or desire to have, a WebTrust audit related to the customer's electronic commerce (e-commerce) business and privacy practices for e-commerce transactions and the related controls over privacy and the processing of such transactions, (2) selectively testing transactions executed in accordance with disclosed business and privacy 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 audit provides a reasonable basis for our opinion.

In our opinion, TPSP's management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, in conformity with the AICPA/CICA WebTrust Criteria.

This information has been provided to customers of TPSP and to their auditors to be taken into consideration, along with the information about controls at customers, when evaluating the customer's controls in relation to the AICPA/CICA WebTrust Business Practices/Transaction Integrity Criteria and the WebTrust Privacy Criteria. The relative effectiveness and significance of specific controls at TPSP and their effect on assessments of controls at customers depend on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual customers.

Because of inherent limitations in controls, error 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 the validity of such conclusions may be altered because of (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) a deterioration in the degree of compliance with the policies or procedures.

This report is intended solely for the information and use of the management of TPSP, its customers, and their independent WebTrust practitioners and is not intended to be, and should not be, used by anyone other than those specified parties.

This report does not include any representations as to the quality of services beyond those covered by the accompanying description of controls, nor to the suitability of any of TPSP's services for any customer's intended purposes.

City, Province
Date of Report

TPSP Auditor LLP
Chartered Accountants

Illustration No. 3, for Use in the United States (Direct Report)

Independent Accountant's Report

To the Management of TPSP:

We have examined the description of controls presented in Attachment One for which TPSP is responsible with respect to services provided to Web site customers that, when combined with a customer's procedures, contribute to compliance with the AICPA/CICA WebTrust Criteria, and the effectiveness of those controls during the period from _____ to _____.

The description of controls, and the effectiveness of those controls, are the responsibility of TPSP's management. Our responsibility is to express an opinion 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 TPSP's services provided to its customers that have, or desire to have, a CPA WebTrust examination related to the customer's electronic commerce (e-commerce) confidentiality practices and the related controls over confidentiality; (2) selectively testing transactions executed in accordance with disclosed confidentiality 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.

In our opinion, the controls maintained by TPSP presented in Attachment One, operated effectively during the period _____ through _____, in all material respects, based on the AICPA/CICA WebTrust Criteria.

Because of inherent limitations in controls, error 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 the validity of such conclusions may be altered because of (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) a deterioration in the degree of compliance with the policies or procedures.

This information has been provided to customers of TPSP and to their practitioners to be taken into consideration, along with the information about controls at customers, when evaluating the customer's controls in relation to the AICPA/CICA WebTrust Confidentiality Criteria. The relative effectiveness and significance of specific controls at TPSP and their effect on assessments of controls at customers depend on their interaction with the controls and other factors present at individual customer organizations. We have performed no procedures to evaluate the effectiveness of controls at individual customers.

This report is intended solely for the information and use of the management of TPSP, its customers, and their independent WebTrust practitioners and is not intended to be, and should not be, used by anyone other than those specified parties.

This report does not include any representations as to the quality of services beyond those covered by the accompanying description of controls, nor to the suitability of any of TPSP's services for any customer's intended purposes.

TPSP Auditor LLP
Certified Public Accountants
City, State
Date of Report

Illustration No. 4, for Use in Canada (Direct Report)

Auditor's Report

To the Management of TPSP:

With respect to services provided to Web site customers, we have audited TPSP's description of those controls for which TPSP is responsible that, when combined with a customer's procedures, contribute to compliance with the AICPA/CICA WebTrust Criteria and the effectiveness of those controls during the period from _____ to _____. The controls are outlined in Attachment One.

The description and the controls are the responsibility of TPSP's management. Our responsibility is to express an opinion on the conformity of the description and the controls with the AICPA/CICA WebTrust Criteria based on our audit.

Our audit was made in accordance with standards for assurance engagements established by the Canadian Institute of Chartered Accountants. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of TPSP's services provided to its customers who have, or desire to have, a WebTrust audit insofar as they relate to the customer's electronic commerce (e-commerce) confidentiality practices and the related controls over confidentiality, (2) selectively testing transactions executed in accordance with disclosed confidentiality 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 audit provides a reasonable basis for our opinion.

In our opinion, in all material respects, the controls maintained by TPSP as presented in Attachment One operated effectively during the period from _____ to _____ in conformity with the AICPA/CICA WebTrust Criteria.

This information has been provided to customers of TPSP and to their auditors to be taken into consideration, along with the information about controls at customers, when evaluating the customer's controls in relation to the AICPA/CICA WebTrust Criteria. The relative effectiveness and significance of specific controls at TPSP and their effect on assessments of controls at customers are dependent on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual customers.

Because of inherent limitations in controls, error 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 the validity of such conclusions may be altered because of (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) a deterioration in the degree of compliance with the policies or procedures

Because of inherent limitations in controls, error 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 the validity of such conclusions may be altered because of (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) a deterioration in the degree of compliance with the policies or procedures.

This report is intended solely for the information and use of the management of TPSP, its customers, and their independent WebTrust practitioners and is not intended to be, and should not be, used by anyone other than those specified parties.

This report does not include any representations as to the quality of services beyond those covered by the accompanying description of controls, nor to the suitability of any of TPSP's services for any customer's intended purposes.

City, Province **TPSP Auditor LLP**

Date of Report **Chartered**

Accountants

Illustration No. 5 - Illustrative Controls Attachment

Attachment One To Auditor's Report

TPSP NAME

PERIOD OF COVERAGE

The following controls that exist at TPSP have been identified by TPSP management as contributing to the ability of TPSP clients to achieve compliance with the criteria related to the selected WebTrust Principles. Additional control procedures at individual TPSP clients may be necessary for a TPSP client to achieve compliance with all of the criteria for a selected principle.

PRINCIPLE SELECTED

Controls at TPSP

- List controls

PRINCIPLE SELECTED

Controls at TPSP

- List controls

PRINCIPLE SELECTED

Controls at TPSP

- List controls

Illustration No. 6 - Illustrative Management Assertion

TPSP makes the following assertion with respect to services provided to its customers,

- The description of controls set out in Appendix One presents those controls for which TPSP is responsible; and
- The controls set out in Appendix One operated effectively, in all material respects, during the period _July 1, 20xx_ through _December 31, 20xx;

and contribute to compliance with the AICPA/CICA WebTrust™ Criteria.

Appendix Two - Case Study Examples

Appendix Two applies the illustrative audit report guidance in Appendix One to the two case studies described earlier. Illustrations No. 7 and No. 8 are prepared for the business-to-consumer example (the TPSP report is prepared for NoWallsMall.net) with respect to the WebTrust Business Disclosure/Transaction Integrity and Privacy Principles. Illustrations No. 12 and No. 13 are prepared for the business-to-business example (the TPSP report is prepared for OuiBServices.com) for the WebTrust Confidentiality Principle.

In this business-to-consumer example, the potential controls exercised at RetailJoe.com have been illustrated to show a possible interrelationship that RetailJoe.com's WebTrust auditor might encounter. Since the TPSP auditor would not be aware of the controls exercised at the retail client, they would not be included in the TPSP Auditor's report.

EXAMPLE ONE – ILLUSTRATIVE BUSINESS-TO-CONSUMER CASE STUDY

The example was discussed in detail earlier in this Guide. In order to assist in the understanding the content of Appendix One to the TPSP auditor's report (the controls attachment) and how they could interrelate with the controls and procedures at the WebTrust client, this first example sets out illustrative controls for both parties. This is for illustration only. Normally the details of the controls exercised at the WebTrust client would not be known to the TPSP, nor would it be the TPSP's responsibility to make sure that such controls were exercised at the WebTrust client level. These illustrated controls are set out as Illustration No. 10.

Illustration No. 7, for Use in the United States - NoWallsMall.net

Independent Accountant's Report

To the Management of NoWallsMall.net:

We have examined the following [accompanying] assertion by the management of NoWallsMall.net (NWM) that, with respect to services provided to customers—

- The description of controls, presented in Attachment One, are controls for which NWM is responsible; and
- The controls presented in Attachment One operated effectively, in all material respects, during the period _____ through _____

and contribute to compliance with the AICPA/CICA WebTrust™ Criteria.

The description of controls, and the effectiveness of those controls, are the responsibility of NWM's management. Our responsibility is to express an opinion 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 NWM's services provided to its customers, who have or desire to have, a CPA WebTrust examination related to the customer's electronic commerce (e-commerce) business and privacy practices for e-commerce transactions and the related controls over privacy and the processing of such transactions, (2) selectively testing transactions executed in accordance with disclosed business and privacy 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.

In our opinion, NWM's management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA/CICA WebTrust Criteria.

Because of inherent limitations in controls, error 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 the validity of such conclusions may be altered because of (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) a deterioration in the degree of compliance with the policies or procedures.

This information has been provided to customers of NWM and to their practitioners to be taken into consideration, along with the information about controls at customers, when evaluating the customer's controls in relation to the AICPA/CICA WebTrust Business Practices/Transaction Integrity Criteria and the WebTrust Privacy Criteria. The relative effectiveness and significance of specific controls at NWM and their effect on assessments of controls at customers depend on their interaction with the controls and other factors present at individual customer organizations. We have performed no procedures to evaluate the effectiveness of controls at individual customers.

This report is intended solely for the information and use of the management of NWM, its customers, and their independent WebTrust practitioners and is not intended to be, and should not be, used by anyone other than those specified parties.

This report does not include any representations as to the quality of services beyond those covered by the accompanying description of controls, nor to the suitability of any of NWM's services for any customer's intended purposes.

TPSP Auditor LLP
Certified Public Accountants
City, State
Date of Report

Illustration No. 8, for Use in Canada - NoWallsMall.net

Auditor's Report

To the Management of NoWallsMall.net:

We have audited the following [accompanying] assertion by the management of NoWallsMall.net. (NWM) that, with respect to services provided to Web site customers—

- The description of controls, presented in Attachment One, are controls for which NWM is responsible that, when combined with a customer's procedures, contribute to compliance with AICPA/CICA WebTrust™ criteria; and
- The controls presented in Attachment One operated effectively during the period from _____ to _____.

NWM's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our audit.

Our audit was made in accordance with standards for assurance engagements established by the Canadian Institute of Chartered Accountants. Those standards require that we plan and perform our audit to obtain reasonable assurance that management's assertion is not materially misstated. Our audit included (1) obtaining an understanding of NWM's services provided to its customers who have, or desire to have, a WebTrust audit related to the customer's electronic commerce (e-commerce) business and privacy practices for e-commerce transactions and the related controls over privacy and the processing of such transactions, (2) selectively testing transactions executed in accordance with disclosed business and privacy 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 audit provides a reasonable basis for our opinion.

In our opinion, NWM's management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, in conformity with the AICPA/CICA WebTrust Criteria.

This information has been provided to customers of NWM and to their auditors to be taken into consideration, along with the information about controls at customers, when evaluating the customer's controls in relation to the AICPA/CICA WebTrust Business Practices/Transaction Integrity Criteria and the WebTrust Privacy Criteria. The relative effectiveness and significance of specific controls at NWM and their effect on assessments of controls at customers depend on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual customers.

Because of inherent limitations in controls, error 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 the validity of such conclusions may be altered because of (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) a deterioration in the degree of compliance with the policies or procedures.

This report is intended solely for the information and use of the management of NWM, its customers, and their independent WebTrust practitioners and is not intended to be, and should not be, used by anyone other than those specified parties.

This report does not include any representations as to the quality of services beyond those covered by the accompanying description of controls, nor to the suitability of any of NWM's services for any customer's intended purposes.

City, Province
Date of Report

TPSP Auditor LLP
Chartered Accountants

Illustration No. 9 - NoWallsMall.net Controls Attachment

Attachment One to TPSP Practitioner Report

NoWallsMall.net
PERIOD OF COVEREGE

Description of Services Provided by TPSP (Optional)

NoWallsMall.net is a third-party service provider that provides e-commerce business support activities to organizations offering goods or services over the Internet for sale in a virtual shopping mall business model. In general, NoWallsMall.net provides all the Internet infrastructure services for retailers to establish retail stores while allowing them to focus on the business aspects of their e-commerce activities. RetailJoe.com has been established as a sample typical retailer that uses NoWallsMall.net's services.

Included in NoWallsMall.net's services are the following activities:

- Web page design, development, and maintenance assistance
- Tailoring of NoWallsMall.net's proprietary order-taking and fulfillment software to enable the client's specified e-commerce activities over the Internet
- All subsequent application system enhancement, modification, and testing
- Web server acquisition, configuring, and implementation
- Ongoing Web server and related technology configuration and maintenance
- Internet service provision for e-commerce and general uses
- Communications connectivity from the Internet through to a client's processing application(s)
- Telecommunications security
- Internet firewall configuration, maintenance, and monitoring
- Maintenance of a secure e-commerce processing environment

- Maintaining the confidentiality (privacy) of client information

In specific client situations only, systems development and maintenance services in connection with client-owned application systems are provided. These services are not uniform across NoWallsMall.net's client base and are therefore not included in the examination.

Controls

The following controls that exist at NoWallsMall.net have been identified by NoWallsMall.net management as contributing to the ability of NoWallsMall.net clients to achieve compliance with the criteria related to the selected principles. Additional control procedures at individual NoWallsMall.net clients may be necessary for a NoWallsMall.net client to achieve compliance with all of the criteria for a selected principle.

Supporting Privacy

Controls at NoWallsMall.net

- NoWallsMall.net's defined privacy policy details access privileges, information collection needs, accountability, and other such matters. The policy is compared quarterly to NoWallsMall.net's clientele for compliance with clients' defined privacy policiesy. It is available for review and is reviewed and/or updated at quarterly management meetings and undergoes an intense review on an annual basis.

- NoWallsMall.net's privacy policies are reviewed with new employees as part of their orientation, and the key elements of the policies and their impact on the employees are discussed. The employees must then sign a statement signifying that they have read, understand, and will follow the policy. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the policies.

- All NoWallsMall.net employees are aware of and follow the entity's published privacy policies. Employees who deal with personally identifiable information have undergone a privacy training and awareness program before processing.

- Only NoWallsMall.net employees who deal with personally identifiable information within the performance of their assigned job duties (for example, customer service representatives, marketing personnel, and other customer contact personnel) are subject to privacy training and awareness programs.

- NoWallsMall.net's privacy policies are available and accessible via the company's intranet and within the NoWallsMall.net Employee's Handbook.

- Management has assigned responsibility for enforcement of the NoWallsMall.net privacy and security policies to the chief legal officer (CLO). Others on the executive committee assist in the review and update of the policies as outlined in the executive committee handbook.

- NoWallsMall.net has budgeted for privacy and security training for the information technology (IT) department. This amount is reviewed quarterly to ascertain whether additional training is needed based on employee feedback as well as changes in privacy and security policies and procedures at both NoWallsMall.net and its clients. The CIO evaluates this training plan and makes a quarterly report to the executive committee.

- Management reviews its disclosed privacy policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. Management makes any changes or needed modifications to the policy or disclosure within five business days of its evaluation.

- Laws and regulations that affect the disclosed site privacy policy are evaluated and reported on by the corporate attorney at least annually or when new regulations require an update.

- New users are given a secure session in which to provide new user information and select an appropriate user identification (ID) and password.

- New users provide information in a a secure socket layer (SSL) session. User IDs and passwords are provided to users and must contain non-alphanumeric characters.

- All users are required to provide a unique user ID and password to place an order or access their specific customer information.

- To update, change, or delete user information, the user's current ID and password are required. After providing this information in a secure session, the user can proceed to the user profile section for any changes.

- Logical access control procedures (for example, firewalls, routers, and password controls) are maintained by the information technology (IT) department. These controls are tested on a periodic basis by performing penetration

- Customers are required to enter a user ID and password to access their personal information and orders. A challenge word or phrase (for example, favorite sport or music—not a word that is easily identifiable, such as mother's maiden name) is stored on the system in the event a user forgets or misplaces a password.

- Or, the use of strong authentication and authorization procedures are in place. The authentication process allows the user to access only information relevant to that particular user. Other methods are in place to detect users attempting to guess another password or if a brute force attack is under way. If such an attack is detected, the system will disconnect from the user and report the security breach for follow up.

- Employee access to its data file and its customer's data file is limited to individuals based upon their assigned responsibilities. Idle workstations are timed-out after thirty minutes. Access to the corporate information technology facilities is limited to authorized employees by use of a card key system supported by video surveillance monitoring.

- Private information is protected during transmission by using 128-bit encryption technology (SSL technology).

- NoWallsMall.net meets with its technology vendors on a regular basis.

- Identified vendor security issues are documented and conveyed to the vendor by the appropriate level of management, depending on the severity of the exposure and risks associated with its planned or current deployment in the network.

- Resolutions to all vendor security issues are associated with agreed-upon time frames and followed up on by a NoWallsMall.net representative.

- NoWallsMall.net establishes customer support agreements specifically outlining security and privacy requirements of customer information

- NoWallsMall.net establishes customer support agreements specifically outlining security and privacy requirements of customer information.

- Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has access to other individuals or entities.

- Appropriate access controls are in place that limit access to sensitive, confidential, or private information based on job function and need.

- The entity only accepts information directly from the customer. Basic reasonableness tests are performed, and the customer may be asked to confirm information that does not conform to expected norms.

- Each input function requires that the customer confirm the entry by pressing the OK key.

- NoWallsMall.net establishes customer support agreements specifically outlining security and privacy requirements of customer information.

- Noncompliance situations are corrected when discovered and remedial actions taken are closely monitored for thirty days to prevent recurrence.

- The entity requests the customer's permission before it intentionally stores, alters, or copies information (such as cookies and other similar files) in the customer's computer.

- The entity requests the customer's permission before it performs any diagnostic or inventory on the customer's computer.

- NoWallsMall.net establishes customer support agreements specifically outlining security and privacy requirements of customer information. Amendments reducing the security or privacy requirements of such agreements are implemented only when the customer is notified and approves such amendment(s). Until such time, the previous (stricter) privacy policy is adhered to with respect to customer's personal information.

- Commercial and other monitoring software (for example, COPS, SATAN, and ISS) are run on a routine basis. The reports output from these programs are analyzed for potential weaknesses and threats to the systems.

- Legal counsel for the company reviews NoWallsMall.net's privacy policy on an annual basis to assess whether modifications are required.

- NoWallsMall.net is active in current public policy forums and monitors these forums for possible impact on its privacy policy and those of its clientele.

- NoWallsMall.net subscribes to publications and user groups specific to its industry and application in order to receive the most current security information. On a monthly basis, the Webmaster reports to the CIO any weaknesses perceived in the system. Management reviews this report for follow-up and resolution. Quarterly, this information is communicated to customer's

- Weekly IT staff meetings are held to address current security concerns and the findings are discussed at quarterly management meetings.

- Senior management reviews the security policy on a semi-annual basis and considers developments in technology and the impact of any laws or regulations.

- System logs are monitored and evaluated on a daily basis. Monitoring software is in place that will notify the IT manager via e-mail and pager should any incident be in progress. If an incident occurs, a report is filed within twenty-four hours for follow-up and analysis.

- Customers are directed to an area of the Web site to post a message about breaches or suspected breaches as soon as they become concerned. These customer comments are followed up within twenty-four hours for evaluation and a report is issued to the customer and the CIO or the customer may contact the Incident Response hot line any time by telephoning (888) 911-0911.

- All such incidences are communicated to customers within twenty-four hours.

Supporting Business Practices/Transaction Integrity

Controls at NoWallsMall.net

- NoWallsMall.net's policy related to security and transaction integrity is reviewed with new employees as part of their orientation, and the key elements of the policy and its impact on the employees are discussed. The employees must then sign a statement signifying that they have read, understand, and will follow the policy. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the policy.
- NoWallsMall.net's policy is available and accessible via the company's intranet and within the NoWallsMall.net Employee's Handbook.
- Management has assigned responsibility for enforcement of the NoWallsMall.net transaction integrity policy to the chief legal officer (CLO). Others on the executive committee assist in the review and update of the policies as outlined in the executive committee handbook.
- Management reviews its disclosed transaction integrity and related security policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. Management makes any changes or needed modifications to the policy or disclosure within five business days of its evaluation.
- Laws and regulations that affect the disclosed site privacy policy are evaluated and reported on by the corporate attorney at least annually or when new regulations require an update
- NoWallsMall.net provides new users a secure session in which to provide new user information and select an appropriate user ID and password.Passwords must contain at least six characters, one of which is non-alphanumeric.
- To enter the site all customers are required to provide a unique user ID and password. These passwords are case sensitive and need to be updated every ninety days consistent with RetailJoe.com's policy.
- To update, change, or delete user information, the user's current ID and password are required. After providing this information in a secure session, the user can proceed to the user profile section for any changes.
- Remote access is provided to key employees. The system accepts remote calls, verifies the user, and then hangs up and calls the user back at the authorized number.
- Logical access (for example, firewalls, routers, and password controls) is maintained by the IT department. These controls are tested on a periodic basis by performing penetration testing from both within the internal network and from the Internet.
- Identification and authentication is accomplished through the combination of a user ID and one-time password.
- The remote access to and use of the computing resources are restricted by the implementation of an authentication mechanism of identified users and resources associated with access rules. User IDs and passwords are stored in an encrypted database, with the associated encryption key stored off-line.
- Customers are required to enter a user ID and password to access private customer information and orders. Customer sessions between the browser and e-commerce systems are protected to avoid other users from hijacking a customer's session.

- Employee access to its data file and its customer's data file is limited to individuals based upon their assigned responsibilities. Idle workstations are timed out after thirty minutes. Access to the corporate IT facilities is limited to authorized employees by use of a card key system supported by video surveillance monitoring.

- The company uses 128-bit encryption for all transmission of private or confidential information, including user ID and password. Users are also encouraged to upgrade their browser to the most current version to avoid any possible security problems.

- NoWallsMall.net meets with its technology vendors on a regular basis.
- Identified vendor security issues are documented and conveyed to the vendor by the appropriate level of management, depending on the severity of the exposure and risks associated with its planned or current deployment in the network.
- Resolutions to all vendor security issues are associated with agreed-upon time frames and followed up on by a NoWallsMall.net representative.

- System logs are monitored and evaluated on a daily basis. Monitoring software is in place that will notify the IT manager via e-mail and pager should any incident be in progress. If an incident occurs, a report is filed within twenty-four hours for follow-up and analysis.

- Customers are directed to an area of the Web site to post a message about security breaches or possible breaches as soon as they become concerned. These customer comments are followed up within twenty-four hours for evaluation and a report is issued to the customer or the customer may contact the Incident Response hot line at any time by telephoning (888) 911-0911.

- Web scripts contain error checking for invalid inputs.

- The NowallMall.net order entry automatically checks each order for accuracy and completeness of information before processing. All customer-provided information for the order is displayed to the customer. Customer accepts an order, by clicking "yes," before the order is processed

- Before a transaction is processed by the company, the customer is presented with a request to confirm the intended transaction and the customer is required to click on the "Yes, please process this order" button before the transaction is then processed.

- The NoWallsMall.net order entry and fulfillment system produces packing slips from the customer sales order. Commercial delivery methods are used that reliably meet expected delivery schedules.

- Service delivery targets are maintained and actual services provided are monitored against such targets. The company uses a feedback questionnaire to confirm customer satisfaction with completion of service or delivery of information to the customer.

- Computerized back-order records are maintained and are designed to notify customers of back orders within twenty-four hours. Customers are given the option to cancel a back order or have an alternate item delivered.

- Appropriate monitoring software (for example, What's Up Gold, NOCOL, SiteScope, and Keynote Systems) is used to perform network monitoring.
- Monitoring of latency, packet loss, hops, and network hardware is a continuous process.

- The organization maintains network integrity software and has documented network management policies.

- Appropriately documented escalation procedures are in place to initiate corrective actions to unfavorable network performance.

- The Web site and hardware owners are notified of unfavorable network performance, as part of the escalation procedures, on a weekly basis to assist in the escalation process.

- Customers have the option of printing, before an order is processed, an "order confirmation" online for future verification with payment records (such as credit card statement) detailing all information of the order (such as items ordered, sales prices, costs, sales taxes, and shipping charges).

- All costs, including taxes, shipping, and duty costs, and the currency used, are displayed to the customer. Customer accepts an order, by clicking "yes," before the order is processed.

- All foreign exchange rates are displayed to the customer before performing a transaction involving foreign currency

- Total costs and the expected shipping and billing dates are displayed to the customer before the customer accepts the order.

- Billing or settlement errors are followed up and corrected within twenty-four hours of reporting by the customer.

- The company maintains a transaction history for each order.

- Appropriate physical security and access control measures have been established for information technology assets, including those maintained at an off-site location in conformity with the general security policy. Access to facilities and physical data storage is controlled (for example, doors and cabinets are locked at all times).

- Backup media library management responsibilities and controls exist to protect and ensure the accuracy of data and information stored in backup libraries.

- Each order has a unique identifier that can be used to access order information. This information can also be accessed by customer name and dates of ordering, shipping, or billing.

- The company maintains this identifier and detailed order records that enable customers to contact the entity about details of orders for at least ninety days from order fulfillment.

- Procedures are in place to ensure that data files are inventoried systematically. An off-site inventory list provides details of all data stored off-site.

- Order history information is maintained for six months from the date of shipment and is available for immediate access by customer service representatives. After six months, this information is maintained in a form that can be accessed by customer service representatives within three days.

- The company performs an annual audit of tapes stored at the off-site storage facility. As part of the audit, tapes at the off-site location are matched to the appropriate tape management system.

- System backups are stored off-site in a fireproof safe. Backups are stored for twelve months.

- The storage site is periodically reviewed regarding physical access security and security of data files and other items.

- NowallMalls.net has implemented transaction editing and error detection routines to detect non-conforming transactions, which are communicated to RetailJoe.com for follow-up.

- The company maintains a transaction history for each order.

- Each order has a unique identifier that can be used to access order information.

- Such information also can be accessed by customer name and dates of ordering, shipping or billing.

- The company maintains this identifier and detailed order records that enable customers to contact the entity about details of orders for at least ninety days from order fulfillment.

- Order history information is maintained for six months from the date of shipment and is available for immediate access by customer service representatives. After six months, this information is maintained in a form that can be accessed by customer service representatives within three days.

- Commercial and other monitoring software (for example, COPS, SATAN, and ISS) are run on a routine basis. The output from these programs is analyzed for potential weaknesses and threats to the systems.

- Changes are made due to the information contained in these reports and with the consultation and approval of management.

- Processing problems are recorded and accumulated in a problem report. Corrective action is noted and monitored by management.

- Monitoring tools and response processes adequately identify and address network and system problems in a timely manner to ensure integrity of the network and related systems.

Illustration No. 10 – Illustrative Controls TPSP and Customer

Privacy			
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Controls Performed at NoWallsMall.net**
B	**Policies**		
B.1	The entity's policies related to the protection of personal information include, but are not limited to, the following items: • Notice to the customer regarding the information collected • Choice to the customer regarding the type(s) of information gathered and any options the customer has regarding the collection of this information • The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access • Employees who are allowed access based upon responsibilities and who authorizes that access • Access by the customer to his or her private information for update and corrective purposes • How complaints about privacy can be addressed • Procedures to handle security incidents • Record retention and destruction practices • The entity's commitment to use third-party dispute resolution that conforms to the Principles of Arbitration for WebTrust.	The company's defined privacy policy details access privileges, information collection needs, accountability, and other such matters. It is available for review and is reviewed and/or updated at quarterly management meetings and undergoes an intense review on an annual basis.	NoWallsMall.net's defined privacy policy details access privileges, information collection needs, accountability, and other such matters. The policy is compared quarterly to NoWallsMall.net's clientele for compliance with clients' defined privacy policy. It is available for review and is reviewed and/or updated at quarterly management meetings and undergoes an intense review on an annual basis.
B.2	The employees responsible for the	The privacy policies are reviewed with	NoWallsMall.net's privacy policies

Privacy			
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Controls Performed at NoWallsMall.net**
	privacy of personally identifiable information are aware of and follow the entity's privacy and related security policies.	new employees as part of their orientation, and the key elements of the policies and their impact on the employees are discussed. The employees must then sign a statement signifying that they have read, understand, and will follow the policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with these policies. All employees are aware of and follow the entity's published privacy policy. Employees who deal with personally identifiable information have undergone a privacy training and awareness program before processing. Only company employees who deal with personally identifiable information within the performance of their assigned job duties (for example, customer service representatives, marketing personnel, and other customer contact personnel) are subject to privacy training and awareness programs. The company's privacy policy is available and accessible via the company's intranet and within the company Employee's Handbook.	are reviewed with new employees as part of their orientation, and the key elements of the policies and their impact on the employees are discussed. The employees must then sign a statement signifying that they have read, understand, and will follow the policy. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the policies. All NoWallsMall.net employees are aware of and follow the entity's published privacy policies. Employees who deal with personally identifiable information have undergone a privacy training and awareness program before processing. Only NoWallsMall.net employees who deal with personally identifiable information within the performance of their assigned job duties (for example, customer service representatives, marketing personnel, and other customer contact personnel) are subject to privacy training and awareness programs. NoWallsMall.net's privacy policies are available and accessible via the company's intranet and within the NoWallsMall.net Employee's Handbook.
B.3	Accountability for the entity's privacy and related security policies has been assigned.	Management has assigned responsibility for enforcement of the company privacy and security policies to the chief information officer (CIO). Others on the executive committee assist in the review and update of the policies as outlined in the executive committee handbook.	Management has assigned responsibility for enforcement of the NoWallsMall.net privacy and security policies to the chief legal officer (CLO). Others on the executive committee assist in the review and update of the policies as outlined in the executive committee handbook.

Privacy			
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Controls Performed at NoWallsMall.net**
B.4	The entity has allocated training and other resources to support its policies related to privacy and relevant security matters.	The company has budgeted for privacy and security training for the information technology (IT) department. This amount is reviewed quarterly to ascertain whether additional training is needed based on employee feedback as well as changes in privacy and security policies and procedures.	NoWallsMall.net has budgeted for privacy and security training for the information technology (IT) department. This amount is reviewed quarterly to ascertain whether additional training is needed based on employee feedback as well as changes in privacy and security policies and procedures at both NoWallsMall.net and its clients. The CIO evaluates this training plan and makes a quarterly report to the executive committee.
B.5	The entity's policies related to privacy and relevant security matters are consistent with disclosed privacy practices and applicable laws and regulations.	Management reviews its disclosed privacy policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. Management makes any changes or needed modifications to the policy or disclosure within five business days of its evaluation. Laws and regulations that affect the disclosed site privacy policy are evaluated and reported on by the corporate attorney at least annually or when new regulations require an update.	Management reviews its disclosed privacy policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. Management makes any changes or needed modifications to the policy or disclosure within five business days of its evaluation. Laws and regulations that affect the disclosed site privacy policy are evaluated and reported on by the corporate attorney at least annually or when new regulations require an update.
C	**Procedures**		
C.1	The entity has security procedures to establish new users.	RetailJoe.com has established policies regarding the privacy of customer information and communicated these to NoWallsMall.net.	New users are given a secure session in which to provide new user information and select an appropriate user identification (ID) and password. New users provide information in a a secure socket layer (SSL) session. User IDs and passwords are provided to users and must contain non-alphanumeric characters.
C.2	The entity has procedures to identify and authenticate authorized users.	RetailJoe.com has established policies regarding the privacy of customer information and communicated these to NoWallsMall.net.	All users are required to provide a unique user ID and password to place an order or access their specific customer information.

Privacy			
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Controls Performed at NoWallsMall.net**
C.3	The entity has procedures to allow users to change, update, or delete their own user profile.	RetailJoe.com has established policies regarding the privacy of customer information and communicated these to NoWallsMall.net.	To update, change, or delete user information, the user's current ID and password are required. After providing this information in a secure session, the user can proceed to the user profile section for any changes.
C.4	The entity has procedures to limit remote access to the internal network to only authorized personnel.	RetailJoe.com has established policies regarding the privacy of customer information and communicated these to NoWallsMall.net.	Logical access control procedures (for example, firewalls, routers, and password controls) are maintained by the information technology (IT) department. These controls are tested on a periodic basis by performing penetration testing from both within the internal network and from the Internet.
C.5	The entity has procedures to prevent customers, groups of individuals, or other entities from accessing other than their own private or sensitive information.	RetailJoe.com has established policies regarding the privacy of customer information and communicated these to NoWallsMall.net.	Customers are required to enter a user ID and password to access their personal information and orders. A challenge word or phrase (for example, favorite sport or music—not a word that is easily identifiable, such as mother's maiden name) is stored on the system in the event a user forgets or misplaces a password. Or, the use of strong authentication and authorization procedures are in place. The authentication process allows the user to access only information relevant to that particular user. Other methods are in place to detect users attempting to guess another password or if a brute force attack is under way. If such an attack is detected, the system will disconnect from the user and report the security breach for follow up.
C.6	The entity has procedures to limit access to personally identifiable information to only authorized employees based upon their assigned roles and responsibilities.	RetailJoe.com has established policies regarding the privacy of customer information and communicated these to NoWallsMall.net.	Employee access to its data file and its customer's data file is limited to individuals based upon their assigned responsibilities. Idle workstations are timed-out after thirty minutes. Access to the corporate information technology facilities is limited to authorized employees by use of a card key system supported by video

Privacy			
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Controls Performed at NoWallsMall.net**
			surveillance monitoring.
C.7	The entity utilizes a minimum of 128-bit encryption to protect transmission of user authentication, verification, and sensitive or private information that is passed over the Internet from unintended recipients.	RetailJoe.com has strict policies and monitoring procedures to ensure that only certain employees can access private customer information. These policies also set forth ways that customer information should and should not be used. These policies have been communicated to NoWallsMall.net, the entity's third-party service provider. RetailJoe.com's Web site has a digital certificate, which can be checked using features in a standard Web browser.	Private information is protected during transmission by using 128-bit encryption technology (SSL technology).
C.8	The entity has procedures to maintain system configurations that minimize security exposures that potentially affect private or sensitive information.	RetailJoe.com's management routinely evaluates the level of performance it receives from its outsourced service provider, NoWallsMall.net, which hosts this Web site. This evaluation is done by evaluating the security controls NoWallsMall.net has in place by an independent third party as well as by following up with NoWallsMall.net management on any open items or causes for concern.	NoWallsMall.net meets with its technology vendors on a regular basis. Identified vendor security issues are documented and conveyed to the vendor by the appropriate level of management, depending on the severity of the exposure and risks associated with its planned or current deployment in the network. Resolutions to all vendor security issues are associated with agreed-upon time frames and followed up on by a NoWallsMall.net representative.
C.9	The entity has procedures to ensure that private information obtained as a result of electronic commerce is only disclosed to parties essential to the transaction unless customers are clearly notified prior to providing such information. If the customer was not clearly notified when he or she submitted the information, customer permission is obtained before such information is released to third parties.	RetailJoe.com has disclosed it's client information privacy and confidentiality polices on its Web page as part of its business practices disclosure. RetailJoe.com has established policies regarding the privacy and confidentiality of customer information and communicated these to the entity's third-party service provider.	NoWallsMall.net establishes customer support agreements specifically outlining security and privacy requirements of customer information
C.10	The entity has procedures to ensure that private information obtained as a result of electronic commerce is	RetailJoe.com outsources technology support or service and transfers data to the outsource provider. RetailJoe.com	NoWallsMall.net establishes customer support agreements specifically outlining security and

Privacy			
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Controls Performed at NoWallsMall.net**
	used by employees only in ways associated with the entity's business.	obtains representation as to the controls that are followed by the outsource provider.	privacy requirements of customer information. Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has access to other individuals or entities. Appropriate access controls are in place that limit access to sensitive, confidential, or private information based on job function and need.
C.11	The entity has procedures for personally identifiable information collected, created, or maintained by it to subject the information to reasonable edit and validation checks as it is collected.	RetailJoe.com only accepts data from customers or other reliable sources and uses reliable collection methods. Before completing the transaction, the customers are prompted by the system to check the personal data they have entered. Customers have the opportunity to correct any personal data entered prior to completing the transaction.	The entity only accepts information directly from the customer. Basic reasonableness tests are performed, and the customer may be asked to confirm information that does not conform to expected norms. Each input function requires that the customer confirm the entry by pressing the OK key.
C.12	The entity has procedures to obtain assurance or a representation that the adequacy of information protection and privacy policies of third parties to whom information is transferred, and upon which the entity relies, is in conformity with the entity's disclosed privacy practices.	RetailJoe.com outsources technology support or service and transfer data to NoWallsMall.net. RetailJoe.com obtains representation as to the controls that are followed by NoWallsMall.net and obtains a report on the effectiveness of such controls from NoWallsMall.net's independent auditor.	NoWallsMall.net establishes customer support agreements specifically outlining security and privacy requirements of customer information.
C.13	Customer permission is obtained before downloading files to be stored, or to alter or copy information on a customer's computer. If the customer has indicated to the entity that it does not want cookies, the entity has controls to ensure that cookies are not stored on the customer's computer. The entity requests customer	RetailJoe.com requests the customer's permission before it intentionally stores, alters, or copies information (such as cookies and other similar files) in the customer's computer. RetailJoe.com requests the customer's permission before it performs any diagnostic or inventory on the customer's computer.	Noncompliance situations are corrected when discovered and remedial actions taken are closely monitored for thirty days to prevent recurrence. The entity requests the customer's permission before it intentionally stores, alters, or copies information (such as cookies and other similar files) in the customer's computer. The entity requests the customer's permission before it performs any

Privacy			
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Controls Performed at NoWallsMall.net**
	permission to store, alter, or copy information (other than cookies) in the customer's computer.		diagnostic or inventory on the customer's computer.
C.14	In the event that a disclosed privacy policy is changed or deleted to be *less* restrictive, the entity has procedures to protect personal information in accordance with the privacy policies in place when such information was collected. Clear and conspicuous customer notification and choice are required to allow the entity to follow the new privacy policy with respect to their personal information.	It is RetailJoe.com's policy to request the customer's permission before it implements the new policy with respect to customer's private data.	NoWallsMall.net establishes customer support agreements specifically outlining security and privacy requirements of customer information. Amendments reducing the security or privacy requirements of such agreements are implemented only when the customer is notified and approves such amendment(s). Until such time, the previous (stricter) privacy policy is adhered to with respect to customer's personal information.
D	**Monitoring**		
D.1	The entity has procedures to monitor the security of its electronic commerce systems.	RetailJoe.com outsources technology support or service and transfer data to NoWallsMall.net. RetailJoe.com obtains representation as to the controls that are followed by NoWallsMall.net and obtains a report on the effectiveness of such controls from NoWallsMall.net's independent auditor.	Commercial and other monitoring software (for example, COPS, SATAN, and ISS) are run on a routine basis. The reports output from these programs are analyzed for potential weaknesses and threats to the systems.
D.2	The entity has procedures to monitor environmental and technology changes, and the related risks to keep its disclosed privacy and related security policies current with laws and regulations.	Staff meetings are held on a regular basis to address current privacy concerns and their findings are discussed at quarterly management meetings. RetailJoe.com's management meets with NoWallsMall.net's IT team on a quarterly basis to address identified or perceived weaknesses in the company's systems.	Legal counsel for the company reviews NoWallsMall.net's privacy policy on an annual basis to assess whether modifications are required. NoWallsMall.net is active in current public policy forums and monitors these forums for possible impact on its privacy policy and those of its clientele. NoWallsMall.net subscribes to publications and user groups specific to its industry and application in order to receive the most current security information. On a monthly basis, the Webmaster reports to the CIO any weaknesses perceived in the system. Management reviews this

Privacy			
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Controls Performed at NoWallsMall.net**
			report for follow-up and resolution. Quarterly, this information is communicated to RetailJoe.com.
D.3	The entity has procedures in place to monitor its privacy and security incident procedures and update these as needed due to technology changes, changes in the structure of the electronic commerce system(s), or other information.	RetailJoe.com's management meets with NoWallsMall.net's IT team on a quarterly basis to address identified or perceived weaknesses in the company's systems.	Weekly IT staff meetings are held to address current security concerns and the findings are discussed at quarterly management meetings. Senior management reviews the security policy on a semi-annual basis and considers developments in technology and the impact of any laws or regulations.
D.4	The entity has procedures to monitor and act upon privacy and security breaches.	N/A	System logs are monitored and evaluated on a daily basis. Monitoring software is in place that will notify the IT manager via e-mail and pager should any incident be in progress. If an incident occurs, a report is filed within twenty-four hours for follow-up and analysis. Customers are directed to an area of the Web site to post a message about breaches or suspected breaches as soon as they become concerned. These customer comments are followed up within twenty-four hours for evaluation and a report is issued to the customer and the CIO or the customer may contact the Incident Response hot line any time by telephoning (888) 911-0911. All such incidences are communicated to RetailJoe.com. within twenty-four hours.

Business Practices/Transaction Integrity			
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Controls Performed at NoWallsMall.net**
B	**Policies**		
B.1	The entity's policies related to transaction integrity include, but are not limited to, the following items: • Who is allowed access, what is the nature of that access, and who authorizes such access • The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access • Security procedures to protect transaction integrity • Procedures to document and allow for follow-up on transactions • How complaints and requests about transactions can be addressed • Procedures to handle security incidents • The entity's commitment to use third-party dispute resolution that conforms to the Principles of Arbitration for WebTrust	RetailJoe.com's policy provides guidelines for user profile creation and documentation requirements for modification and deletion along with the assignment of corresponding permissions for the user. For service and other information, contact one of the DoWeCare.org customer service representatives at (800) 555-1212 between 7:00 A.M. and 8:00 P.M. (Eastern Standard Time) or you can write to: DoWeCare.org 1517 Gervais Street World Hqtrs. Bldg. Anytown, South Carolina or CustServ@dowecare.org Proper historic audit trails of e-commerce transactions are maintained for any needed follow-up. These records are maintained for the time mandated by the regulatory agency or legal entity, after which time they are deleted. The record retention and deletion policy is reviewed on a periodic basis by company management. Management has procedures in place to allow employees and customers to report a breech or suspected breech to the security of the Web site. Employees are required to report such incidents within two hours of the breech (or suspected breech). Customers are encouraged to call the toll-free number posted at the company Web site.	NoWallsMall.net policies require written documentation from RetailJoe.com to support establishing user access rules. NoWallsMall.net order entry, payment, financing, and fulfillment systems incorporate appropriate automated data editing and validation checks. Inquiries regarding transactions are referred directly to RetailJoe.com for follow-up. Complaints and disputes are referred directly to RetialJoe.com for follow-up.
B.2	The employees responsible for transaction integrity are aware of and follow the entity's policies related to transaction integrity and relevant security matters.	The policies related to transaction integrity and related security is reviewed with new employees as part of their orientation, and the key	NoWallsMall.net's policy related to security and transaction integrity is reviewed with new employees as part of their orientation, and the key

Business Practices/Transaction Integrity			
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Controls Performed at NoWallsMall.net**
		elements of the policy and its impact on the employees are discussed. The employees must then sign a statement signifying that they have read, understand, and will follow the policy. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the policy.The company's policy is available and accessible via the company's intranet and within the company Employee's Handbook.	elements of the policy and its impact on the employees are discussed. The employees must then sign a statement signifying that they have read, understand, and will follow the policy. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the policy. NoWallsMall.net's policy is available and accessible via the company's intranet and within the NoWallsMall.net Employee's Handbook.
B.3	Accountability for the entity's policies related to transaction integrity and relevant security matters has been assigned..	Management has assigned responsibility for enforcement of the company transaction integrity to the chief information officer (CIO). Others on the executive committee assist in the review and update of the policies as outlined in the executive committee handbook.	Management has assigned responsibility for enforcement of the NoWallsMall.net transaction integrity policy to the chief legal officer (CLO). Others on the executive committee assist in the review and update of the policies as outlined in the executive committee handbook.
B.4	The entity's policies related to transaction integrity and relevant security matters are consistent with disclosed business practices and applicable laws and regulations.	Management reviews its disclosed transaction integrity and related security policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. Management makes any changes or needed modifications to the policy or disclosure within five business days of its evaluation. Laws and regulations that affect the disclosed site privacy policy are evaluated and reported on by the corporate attorney at least annually or when new regulations require an update	Management reviews its disclosed transaction integrity and related security policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. Management makes any changes or needed modifications to the policy or disclosure within five business days of its evaluation. Laws and regulations that affect the disclosed site privacy policy are evaluated and reported on by the corporate attorney at least annually or when new regulations require an update

	Business Practices / Transaction Integrity		
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Control Performed at NoWallsMall.net**
C	**Procedures**		
C.1	The entity has security procedures to establish new users.	RetailJoe.com establishes the requirements for the establishment and identification of new customers.	NoWallsMall.net provides new users a secure session in which to provide new user information and select an appropriate user ID and password.Passwords must contain at least six characters, one of which is non-alphanumeric.
C.2.	The entity has security procedures to identify and authenticate authorized users.	RetailJoe.com establishes the requirements for the identification and authentication of authorized customers.	To enter the site all customers are required to provide a unique user ID and password. These passwords are case sensitive and need to be updated every ninety days consistent with RetailJoe.com's policy.
C.3	The entity has procedures to allow users to change, update, or delete their own user profile.	RetailJoe.com defines the procedure to be used for users to change, update or delete their own profiles.	To update, change, or delete user information, the user's current ID and password are required. After providing this information in a secure session, the user can proceed to the user profile section for any changes.
C.4	The entity has procedures to limit remote access to the internal network to only authorized personnel.	Remote access controls are provided by NoWallsMall.net.	Remote access is provided to key employees. The system accepts remote calls, verifies the user, and then hangs up and calls the user back at the authorized number. Logical access (for example, firewalls, routers, and password controls) is maintained by the IT department. These controls are tested on a periodic basis by performing penetration testing from both within the internal network and from the Internet. Identification and authentication is accomplished through the combination of a user ID and one-time password. The remote access to and use of the computing resources are

	Business Practices / Transaction Integrity		
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Control Performed at NoWallsMall.net**
			restricted by the implementation of an authentication mechanism of identified users and resources associated with access rules. User IDs and passwords are stored in an encrypted database, with the associated encryption key stored off-line.
C.5	The entity has procedures to prevent customers, groups of individuals, or other entities from accessing other than their own transaction information.	N/A	Customers are required to enter a user ID and password to access private customer information and orders. Customer sessions between the browser and e-commerce systems are protected to avoid other users from hijacking a customer's session.
C.6	The entity has procedures to limit access to systems and data to only authorized employees based upon their assigned roles and responsibilities.	RetailJoe.com has established policies regarding access to customer data and communicated these to NoWallsMall.net.	Employee access to its data file and its customer's data file is limited to individuals based upon their assigned responsibilities. Idle workstations are timed out after thirty minutes. Access to the corporate IT facilities is limited to authorized employees by use of a card key system supported by video surveillance monitoring.
C.7	The entity uses encryption or other equivalent security procedures to protect transmissions of user authentication and verification information passed over the Internet..	RetailJoe.com has strict policies and monitoring procedures to ensure that only certain employees can access private or confidentialinformation. These policies also set forth ways that customer information should and should not be used. These policies have been communicated to NoWallsMall.net, the entity's third-party service provider. RetailJoe.com's Web site has a digital certificate, which can be checked using features in a standard Web browser.	The company uses 128-bit encryption for all transmission of private or confidential information, including user ID and password. Users are also encouraged to upgrade their browser to the most current version to avoid any possible security problems.
C.8	The entity has procedures to maintain system configurations that minimize transaction integrity and related security exposures	RetailJoe.com's management routinely evaluates the level of performance it receives from its outsourced service provider,	NoWallsMall.net meets with its technology vendors on a regular basis. Identified vendor security issues

	Business Practices / Transaction Integrity		
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Control Performed at NoWallsMall.net**
		NoWallsMall.net, which hosts this Web site. This evaluation is done by evaluating the security controls NoWallsMall.net has in place by an independent third party as well as by following up with NoWallsMall.net management on any open items or causes for concern.	are documented and conveyed to the vendor by the appropriate level of management, depending on the severity of the exposure and risks associated with its planned or current deployment in the network. Resolutions to all vendor security issues are associated with agreed-upon time frames and followed up on by a NoWallsMall.net representative.
C.9	The entity has procedures in place to monitor and act on security breaches that affect transaction integrity.	Information regarding suspected security breaches is communicated to NoWallsMall.net for investigation and follow-up.	System logs are monitored and evaluated on a daily basis. Monitoring software is in place that will notify the IT manager via e-mail and pager should any incident be in progress. If an incident occurs, a report is filed within twenty-four hours for follow-up and analysis. Customers are directed to an area of the Web site to post a message about security breaches or possible breaches as soon as they become concerned. These customer comments are followed up within twenty-four hours for evaluation and a report is issued to the customer or the customer may contact the Incident Response hot line at any time by telephoning (888) 911-0911.
C.10	The entity checks each request or transaction for accuracy and completeness.	RetailJoe.com specifies transaction editing rules and communicates to NoWallsMall.net	Web scripts contain error checking for invalid inputs. The NowallMall.net order entry automatically checks each order for accuracy and completeness of information before processing. All customer-provided information for the order is displayed to the customer. Customer accepts an order, by clicking “yes,” before the order is processed.

	Business Practices / Transaction Integrity		
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Control Performed at NoWallsMall.net**
C.11	Positive acknowledgment is received from the customer before the transaction is processed.	N/A	Before a transaction is processed by the company, the customer is presented with a request to confirm the intended transaction and the customer is required to click on the "Yes, please process this order" button before the transaction is then processed.
C.12	The correct goods are shipped in the correct quantities in the time frame agreed, or services and information are provided to the customer as requested.	N/A	The NoWallsMall.net order entry and fulfillment system produces packing slips from the customer sales order. Commercial delivery methods are used that reliably meet expected delivery schedules. Service delivery targets are maintained and actual services provided are monitored against such targets. The company uses a feedback questionnaire to confirm customer satisfaction with completion of service or delivery of information to the customer.
C.13	Transaction exceptions are promptly communicated to the customer.	N/A	Computerized back-order records are maintained and are designed to notify customers of back orders within twenty-four hours. Customers are given the option to cancel a back order or have an alternate item delivered.
C.14	Incoming messages are processed and delivered accurately and completely to the correct IP address.	N/A	Appropriate monitoring software (for example, What's Up Gold, NOCOL, SiteScope, and Keynote Systems) is used to perform network monitoring. Monitoring of latency, packet loss, hops, and network hardware is a continuous process. The organization maintains network integrity software and has documented network management policies. Appropriately documented

	Business Practices / Transaction Integrity		
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Control Performed at NoWallsMall.net**
			escalation procedures are in place to initiate corrective actions to unfavorable network performance. The Web site and hardware owners are notified of unfavorable network performance, as part of the escalation procedures, on a weekly basis to assist in the escalation process.
C.15	Outgoing messages are processed and delivered accurately and completely to the service provider's (SP's) Internet access point.	N/A	Appropriate monitoring software (for example, What's Up Gold, NOCOL, SiteScope and Keynote Systems) is used to perform network monitoring. Monitoring of latency, packet loss, hops and network hardware is a continuous process.
C.16	Messages remain intact while in transit within the confines of the SP's network.	N/A	See C.14.
C.17	The entity displays sales prices and all other costs and fees to the customer before processing the transaction.	N/A	Customers have the option of printing, before an order is processed, an "order confirmation" online for future verification with payment records (such as credit card statement) detailing all information of the order (such as items ordered, sales prices, costs, sales taxes, and shipping charges). All costs, including taxes, shipping, and duty costs, and the currency used, are displayed to the customer. Customer accepts an order, by clicking "yes," before the order is processed. All foreign exchange rates are displayed to the customer before performing a transaction involving foreign currency.
C.18	Transactions are billed and electronically settled as agreed.	N/A	Total costs and the expected shipping and billing dates are displayed to the customer before

	Business Practices / Transaction Integrity		
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Control Performed at NoWallsMall.net**
			the customer accepts the order.
C.19	Billing or settlement errors are promptly corrected.	N/A	Billing or settlement errors are followed up and corrected within twenty-four hours of reporting by the customer.
C.20	Transaction histories are retained in a secure location, may not be altered without appropriate authorization, and are retrievable for review and investigation.	N/A	The company maintains a transaction history for each order. Appropriate physical security and access control measures have been established for information technology assets, including those maintained at an off-site location in conformity with the general security policy. Access to facilities and physical data storage is controlled (for example, doors and cabinets are locked at all times). Backup media library management responsibilities and controls exist to protect and ensure the accuracy of data and information stored in backup libraries. Each order has a unique identifier that can be used to access order information. This information can also be accessed by customer name and dates of ordering, shipping, or billing. The company maintains this identifier and detailed order records that enable customers to contact the entity about details of orders for at least ninety days from order fulfillment. Procedures are in place to ensure that data files are inventoried systematically. An off-site inventory list provides details of all data stored off-site. Order history information is maintained for six months from the

	Business Practices / Transaction Integrity		
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Control Performed at NoWallsMall.net**
			date of shipment and is available for immediate access by customer service representatives. After six months, this information is maintained in a form that can be accessed by customer service representatives within three days. The company performs an annual audit of tapes stored at the off-site storage facility. As part of the audit, tapes at the off-site location are matched to the appropriate tape management system. System backups are stored off-site in a fireproof safe. Backups are stored for twelve months. The storage site is periodically reviewed regarding physical access security and security of data files and other items.
C.21	Transactions are processed accurately and in conformity with the entity's disclosed business practices.	RetailJoe.com has implemented a process to regularly review customer complaints, back-order logs and other transactional analysis. This information is compared to the company's disclosed practices to ascertain the company's compliance.	NowallMalls.net has implemented transaction editing and error detection routines to detect non-conforming transactions, which are communicated to RetailJoe.com for follow-up.
C.22	The entity logs transactions for subsequent follow-up.	N/A	The company maintains a transaction history for each order. Each order has a unique identifier that can be used to access order information. Such information also can be accessed by customer name and dates of ordering, shipping or billing. The company maintains this identifier and detailed order records that enable customers to contact the entity about details of orders for at least ninety days from

	Business Practices / Transaction Integrity		
	Criteria	**Illustrative Controls Performed at RetailJoe.com**	**Illustrative Control Performed at NoWallsMall.net**
			order fulfillment. Order history information is maintained for six months from the date of shipment and is available for immediate access by customer service representatives. After six months, this information is maintained in a form that can be accessed by customer service representatives within three days.
D	**Monitoring**		
D,1	The entity has procedures to monitor the transaction integrity of its e-commerce systems and to identify any need for changes to its transaction integrity and related security controls.	RetailJoe.com outsources technology support or service and transfer data to NoWallsMall.net. RetailJoe.com obtains representation as to the controls that are followed by NoWallsMall.net and obtains a report on the effectiveness of such controls from NoWallsMall.net's independent auditor.	Commercial and other monitoring software (for example, COPS, SATAN, and ISS) are run on a routine basis. The output from these programs is analyzed for potential weaknesses and threats to the systems. Changes are made due to the information contained in these reports and with the consultation and approval of management.
D.2	The entity has procedures to provide that transaction history and related information is monitored and corrective measures are taken on a regular and timely basis.	N/A	Processing problems are recorded and accumulated in a problem report. Corrective action is noted and monitored by management. Monitoring tools and response processes adequately identify and address network and system problems in a timely manner to ensure integrity of the network and related systems.

Illustration No. 11 - Illustrative TPSP Security Controls Within a Virtual Retail Mall Environment

Security Performed at NoWallsMall.net for RetailJoe.com

Almost all of RetailJoe.com's security is performed by the third-party service provider, NoWallsMall.net, including the following:

- Disclosure related:
  - Disclosures are provided that are related to the establishment of a secure session in which a site customer provides confidential customer information, establishes a user identification (ID) and password, and ultimately conducts business with RetailJoe.com.
  - Disclosures are provided to RetailJoe.com's customers with a point of contact should they believe there has been a breach of security at the site.

- Policy related:
  - A majority of security related policies for RetailJoe.com are in the domain of third-party service provider NoWallsMall.net. This may include a security policy detailing access privileges, hardware and software modification procedures (including updates), Web access, and Web posting. Outsourced security policies may also include procedures to control logical as well as physical access to the system. These system security requirements would normally be expected to be defined in contractual, legal, and other service level agreements between RetailJoe.com and NoWallsMall.net.

- Procedures related:
  - New users of RetailJoe.com will provide information in a secure socket layer (SSL) session administered by NoWallsMall.net. The process where User IDs and passwords are provided to the user, presumably containing nonalphanumeric characters, is managed by NoWallsMall.net.
  - NoWallsMall.net will also manage the security procedures to identify and authenticate authorized users.
  - Processing changes to user profiles is also managed by NoWallsMall.net. These changes are done after a customer provides user ID and password.
  - Remote access to RetailJoe.com's computing resources will be managed and restricted by NoWallsMall.net by the implementation of an authentication mechanism for identified users and resources associated with access rules.
  - Virus prevention and detection procedures will be the responsibility of NoWallsMall.net.
  - Management of network services (port management) will be provided by third-party service provider NoWallsMall.net.
  - All software managed by NoWallsMall.net will be updated on a timely basis for known security issues with patches and other software upgrades issued by software vendors.

NoWallsMall.net personnel will actively manage this process to minimize the risk of security breaches.

— NoWallsMall.net will have procedures in place to prevent individuals, entities, or others from accessing data that is other than their own. This will, most likely, involve the use of access control lists set up in accordance with the firewall policy of NoWallsMall.net, anti-spoof filters at the router level, and firewalls to segment related local area network access.

— Super-user passwords for the Web site are managed by NoWallsMall.net. System passwords and other key passwords are encrypted and stored in the company safe under dual control.

— All of RetailJoe.com's servers and related hardware are physically located at NoWallsMall.net's facilities. Physical access to servers and related hardware (for example, firewalls and routers) is controlled and monitored by video surveillance maintained by NoWallsMall.net personnel.

- Monitoring:
  — NoWallsMall.net is responsible for monitoring the security of its electronic commerce systems and to identify any need for changes to its security procedures. They will need to run commercial and other monitoring software (for example, COPS, SATAN, and ISS) on a routine basis. Reports generated from these monitoring processes are analyzed for potential weaknesses and threats to the system.
  — Security policies, procedures, and related risks are discussed with management of RetailJoe.com on a monthly or quarterly basis. Updates and changes are implemented by NoWallsMall.net on a timely basis.

EXAMPLE TWO – ILLUSTRATIVE BUSINESS-TO-BUSINESS CASE STUDY

The second case study involves an electronic components exchange, BtwoBExchange.org, that facilitates business-to-business transactions among a number of electronic component supplier and customers. It uses a third-party service provider, OuiBServices.com to deliver its exchange services. In this business-to-business example, the potential controls exercised at the client level, BtwoBExchange.org, have not been illustrated. Since the TPSP auditor would not be aware of the controls exercised at the retail client, they would not be included in the TPSP Auditor report.

Illustration No. 12, for Use in the United States (Direct Report) - OuiBServices.com

Independent Accountant's Report

To the Management of OuiBServices.com (OBS):

We have examined the description of controls presented in Attachment One for which OBS is responsible with respect to services provided to Web site customers that, when combined with a customer's procedures, contribute to compliance with the AICPA/CICA WebTrust Criteria, and the effectiveness of those controls during the period from _____ to _____.

The description of controls, and the effectiveness of those controls, are the responsibility of OBS's management. Our responsibility is to express an opinion 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 OBS's services provided to its customers that have, or desire to have, a CPA WebTrust examination related to the customer's electronic commerce (e-commerce) confidentiality practices and the related controls over confidentiality; (2) selectively testing transactions executed in accordance with disclosed confidentiality 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.

In our opinion, the controls maintained by OBS presented in Attachment One, operated effectively during the period _____ through _____, in all material respects, based on the AICPA/CICA WebTrust Criteria.

Because of inherent limitations in controls, error 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 the validity of such conclusions may be altered because of (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) a deterioration in the degree of compliance with the policies or procedures.

This information has been provided to customers of OBS and to their practitioners to be taken into consideration, along with the information about controls at customers, when evaluating the customer's controls in relation to the AICPA/CICA WebTrust Confidentiality Criteria. The relative effectiveness and significance of specific controls at OBS and their effect on assessments of controls at customers depend on their interaction with the controls and other factors present at individual customer organizations. We have performed no procedures to evaluate the effectiveness of controls at individual customers.

This report is intended solely for the information and use of the management of OBS, its customers, and their independent WebTrust practitioners and is not intended to be, and should not be, used by anyone other than those specified parties.

This report does not include any representations as to the quality of services beyond those covered by the accompanying description of controls, nor to the suitability of any of OBS's services for any customer's intended purposes.

TPSP Auditor LLP
Certified Public Accountants
City, State
Date of Report

Illustration No. 13, for Use in Canada (Direct Report) - OuiBServices.com

Auditor's Report

To the Management of OuiBServices.com (OBS):

With respect to services provided to Web site customers, we have audited OBS's description of those controls for which OBS is responsible that, when combined with a customer's procedures, contribute to compliance with the AICPA/CICA WebTrust Criteria and the effectiveness of those controls during the period from _____ to _____. The controls are outlined in Attachment One.

The description and the controls are the responsibility of OBS's management. Our responsibility is to express an opinion on the conformity of the description and the controls with the AICPA/CICA WebTrust Criteria based on our audit.

Our audit was made in accordance with standards for assurance engagements established by the Canadian Institute of Chartered Accountants. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of OBS's services provided to its customers who have, or desire to have, a WebTrust audit insofar as they relate to the customer's electronic commerce (e-commerce) confidentiality practices and the related controls over confidentiality, (2) selectively testing transactions executed in accordance with disclosed confidentiality 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 audit provides a reasonable basis for our opinion.

In our opinion, in all material respects, the controls maintained by OBS as presented in Attachment One operated effectively during the period from _____ to _____ in conformity with the AICPA/CICA WebTrust Criteria.

This information has been provided to customers of OBS and to their auditors to be taken into consideration, along with the information about controls at customers, when evaluating the customer's controls in relation to the AICPA/CICA WebTrust Criteria. The relative effectiveness and significance of specific controls at TPSP and their effect on assessments of controls at customers are dependent on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual customers.

Because of inherent limitations in controls, error 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 the validity of such conclusions may be altered because of (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) a deterioration in the degree of compliance with the policies or procedures

Because of inherent limitations in controls, error 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 the validity of such conclusions may be altered because of (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) a deterioration in the degree of compliance with the policies or procedures.

This report is intended solely for the information and use of the management of OBS, its customers, and their independent WebTrust practitioners and is not intended to be, and should not be, used by anyone other than those specified parties.

This report does not include any representations as to the quality of services beyond those covered by the accompanying description of controls, nor to the suitability of any of OBS's services for any customer's intended purposes.

City, Province

TPSP Auditor

LLP
Date of Report

Chartered Accountants

Illustration No. 14, Controls Attachment - OuiBServices.com

Attachment One to TPSP Practitioner Report

PERIOD OF COVERAGE

Description of Services Provided by OuiBServices.com (Optional)

OuiBServices.com hosts a number of e-commerce business-to-business exchanges. Each exchange is responsible for its Web site management and for other aspects of exchange commerce, including obtaining and then maintaining relevant credit information for transaction participants before a transaction is consummated by the trading partners.

OuiBServices.com handles the exchange transactions and related settlement through its back-end systems. Any subsequent application system maintenance is performed by its customers in coordination with a designated client representative.

Following are the activities performed by OuiBServices.com on behalf of its e-commerce clients:

- Tailoring of OuiBServices.com's proprietary fulfillment and settlement software to enable the client's specifies e-commerce activities over the Internet
- All subsequent application system enhancement, modification, and testing
- Web server acquisition, configuring and implementation
- Ongoing Web server and related technology configuration and maintenance
- Internet service provisioning for e-commerce and general uses
- Communications connectivity from the Internet through to a client's business processing environment
- Telecommunications security
- Internet firewall configuration, maintenance and monitoring

- Maintenance of a secure e-commerce processing environment
- Maintaining the confidentiality of client information

Controls

The following controls that exist at OuiBServices.com have been identified by OuiBServices.com's management as contributing to the ability of OuiBServices.com clients to achieve compliance with the criteria related to the selected principles. Additional control procedures at individual OuiBServices.com clients may be necessary for OuiBServices.com client to achieve compliance with all of the criteria for a selected principle.

Confidentiality[6]		
	Criteria	**Illustrative Controls Performed at OuiBServices.com**
B	**Policies**	
B.1	The entity's policies related to the protection of confidential information include, but are not limited to, the following items:[7] • Who is allowed access, what is the nature of that access, and who authorizes such access • The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access • Complaint-resolution process • Procedures to handle security incidents • Controls over physical access to the system(s) • Security procedures to protect confidential information	OuiBServices.com policies require written documentation from BtwoBEchange.org to support establishing user access rules. OuiBServices.com payment and fulfillment systems incorporate appropriate automated data editing and validation checks. Policies provide for employees and business partners to report a breech or suspected breech of the confidentiality and related security of the Web site. Employees are required to report such incidents within two hours of the breech (or suspected breech). Business partners are encouraged to call the toll-free number posted at the company Web site. Physical access is controlled through a combination of guarded entrances, card key access, and monitoring cameras.
B.2	The employees responsible for information security and related confidentiality of information are aware of and follow the entity's security and related confidentiality policies.	The confidentiality and related security policies are reviewed with new employees as part of their orientation, and the key elements of the policies and their impact on employees are discussed. Employees must then sign a statement signifying that they have read, understand, and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with these policies. Employees who deal with confidential information are required to undergo an annual training and awareness program.

[6] This is another example of a controls format that could be used. This one is referenced to the particular criteria.

[7] Often an entity's confidentiality policy is addressed within the broader context as part of its information or data security policy statement.

Confidentiality[6]		
	Criteria	**Illustrative Controls Performed at OuiBServices.com**
B.3	Accountability for management of the entity's policies related to confidentiality and relevant security matters has been assigned.	Management has assigned responsibility for enforcement of the company confidentiality and security policies to the chief information officer (CIO). Others on the executive committee assist in the review and update of the policies as outlined in the executive committee handbook.
B.4	The entity has allocated resources for awareness and support of its policies related to confidentiality and relevant security matters.	Management has an ongoing confidentiality and security training program for all employees. IT staff is required to submit an annual training request based on job description. All employees are given periodic confidentiality and security training courses put on by the IT Department. The CIO evaluates these programs and makes a quarterly report to the executive committee.
C	**Procedures**	
C.1	The entity has security procedures to establish new users.	The business partner's designated administrative user uses a secure session to authorize new users and select an appropriate user identification (ID), password, and level of access for each of its users.
C.2	The entity has security procedures to identify and authenticate authorized users.	All external users are required to provide a unique user ID and password to place an order or access their specific business partner information. System level access to all production systems is provided via a digital signature and password. Strong, static passwords are used for systems that do not require a strong identification and authentication mechanism. Controlled access by a software authentication product with a strong identification and authentication mechanism is required for access to any routers.
C.3	The entity has procedures to allow users to change, update, or delete their own user profile.	All changes to user profiles are done after providing user ID and password. The only changes allowed are updates to the user ID and password. Changes to personal information or deletions must be processed in writing.
C.4	The entity has procedures to limit remote access to the internal network to only authorized entity personnel.	Logical access control procedures (for example, firewalls, routers, and password controls) are maintained by the information technology (IT) department. These controls are tested on a periodic basis by performing penetration testing both from within the internal network and from the Internet. The remote access to and use of the computing resources are restricted by the implementation of an authentication mechanism for identified users and resources associated with access rules. User IDs and passwords are stored in an encrypted database, with the associated encryption key stored off-line. Identification and authorization is accomplished through the combination of

Confidentiality[6]		
	Criteria	**Illustrative Controls Performed at OuiBServices.com**
		user ID and one-time password.
C.5	The entity has procedures to prevent business partners, groups of individuals, or other entities from accessing information other than that which they are authorized to access.	One-time passwords, smart cards, or both, restrict all system access from outside the entity, other than for customary e-commerce transactions through the Web page. Business partner Web sites hosted by the Internet service provider (ISP) are prevented from intercepting messages not addressed to them. Packet filters are implemented on the ISP Internet gateway routers using access control lists (ACLs) according to the ISP firewall policy. Anti-spoof filters are used on the routers to prevent spoofing of trusted sources. Additional ACLs are used to control business partner access to only their network segments. The various LAN segments are firewalled from the rest of the networks. The use of strong authentication and authorization procedures are in place. The authentication process allows the user to access only information relevant to that particular user. Other methods are in place to detect users attempting to guess another password or if a brute force attack is under way. If such an attack is detected, the system will disconnect from the user and report the security breach for follow-up.
C.6	The entity has procedures to limit access to confidential information to only its authorized employees based upon their assigned roles and responsibilities consistent with its disclosed confidentiality practices.	Employee access to business partner data is limited to individuals based upon their assigned responsibilities. Idle workstations are timed out after thirty minutes. Access to the corporate information technology facilities is limited to authorized employees by use of a card key system supported by video surveillance monitoring. Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has access to other individuals or entities. Appropriate access controls are in place that limit access to confidential information based on job function and need. Other business partners are subject to nondisclosure agreements (NDAs).
C.6.1	The entity secures its programs and data during the backup, off-site storage, and restoration processes.	During the daily backup routine, the data is secured from both physical and logical access by unauthorized personnel. During any restoration process, no access is allowed by unauthorized personnel.
C.7	The entity uses a minimum of 128-bit encryption to protect transmission of user authentication, verification, and confidential information that is passed over the	Confidential information is protected during transmission by using 128-bit encryption technology (SSL technology). The company's Web site has a digital certificate that can be checked using features in a standard Web browser.

Confidentiality[6]		
	Criteria	**Illustrative Controls Performed at OuiBServices.com**
	Internet from unintended recipients.	
C.8	The entity has procedures to maintain system configurations that minimize security exposures that potentially affect confidential information.	The service provider meets with its technology vendors (for example, SUN, Cisco, and Microsoft) on a regular basis. Identified vendor security issues are documented and conveyed to the vendor to the appropriate level of management, depending on the severity of the exposure and risks associated with its planned or current deployment in the network. All vendor security issues are associated with agreed-upon time frames and followed up on by an ISP representative.
C.9	The entity has procedures to monitor and act upon confidentiality and security breaches.	System logs are monitored and evaluated on a daily basis. Monitoring software is in place that will notify the IT manager via e-mail and pager should any incident be in progress. If an incident occurs, a report is filed within twenty-four hours for follow-up and analysis. Business partners are directed to an area of the Web site to post a message about breaches or suspected breaches as soon as they become concerned. These business partner comments are followed up within twenty-four hours for evaluation and a report is issued to the business partner and CIO or the business partner may contact the Incident Response hot line at any time by telephoning (888) 911-0911.
C.10	The entity has procedures to ensure that confidential information obtained as a result of electronic commerce is disclosed only to parties consistent with its disclosed confidentiality practices.	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has access to other individuals or entities. Appropriate access controls are in place that limit access to confidential information based on job function and need. Other business partners are subject to nondisclosure agreements (NDAs).
C.11	The entity has procedures to obtain assurance or a representation that the adequacy of confidentiality policies of third parties to whom information is transferred, and upon which the entity relies, is in conformity with the entity's disclosed confidentiality practices.	
C.12	In the event that a disclosed confidentiality practice is deleted or changed to be *less* restrictive, the entity has procedures to protect	The entity maintains copies of all versions of the confidentiality policy. The entity attorney summarizes the key changes to this policy statement. When changes to a less restrictive policy are made, the company attempts

Confidentiality[6]		
	Criteria	**Illustrative Controls Performed at OuiBServices.com**
	confidential information in accordance with the confidentiality practices in place when such information was received, unless the business partner agrees to the change in practice.	to obtain the agreement of its customers to the new policy. Confidential information for those customers who do not agree to the new policy is isolated and receives continued protection under the old policy.
D	**Monitoring**	
D.1	The entity has procedures to monitor the security of its electronic commerce systems and to identify any need for changes to its confidentiality and related security controls.	Commercial and other monitoring software (for example, COPS, SATAN, and ISS) is run on a routine basis. The report output from these programs is analyzed for potential weaknesses and threats to the systems. Changes are made due to the information contained in these reports and with the consultation and approval of management.
D.2	The entity has procedures to monitor environmental and technology changes, and the related risks, to keep its disclosed confidentiality practices and related policies consistent and current with laws and regulations.	Management reviews its disclosed confidentiality policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. Management makes any changes or needed modifications to the policy or disclosure within five business days of its evaluation. Laws and regulations that affect the disclosed site confidentiality policy are evaluated and reported on by the corporate attorney at least annually or when new regulations require an update. Staff meetings are held on a regular basis to address current privacy concerns and their findings are discussed at quarterly management meetings.
D.3	The entity has procedures in place to monitor its security incident procedures and update these as needed due to technology changes, changes in the structure of the electronic commerce system(s), or other information.	Senior management reviews the security policy on a biannual basis and considers developments in technology and the impact of any laws or regulations.