2000

AICPA/CICA WebTrust program for online privacy, November 30, 2000, Version 3.0

American Institute of Certified Public Accountants (AICPA)

Canadian Institute of Chartered Accountants

The CPA. Never Underestimate The Value.SM

Chartered Accountants of Canada

Comptables agréés du Canada

AICPA/CICA

WebTrust SM/TM Program for Online Privacy

November 30, 2000

Version 3.0

The Principles and Criteria contained in this program supersede Version 2.0 of the WebTrust Principles and Criteria insofar as they relate to privacy and information protection and are effective for examination periods beginning after December 31, 2000. Earlier adoption is encouraged.

COMMITTEE AND TASK FORCE MEMBERS

AICPA
Assurance Services Executive Committee

Susan C. Rucker, *Chair*
Gari Fails
Ted Horne
Everett C. Johnson, Jr.
John Lainhart
J. W. Mike Starr
Wendy E. Visconty
Thomas E. Wallace
Neal West

Staff Contacts:

Alan Anderson,
Senior Vice President, Technical Services

Anthony J. Pugliese,
Director of Assurance Services

CICA
Assurance Services Development Board

Doug McPhie, *Chair*
Diana Chant
Douglas C. Isaac
Marilyn Kuntz
Jeff Orchard
Frederick J. Phillips
David W. Stephen
Doug Timmins
Keith S. Vance

Staff Contacts:

Cairine M. Wilson,
Vice President, Innovation

Gregory P. Shields
Director, Assurance Service Development

AICPA / CICA Electronic Commerce
Assurance Services Task Force

Everett C. Johnson, Jr., *Chair*
Bruce R. Barrick
Jerry R. DeVault
Joseph G. Griffin
Christopher J. Leach , *Vice Chair*
Patrick J. Moriarty
William Powers
Kerry L. Shackelford
Donald E. Sheehy
Christian R. Stormer
Alfred F. Van Ranst

Staff Contacts:

Bryan Walker, CICA
Principal, Assurance Services Development

Sheryl Martin, AICPA
WebTrust Team Leader

CONTENTS

INTRODUCTION

The Internet provides consumers with a new means for obtaining useful information and for purchasing goods, information and services. Although this form of electronic commerce (e-commerce) has undergone rapid growth, particularly through the use of the World Wide Web (the Web), its growth has been inhibited by consumer fears and concerns about the risks, both real and perceived, of doing business electronically.

In response to these fears and concerns and to increase consumer confidence in this new electronic marketplace, the public accounting profession has developed and is promoting a program with corresponding criteria for e-commerce for the protection of personally identifiable information ("personal information") referred to as the WebTrust℠ Program for Online Privacy, and the related WebTrust Privacy Seal of assurance, also referred to as WebTrust℠/™. Public accounting firms and practitioners, who have a WebTrust business license from the American Institute of Certified Public Accountants (AICPA), Canadian Institute of Chartered Accountants (CICA), or other authorized national institutes (practitioners), can provide assurance services to evaluate and test whether a particular Web site meets the WebTrust Privacy Principle and Criteria as set forth in this document. A complete listing of authorized national institutes can be viewed at www.cpawebtrust.org/abtlinks.htm. The WebTrust Seal of assurance is a symbolic representation of a practitioner's unqualified report. It also indicates to customers that they need to click to see the practitioner's report**.** This seal can be displayed on the entity's Web site together with links to the practitioner's report and other relevant information.

This is the WebTrust Program for Online Privacy, which is a part of Version 3.0 of the WebTrust Program. The principal changes in Version 3.0 of the WebTrust Program 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 and Transaction Integrity
    - Availability
    - Confidentiality
    - Non-Repudiation
    - Customized Disclosures
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, except for the principle of Customized Disclosures alone (one of the other principles must be evaluated in combination with this principle).
3. Expansion of the WebTrust program to include transactions in the business-to-business market place by adding new principles that can be applied to this market.

4. Expansion of the WebTrust program to include a variety of service providers (for example, Application Service Providers) in addition to Internet Service Providers.

The new modules are being exposed and released as they are developed.

We anticipate that the WebTrust program will continue to be refined as changes in the technology occur, and in response to market demands.

The WebTrust Principles and Criteria are intended to address user needs and concerns and are designed to benefit users and providers of e-commerce services. Your input is not only welcome, it is essential to help ensure that these principles and their supporting criteria are kept up-to-date and remain responsive to marketplace needs.

This version of the WebTrust Program for Online Privacy has been approved by the AICPA Assurance Services Executive Committee and the CICA Assurance Services Development Board.

BACKGROUND

What Is E-commerce?

E-commerce involves individuals as well as organizations engaging in a variety of electronic business transactions, without paper documents, using computer and telecommunication networks. These networks can be public, private, or a combination of the two. Traditionally, the definition of e-commerce has focused on Electronic Data Interchange (EDI) as the primary means of conducting business electronically between entities having a pre-established contractual relationship. More recently, however, the definition of e-commerce has broadened to encompass business conducted over the Internet (specifically the Web) and includes entities not previously known to each other. This trend is attributable to the Web's surge in popularity and the acceptance of the Internet as a viable transport mechanism for business information. The use of a public network-based infrastructure like the Internet can reduce costs and "level the playing field" for small and large businesses. This allows companies of all sizes to extend their reach to a broad customer base.

Information Privacy

E-commerce facilitates the gathering of information from and about individuals and its subsequent exchange with other entities. Some consumers like this because it allows them to receive targeted marketing materials, which focus on their needs. On the other hand, many consumers consider such uses of information about them to be an invasion of their privacy. For this reason, it is important that Web sites inform their customers about the kinds of information that are collected about them, the uses of such information, customer options, and related matters. In addition, many countries have implemented laws and regulations covering the privacy of information obtained through e-commerce.

Privacy can have many aspects, but for purposes of this document and the corresponding criteria, *privacy is defined as the protection of the collection, storage, destruction and dissemination of personal information. Personal information is defined as any information relating to an identified or identifiable individual.* Such information includes but is not limited to the customer's name, address, telephone number, social security/insurance or other government identification numbers, employer, credit card numbers, personal or family financial information, personal or family medical information, employment history, history of purchases or other transactions, credit records, and similar information. *Sensitive information is defined as personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offences or criminal convictions.*[1]

Information privacy can be a double-edged sword. On the one hand, merchants need certain information in order to process a customer order. On the other hand, the customer may not want this information distributed to parties not involved with the transaction without their consent. In addition, errors can occur in a company database that the consumer should be able to correct or amend as needed. Without such a process in place, decisions can be made that could negatively affect the consumer.

It is important for consumers to have confidence that they have reached a Web site that takes appropriate steps to protect personal information. Although it is relatively easy to establish a Web site on the Internet, the underlying technology can be complex and can entail a multitude of information protection and related security issues. The privacy of sensitive information transmitted over the Internet can be compromised. For example, without the use of basic encryption techniques, consumer credit card numbers can be intercepted and stolen during transmission. Without appropriate firewalls and other security practices, personal information residing on an entity's e-commerce computer system can be intentionally or unintentionally provided to third parties not related to the entity's business.

Privacy Concepts

With the rapidly expanding interest in privacy, the following concepts are widely used to facilitate the creation and implementation of privacy policies and practices:

> NOTICE – An organization should inform customers about (1) the purposes for which information is collected, (2) uses of the information provided, (3) the manner in which the customer can contact the entity to change or update information provided by the customer, (4) other parties to whom information is shared, and (5) the choices for the customer to limit the use of information provided or the consequences to the customer if certain information is not provided.
>
> CHOICE – The entity should offer customers to choose (or opt-out) whether their personal information is disclosed to third parties. For sensitive information, the entity

[1] As defined by the European Union (EU) directives, and the United States Safe Harbor Privacy Principles, July 21, 2000.

should provide an explicit (**opt-in**) choice if information is to be disclosed to a third party or for a purpose other than that for which is was originally collected.

ONWARD TRANSFER – The entity should apply the Notice and Choice guidelines in order to transmit information to other entities or parties not a part of the original transaction.

SECURITY – The entity that gathers, maintains, or uses personal information must take reasonable precautions to protect the information from loss, misuse, unauthorized access, disclosure, alteration, and destruction.

DATA INTEGRITY – The entity should take reasonable care that the information it collects, whether personal or sensitive, be relevant for the purposes for which it is to be used.

ACCESS – Customers should have access to their own personal or sensitive information for the purposes of correction, update and deletion.

ENFORCEMENT – The entity should provide procedures for assurance of compliance with its own privacy policies and independent recourse procedures to address any unresolved complaints and disputes.

Global Impact of Privacy Criteria

E-commerce by its nature is global. As companies cross international boundaries, they are faced with the challenges of meeting standards and complying with laws regarding privacy. Merchants who wish to tap into the global marketplace may find that without adequate privacy standards and disclosures at their site may face prohibitions or restrictions on how they do business.

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

Countries around the globe are putting policies in place to assure their citizens that their information is kept private. The European Union (EU) privacy directives took an early lead in this area, and Canada has recently passed similar privacy legislation. The U.S. Department of Commerce has issued its Safe Harbor Principles in July of 2000, and as of August 2000, the United States also has several privacy bills under consideration, as do several other countries around the globe. WebTrust currently meets the critical requirements regarding privacy and consumer recourse for information obtained through e-commerce as required by these initiatives.

In response to global need, companies, consumers, and other entities around the world can benefit from the WebTrust Program. The WebTrust Program is offered in most countries around the world by international accounting firms. In addition, many institutes are offering their

members the opportunity to become licensed to provide the WebTrust Program so that a broader market may be reached.

Consumer Recourse

As a result of the unique nature of e-commerce, Web site customers are concerned about how their complaints are addressed. If a Web site is unwilling or unable to address a consumer's concerns, what recourse does the consumer have? If the consumer is in one country and the business is in another, how will the consumer's rights be protected? Some governments already require consumer recourse procedures to ensure consumer protection. Traditional dispute resolution through the court system can be time-consuming and expensive.

To facilitate dispute resolution matters for both the consumer and the online business, the National Arbitration Forum (NAF) has assisted in the design of a program for e-commerce and specifically WebTrust. Forms and complaints can be filed electronically, over the telephone or through the postal service. Through third-party dispute resolution, global consumers will now have access to low-cost, expedient arbitration. Companies that currently have a dispute resolution mechanism covering their e-commerce processes (or the privacy aspects thereof) would continue to use their current mechanism. All such mechanisms should conform to the Principles of Arbitration in Appendix C, "Consumer Arbitration," which includes a broad overview of the arbitration process. For countries that have programs mandated by regulatory bodies, that program would be followed and disclosed at the Web site.

The WebTrust Privacy criteria include a requirement that the audited entity both commit to the use of third-party dispute resolution that conforms to the Principles of Arbitration in Appendix C and that the entity disclose its procedures for consumer recourse for issues not resolved by the entity. Such commitment and disclosures are required for all entities[2]. Such third-party dispute resolution (that meets the requirements in Appendix C) may be provided by any organization or governmental function offering such service.

THE WEBTRUST SEAL OF ASSURANCE

The Web has captured the attention of businesses and consumers, causing the number and kinds of electronic transactions to grow rapidly. Nevertheless, many believe that e-commerce will not reach its full potential until customers perceive that the risks of doing business electronically have been reduced to an acceptable level. Customers may have legitimate concerns about privacy and anonymity. In the faceless world of e-commerce, participants need the assurance of an objective third party. This assurance can be provided by an independent and objective certified public accountant (CPA), chartered accountant (CA), or their equivalent, (referred to as a "practitioner") and demonstrated through the display of the WebTrust Seal.

[2] In some countries around the world, third party arbitration is not an accepted means for the handling of consumer complaints. In those countries, the site should follow customary laws and regulations. Such practices should be disclosed at the Web site.

The WebTrust Privacy Seal of assurance symbolizes to potential customers that a practitioner has evaluated and independently verified the Web site's disclosed privacy practices and related controls and has issued a report with an unqualified opinion. The practitioner's report ordinarily provides an opinion that, during the period covered by the examination, the entity, in all material respects—

- Disclosed its privacy practices for electronic commerce,
- Complied with such privacy practices,
- Maintained effective controls to provide reasonable assurance that personally identifiable customer information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices

based on the AICPA/CICA WebTrust Privacy Criteria.

See Appendix A, "Illustrative Practitioner Reports." The WebTrust Privacy Principle and Criteria reflect fundamental standards for disclosure of information privacy practices and maintenance of related controls over information privacy.

THE PRACTITIONER AS AN ASSURANCE PROFESSIONAL

Practitioners are in the business of providing assurance services, the most publicly recognized of which is the audit of financial statements. An audit opinion signed by a practitioner is valued because these professionals are experienced in assurance matters and financial accounting subject matter and are recognized for their independence, integrity, discretion, and objectivity. Practitioners also follow comprehensive ethics rules and professional standards in providing their services. However, financial statement assurance is only one of the many kinds of assurance services that can be provided by a Practitioner. Practitioners also provide assurance about internal controls and compliance with specified criteria. The business and professional experience, subject matter expertise (e-commerce information systems security, privacy, auditability, and control) and professional characteristics (independence, integrity, discretion, and objectivity) needed for such projects are the same key elements that enable a Practitioner to comprehensively and to objectively assess the risks, controls, and business disclosures associated with e-commerce.

OBTAINING AND KEEPING THE WEBTRUST SEAL OF ASSURANCE

The Assurance Process

The entity's management will make representations or assertions to the practitioner ordinarily along the following lines:

> ABC Company, on its Web site for electronic commerce (at WWW.ABC.COM), during the period Xxxx xx, 200x through Yyyy yy, 200x—
>
> - Disclosed its privacy practices for electronic commerce,
> - Complied with such privacy practices,

- Maintained effective controls to provide reasonable assurance that personally identifiable customer information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices

based on the AICPA/CICA WebTrust Privacy Criteria.

For an initial representation, the historical period covered typically would be at least two months or more, as determined by the practitioner. (In certain circumstances, practitioners can issue an initial report covering a period of less than two months, including a point-in-time report. In these circumstances, the initial representation would need to be modified. See guidance below under the section "Other Reporting Issues.") For subsequent representations, the period covered should begin with the end of the prior period to provide continuous representation.

In order to have a basis for such representations, the entity's management should have implemented effective internal controls[3] for the privacy of its e-commerce transactions. Helpful guidance on appropriate control frameworks can be found, for example, in material developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in the United States, and the Criteria of Control (CoCo) in Canada. Nevertheless, for purposes of obtaining the WebTrust Seal of assurance, the practitioner will only evaluate those elements of internal control that are relevant to privacy of information obtained through e-commerce. In professional engagements, like WebTrust, an analysis and understanding of the internal controls that surround business processes is important. Management's tone with regard to establishing and following sound business practices, its commitment to assure that it follows its own practices, and its process for managing change are among the elements of sound control environment practices. The control environment reflects the overall attitude, awareness, commitment, and actions of management concerning the importance of internal control and its importance in the entity. A strong control environment is one that will enhance e-commerce and promote customer confidence and trust.

[3] Certain WebTrust entities rely upon a Third Party Service Provider (TPSP) to perform key processing and administer security relating to the Web 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 WebTrust entity. In these situations, the WebTrust practitioner may refer to the "Guide to Practitioners and Users of a Third Party Service Provider Practitioner Report in a WebTrust engagement," which has been prepared by the AICPA/CICA Electronic Commerce Assurance Task Force and provides guidance for the WebTrust practitioner. This Guide may be found at (www.aicpa.org/webtrust/index.htm and the CICA site www.cica.ca/webtrust).

An independent, objective and knowledgeable practitioner will perform tests of these representations under AICPA or CICA professional standards[4] and provide a professional opinion, which adds to the credibility of management's representations.

Scope of Work

WebTrust Privacy focuses on private and/or sensitive customer information obtained as a result of e-commerce. However, where such information is commingled with customer information obtained by other means, the practitioner will need to consider the entity's privacy practices and related controls covering all such customer information.

Transfer of Information to Third Parties

If the entity passes personal information on to third parties, it has the option to disclose any limitations on the reliance it places on the privacy practices and controls of such third parties. In the absence of such disclosures: (1) the entity is assumed to be relying on such third-party practices and controls, and (2) the entity needs to obtain assurance or representation that the third-party privacy practices and controls provide appropriate protection for such information in conformity with the entity's disclosed privacy practices. The assurance or representation obtained by the entity should be in an appropriate form, such as contractual provisions, representation letters from the third party, or audits of the third-party's privacy practices and controls.

The practitioner considers the significance of privacy practices and controls of such third parties, the reliance of the entity on such practices and controls, and the sources of such assurance or representation obtained by the entity. The practitioner then designs and applies auditing procedures appropriate in the circumstances.

Obtaining the Seal

To obtain the WebTrust Seal of assurance, the entity must meet the WebTrust Principle for Privacy as measured by the WebTrust Criteria associated with the principle. In addition, the entity must, (1) engage a practitioner, who has a WebTrust business license from the AICPA, CICA, or other authorized national accounting institute, to provide the WebTrust service and, (2) obtain an unqualified report from such practitioner.

---

[4] These services are performed in the United States under the AICPA's Statements on Standards for Attestation Engagements (AICPA, *Professional Standards*, vol. 1, AT sec. 100) or in Canada under the CICA's Standards for Assurance Engagements (also known as CICA Handbook Section 5025). Practitioners will need the appropriate skills and experience, training in the WebTrust service offering, and a WebTrust business license from the AICPA or CICA to provide the WebTrust services to their clients. The practitioner needs to perform an examination (audit) level engagement to award the WebTrust Seal. A review-level engagement is not sufficient. The WebTrust name has been servicemarked by the AICPA and trademarked by the CICA. Under the terms of the servicemark/trademark, the practitioner can provide assurance on the WebTrust Principles and Criteria in a report only when such report is based on an engagement under AICPA *Professional Standards*, Section AT 100, at the examination level, the CICA Standards for Assurance Services, Section 5025, at the audit level, or similar standards and level of assurance in other countries as specifically authorized by the AICPA/CICA.

Keeping the Seal

Once the seal is obtained, the entity will be able to continue displaying it on its Web site provided the following are performed.

1. The practitioner updates his or her assurance examination of the assertion on a regular basis. The entity must continue to obtain an unqualified report from such practitioner. The interval between such updates will depend on matters such as the following:

   - The nature and complexity of the entity's operation
   - The frequency of significant changes to its privacy disclosures, policies, and related privacy and security controls
   - The relative effectiveness of the entity's monitoring and change management controls for ensuring continued conformity with the WebTrust Privacy Criteria as such changes are made
   - The practitioner's professional judgment.

   For example, an update might be required more frequently for a financial institution's fast-changing Web site for securities transactions than for an online service that sells archival information using a Web site that rarely changes. *In no event should the interval between updates exceed six months and this interval often may be considerably shorter*. In order to provide continuous coverage and retain the seal, the period covered for update reports should either begin with the end of the prior period or the start of the period in the initial report issued under this version of WebTrust.

2. During the period between updates, the entity should undertake to inform the practitioner of (1) any significant changes to its information privacy policies, practices, processes, and controls particularly if such changes might affect the entity's ability to continue meeting the WebTrust Privacy principle and corresponding criteria, or (2) the manner in which they are met or a failure to meet them. Such changes may trigger the need for an assurance update or, in some cases, removal of the seal until an update examination by the practitioner can be made. If the practitioner becomes aware of such a change in circumstances, he or she would determine whether an update examination would need to be performed and whether the seal would need to be removed until the update examination is completed and the auditor's updated and unqualified report is issued.

The Seal Management Process

The WebTrust Seal of assurance will be managed by a Seal Manager along the following lines.

- The licensing authority authenticates WebTrust practitioners and establishes an identification (ID) and password with each practitioner.
- When the practitioner is prepared to issue a WebTrust Seal, the practitioner contacts the licensing authority. Upon payment of a registration fee, the practitioner receives IDs and passwords unique to the engagement. The Seal Manager issues these to the practitioner in pairs. One set allows the practitioner to read and write to the secure server (see below) and the other permits the entity to preview the presentation. The registration fee is an annual amount as determined by the licensing authority.

- The practitioner posts a draft of the practitioner's report and management's assertions to the secure server preview site.
- The Seal Manager then delivers a graphic copy of the WebTrust Seal to the entity with the appropriate links to the preview site. Notification of delivery is provided to the practitioner.
- When the practitioner determines that the seal may become active, the practitioner requests the Seal Manager to transfer the information from the preview site to the active WebTrust site to allow public access. The practitioner provides to the Seal Manager the expiration date for the engagement (i.e., the date by which the seal should be renewed which is normally six months).
- The seal remains valid for the period provided by the practitioner plus a one-month grace period, unless removed for cause. The one-month period is to allow sufficient time to complete the subsequent engagement and other open items. (For example, if the seal expires on June 30, xxxx, the practitioner has thirty days to complete open items and prepare new documents for posting with the Seal Manager. The next examination period begins July 1, xxxx.)
- If the practitioner determines that the seal should be removed from the entity's Web site, the practitioner will immediately notify the entity and request that the seal be removed from the entity's site. The practitioner will then notify the Seal Manager to remove all the relevant information from the active WebTrust site and to replace it with a statement that the WebTrust Seal for this site is no longer valid.
- The Seal Manager will notify the practitioner thirty days prior to expiration that the seal needs to be renewed. The Seal Manager may revoke seals if the registration fee for the seal is unpaid or for other sufficient cause.

Seal Authentication

To verify that the seal displayed on a Web site is authentic, the customer can—

- "Click" on the seal. The customer will then be linked through a secure connection to a WebTrust Seal verification page hosted by the Seal Manager. It identifies the entity and confirms that the site is entitled to display the WebTrust Seal. It also includes the practitioner's report and management's assertions (if appropriate) as well as links to the appropriate Principle(s), and other relevant information.

- Access the list of entities that have received a WebTrust Seal maintained by the Seal Manager at www.webtrust.org/list.htm. An entity is registered on this list when the seal is issued. Because a seal may be issued for any one, or any combination, of the WebTrust Principles, the list will also identify the specific Principles for which a WebTrust Seal has been issued. (Note this is currently under development with expected implementation in the first quarter of 2001.)

OTHER REPORTING ISSUES

Special Issues for Initial Reports

Typically, an initial report would need to cover a period of two months or more. However, an initial report covering a period of less than two months (including a point-in-time report) can be issued in the following circumstances (guidance that should be considered in these circumstances has been provided in the narratives and in Table 1 below) -

1. When an entity begins the WebTrust program, or

2. When an entity wishes to restore the WebTrust Seal following a significant event that caused the entity to no longer comply with the criteria (that necessitated removal of the auditor's report and the WebTrust Seal from the entity's site).

Similar to any attest engagement, before a practitioner can render an initial audit opinion, sufficient, competent and appropriate evidential matter needs to be obtained. For all criteria, there needs to be sufficient client transaction volumes and other procedure and control evidence to provide the practitioner with the necessary evidential matter. Therefore, in accepting an engagement that will result in the issuance of a report on a period of less than two months (including a point-in-time report) the practitioner should consider, as it relates to management's assertion about compliance with disclosed practices and the operating effectiveness of its controls, whether there will be an appropriate testing period ("look-back period") to provide sufficient evidence to enable the practitioner to issue such a report. The period over which a practitioner should perform tests is a matter of judgment. Additionally, the look-back period appropriate for testing controls may be different in length than the period of time necessary to test compliance.

For example, the period of time over which the practitioner would need to perform tests of controls to determine that such controls were operating effectively will vary with the nature of the controls being tested and with the frequency with which the specific controls operate and specific policies are applied. Some controls operate continuously while others operate only at certain times.

The period of time over which the practitioner would need to perform tests to provide assurance that the entity complied with its disclosed practices will be dependent upon the nature of the practices and the frequency and sufficiency of the evidence. For example if an entity discloses that it will comply with a certain practice at the end of each month, evidence will only exist at month's end.

If it is concluded that there will be an appropriate "look-back period" to provide for such evidential matter, then the practitioner may undertake the engagement to issue a report covering a period of less than two months, or a point-in-time report, on the site's compliance with practices and the effectiveness of controls. If the practitioner decides to issue a point-in-time report, the report should be modified to indicate that the firm has examined management's assertion as of Yyyy yy, 2000, rather than during a period.

In some circumstances, the auditor may conclude that the available "look-back" period is sufficient to obtain evidence regarding the effectiveness of controls, but not sufficient to obtain sufficient competent evidential matter regarding the entity's compliance with its disclosed privacy practices. In such circumstances (and only in these circumstances), a practitioner may accept an engagement to issue an audit opinion that does not address the entity's compliance with its disclosed privacy practices. In this situation, the auditor should modify the introductory and scope paragraphs of his or her report, so as not to indicate that the report is extending to compliance. All subsequent opinions would need to address disclosures, compliance with disclosures, and effectiveness of controls. (Please see section below, "Modifications to Practitioner's Report when not Reporting on Compliance" for further guidance and an illustration of modification to the wording in such a report.)

The AICPA/CICA will be releasing a document in the future which will provide more reporting guidance and further illustrative examples of point-in-time reports (as well as other sample reports). In the interim, the WebTrust practitioner should, in addition to considering the guidance herein, consider the relevant attest standards and consult with their practice management team with respect to the wording of such a report, to assure that he or she is complying with such standards.

The length of the relevant initial period should be determined by the practitioner's professional judgement based on factors such as those set out in Table 1 below.

Table 1

Considerations for use of a Shorter Initial Period	*Considerations for use of a Longer Initial Period*
• Clients for whom control examinations have already been performed • Established site, with little transaction volatility • Operations that experience infrequent changes to disclosures, policies and related controls • Start-up operation with significant transaction volumes and operating conditions (typical of expected normal operations) during the auditor's pre-implementation testing period and a transition to a live operational site that expects infrequent changes in policies and controls once it is operational	• Start-up operation that has not generated sufficient transaction volume and typical operating conditions during the pre-implementation stages • Operations that experience volatile transaction volumes • Complex operations • Operations that experience frequent changes to disclosures, policies and related controls or significant instances that lack compliance with disclosures, policies and related controls

Once the WebTrust Seal is obtained pursuant to this type of engagement, the entity will be able to continue displaying it on its Web site for a period determined by the practitioner (that does not exceed six months), provided that the entity performs the procedures set out in the section

"Keeping the Seal".

Considerations when Restoring a Removed WebTrust Seal

In the situations set out in No. 2 above, in which entity's management has taken steps to remedy the prior removal of a WebTrust Seal, it is important that management consider disclosing to its users the nature of the significant event that created the "out of compliance" situation and the steps taken to remedy the situation. The entity should consider disclosing the event on its Web site or as part of its management assertion. Likewise, before issuing a new report, the practitioner should consider the significance of the event, the related corrective actions, and whether appropriate disclosure has been made. The practitioner also should consider whether this matter should be (1) disclosed as part of management's assertion, (2) emphasized in a separate explanatory paragraph in the auditor's report, or (3) both.

Modifications to Practitioner's Report when not Reporting on Compliance

As discussed above, in a situation in which a practitioner concludes that the available "look-back" period for an initial report is sufficient to obtain evidence regarding the effectiveness of controls over compliance, but not sufficient to obtain sufficient competent evidential matter regarding the entity's compliance with its disclosed privacy practices, the practitioner may accept an engagement to issue an initial audit opinion that does not address the entity's compliance with its disclosed privacy practices. In this situation, the practitioner should modify the introductory and scope paragraphs so as not to indicate that his or her report is extending to compliance with practices, but rather that he or she has examined management's assertion that the company has maintained effective controls to provide reasonable assurance that it complied with its disclosed practices.

An example of an introductory paragraph for a point-in-time report in this situation, when reporting on management's assertion, should be revised as follows -

We have examined management's assertion [hot link to management's assertion] that ABC Company Inc. (ABC) as of Yyyy yy, 2000—

- *Disclosed its privacy practices for electronic commerce, and*
- *Maintained effective controls to provide reasonable assurance that it complied with those privacy practices and that personally identifiable information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices*

based on the AICPA/CICA WebTrust Privacy Criteria [hot link to Privacy principle & criteria.] These practices, disclosures, and controls are the responsibility of ABC Company's management. Our responsibility is to express an opinion based on our examination.

Additionally, the scope paragraph of the report should also be modified to reflect that the engagement has not extended to compliance as follows -

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

WEBTRUST PRIVACY PRINCIPLE AND CRITERIA[5]

Although e-commerce can be conducted through a number of means, including electronic bulletin boards and formalized EDI arrangements, all of which can affect consumer privacy, the focus of this version of the criteria is on e-commerce conducted through the Web.

This principle has been developed with the consumer-user in mind and, as a result, is intended to be practical and somewhat nontechnical in nature.

The WebTrust Privacy Principle[6]

> *The entity discloses its privacy practices, complies with such privacy practices, and maintains effective controls to provide reasonable assurance that personally identifiable information obtained as a result of electronic commerce is protected in conformity with its disclosed privacy practices.*

To enhance customer confidence in e-commerce, it is important that the customer is informed about the entity's privacy practices for e-commerce transactions. The entity needs to disclose its practices relating to the manner in which it uses, protects, and maintains personal information. Additionally, the entity should also disclose management's agreement to third-party arbitration to settle customer complaints.

The WebTrust Criteria

In order to provide more specific guidance, WebTrust Criteria have been developed for each WebTrust Principle. The entity must be in conformity with these criteria to obtain and maintain its WebTrust Seal. The criteria are organized into the four broad areas of disclosures; policies, controls, and objectives; procedures and technology tools; and monitoring/performance measures.

A three-column presentation has been used to present and discuss the criteria. The first column presents the criteria—the attributes that the entity must meet to be able to demonstrate that they have achieved the principle. The second and third columns provide illustrative disclosures and controls for business to consumer transactions and for transactions applicable to service providers. These are examples of disclosures the entity might make and controls that the entity might have in place to conform to the criteria. Alternative and additional disclosures and controls also can be used. Since privacy issues relate primarily to dealings with individual retail customers, no illustrations have been included for business-to-business transactions.

---

5 These criteria meet the definition of "criteria established by a recognized body" described in the third General Standard for attestation engagements in the United States (AICPA, *Professional Standards*, vol. 1, AT sec. 100.14) and in the standards for assurance engagements in Canada (CICA *Handbook*, paragraph 5025.41).

6 The WebTrust Principles meet or exceed the significant requirements of the European Union (EU) Privacy Directives and The Online Privacy Alliance (OPA) Guidelines as of October 1999, Canadian Privacy Law, C6, The OECD Guidelines, and the U.S. Safe Harbor Privacy Principles issued July 21, 2000.

The entity typically must be able to demonstrate that (1) it complied with its disclosed privacy practices for e-commerce, (2) its controls over privacy operated effectively, (3) it maintained a control environment that is conducive to reliable privacy disclosures and effective controls, and (4) it maintained monitoring procedures to ensure that such privacy practices remain current and such controls remain effective in conformity with the WebTrust Privacy Criteria. These concepts are an integral part of the WebTrust Criteria.

WebTrust Principle and Criteria
Privacy

Principle

The entity discloses its privacy practices, complies with such privacy practices, and maintains effective controls to provide reasonable assurance that personally identifiable information obtained as a result of electronic commerce is protected in conformity with its disclosed privacy practices.

Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Service Providers
A Disclosures		
A.1 The entity discloses on its Web site its information privacy practices. These practices include, but are not limited to, the following disclosures:		
A.1.1 The specific kinds and sources of information being collected and maintained, the use of that information, and possible third-party distribution of that information. • If information is provided to third parties, disclosure might include any limitations on the reliance on the third party's privacy practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's privacy practices and controls that meet or exceed those of the entity. Such third-parties might include: – Parties who participate in completing the transaction (for example, credit card processors, delivery services, and fulfillment organizations)	We will need certain information — such as name, Internet address or screen name, billing address, type of computer, and credit card number — in order to provide our service to you. Your email address is used to send information about our company. Your credit card number is used for billing purposes for the products you order. We may also use this information, along with information such as your age, income level, and postal code, to keep you informed about additional products and services from our company, and to send promotional material that may be of interest to you from some of our partners. Your age, income level, and postal code are also used to tailor the content displayed to correspond to your preferences. We do not provide information	We will need certain information — such as name, Internet address or screen name, billing address, social security/insurance number, occupation, citizenship, date of birth, and investing experience. We may also use this information, along with information such as your age, income level, and postal code, to keep you informed about additional products and services from our company, and to send promotional material that may be of interest to you from some of our partners. Your age, income level, and postal code are also used to tailor the content displayed to correspond to your preferences.

Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Service Providers
– Parties not related to the transaction (for example, marketing organizations to whom information is provided)	gathered from you to any other third parties except as required by law.	
A.1.2 Choices regarding how personal information collected from an individual online may be used and/or distributed. Individuals are given the opportunity to opt-out of such use, by either not providing such information or denying its distribution to parties not involved with the transaction.	You can choose not to receive information and promotional material from us and/or our partners by letting us know on the registration screen when you sign up for the product or service. If you subsequently wish to change your preference to opt-in or opt-out, go to the xxx screen, or send an email to xxx@domain.com with the message opt-in or opt-out in the subscribe field.	
A.1.3 Sensitive information needed for the e-commerce transaction. Individuals must **opt-in** before this information is gathered and transmitted.	Before we can process your insurance application, we require that you click here to give us your permission to submit your medical history to the various insurance companies we use. This is your explicit permission for us to process your request. If you do not wish to have this information transmitted, we will be unable to process your application. You may call our customer service department for additional information or assistance.	
A.1.4 The consequences, if any, of an individual's refusal to provide information or of an individual's decision to opt-out (or not **opt-in**) of a particular use of such information.	The minimum information you need to provide to complete the transaction is highlighted on the Web page. You will be unable to place an order without providing this minimum information.	Without providing the information requested and highlighted by an asterisk, you will be unable to establish an account.
A.1.5 How personal information collected can be reviewed and, if necessary, corrected or removed.	This site provides you with the ability to correct, update, or remove your information by emailing CustServ@ABC.COM.	You may review your customer record on our Web site through a secure session and change certain information. Changes to certain other information, such as date of birth and other information used to verify identity, need to be made in writing.

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Service Providers
A.2	If the Web site uses cookies or other tracking methods (for example, Web bugs and middleware), the entity discloses how they are used. If the customer refuses cookies, the consequences, if any, of such refusal are disclosed.	Cookies are used to personalize Web content and suggest items of potential interest based on your previous buying habits. This cookie can only be read by us. If you do not accept this cookie, you may be asked to reenter your name and account number several times during a visit to our Web site or if you return to the site later. By accepting a cookie, certain information (disclose information) will be tracked and used for marketing purposes. Our cookies expire in thirty days. Certain advertisers on our site use tracking methods, including cookies, to analyze patterns and paths through this site. Certain advertisers on our site use tracking methods, including cookies, to analyze patterns and paths through this site. To opt-out of this practice, refer to their privacy policy at www.domain.com/privacy/opt-out.html.	
A.3	The entity discloses its procedure for individuals, companies or other users to inform the entity about breaches or possible breaches to the privacy and security of its electronic commerce system(s).	Should you feel that there has been a breach to the security of this site please contact us *immediately* at (800) 123-1234.	
A.4	The entity discloses information to enable customers to contact it for questions or support.	If you have any questions about our organization or our policies on privacy as stated at this site, please contact CustServ@ABC.COM. Access to your customer data file is made available to our customer support representatives in order to fully service your inquiries. After hours, our customer support inquiries are managed by our service provider xxx who is contractually required to comply with our privacy policy.	

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Service Providers
A.5	The entity discloses its procedures for consumer recourse for issues regarding privacy that are not resolved by the entity. These complaints may relate to collection, use and distribution of private information, and the consequences for failure to resolve such complaints. This resolution process should have the following attributes: • Management's commitment to use a specified third party dispute resolution service or other process mandated by regulatory bodies in the event the customer is not satisfied with the entity's proposed resolution of such a complaint together with a commitment from such third party to handle such unresolved complaints. Procedures to be followed in resolving such complaints, first with the entity and, if necessary, with the designated third party. • What use or other action will be taken with respect to the private information, which is the subject of the complaint, until the complaint is satisfactorily resolved.	Transactions at this site, with respect to privacy, are covered by binding arbitration and arbitrated by the National Arbitration Forum. They can be reached at www.arb-forum.org or by calling toll-free (800) 474-2371. For the details of the terms and conditions of arbitration, click here. Transactions at this site, with respect to privacy, are covered by binding arbitration conducted through our designated arbitrator (name of arbitrator). They can be reached at www.name.org or by calling toll-free (800) 111-2222. For the details of the terms and conditions of arbitration, click here. Transactions at this site, with respect to privacy, are covered by the Banking (Canadian Banking) Industry Ombudsman of the Bankers Association who can be reached at www.bankom.org.xy or by calling toll-free (800) xxx-xxxx. For transactions at this site, with respect to privacy, should you, our customer, require follow up or response to your questions or complaints, you may contact us at www.xxx.org. If your follow up or your complaint is not handled to your satisfaction, then you should contact the electronic commerce ombudsman who handles consumer complaints for e-commerce in this country. He can be reached at www.ecommercombud.org or by calling toll-free at (800) xxx-xxxx.	
A.6	The entity discloses any additional privacy practices needed to comply with applicable laws or regulations or any self-regulatory programs in which the entity participates.	Federal law requires that all personal information be removed from the system after three years of inactivity.	The National Privacy Council requires that all information provided by customers at this site be stored in an encrypted database for a period of five years.

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Service Providers
A.7	The entity discloses changes or updates to its privacy practices.	During the period from May 31 to August 31, 2xxx, we collected customer telephone numbers. Starting September 1, we no longer require this information for the processing of your transaction. On September 30, xxxx, we were acquired by XYZ Co. Accordingly, we adopted the privacy policies of XYZ Co. that allow the distribution of collected personal information to third parties. Since our previous policy did not allow for the distribution of such personal information, we will obtain your permission prior to the distribution of such information collected before September 30, xxxx.	
A.8	The entity clearly discloses to the site's visitors when they have left the site covered by the entity's privacy policy.	Many of our partners have pages that look and navigate like our site. We will notify you via a one-time pop up window to let you know that you are leaving our site and our privacy policy practices. We strive to protect your information and suggest that you read the privacy policies of the site to which you are redirected BEFORE supplying any personal information. We will not pass any information to these sites in accordance with our privacy policy without your express consent.	

Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Service Providers
B	**Policies, Goals and Objectives**	
B.1	The entity's policies regarding 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 in Appendix C.	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.	

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Service Providers
B.2	The employees responsible for the privacy of personally identifiable information are aware of and follow the entity's published privacy and related security policies.	As part of their orientation, the privacy policy is reviewed with new employees and the key elements of the policy and its impact on the employee are discussed. The employee 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. 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. 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.	
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 responsibilities for the enforcement of the company 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.

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Service Providers
B.4	The entity has allocated training and other resources to support its privacy and related security policies.	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 feed back as well as changes in privacy and security policies and procedures.	Management has an on-going privacy 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 privacy and security training courses put on by the IT Department. The CIO evaluates these programs and makes a quarterly report to the executive committee.
B.5	The entity's privacy and related security policies 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.	

Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Service Providers
C	**Procedures and Technology Tools**	
	Security Criteria That Relate to Privacy	
C.1	The entity has appropriate security procedures to establish new users.	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 Secure Socket Layer (SSL) session. User IDs and passwords are provided to the user and must contain non-alphanumeric characters.
C.2	The entity has procedures to identify and authenticate authorized users.	All users are required to provide a unique user ID and password to place an order or access their specific customer information.	System level access to all production systems (for example, UNIX and Windows NT) is provided via a strong identification and authentication mechanism (digital signature, one-time password, SecureID, or other system). 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.

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Service Providers
C.3	The entity has procedures to allow users to change, update, or delete their own user profile.	In order 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.	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 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 from both within the internal network and from the Internet.	
		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. Identification and authorization is accomplished through the combination of 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 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.

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Service Providers
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.	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. 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.	One-time passwords and/or smart cards restrict all system access from outside the entity, other than for customary e-commerce transactions through the Web page. Customer 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 customer access to only their network segments. The various LAN segments are firewalled from the rest of the networks.

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Service Providers
C.6	The entity has procedures to limit access to personally identifiable information to only authorized employees based upon their assigned roles and responsibilities.	Employee access to customer data is limited to individuals based upon their assigned responsibilities. Idle workstations as 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.	
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.	Private information is protected during transmission by using 128-bit encryption technology (SSL technology). The entity's Web site has a digital certificate, which can be checked using features in a standard Web browser.	
C.8	The entity has procedures to maintain system configurations that minimize security exposures potentially affecting private or sensitive information.	Company management routinely evaluates the level of performance it receives from the ISP which hosts the company Web site. This evaluation is done by evaluating the security controls the ISP has in place by an independent third party as well as by following up with the ISP management on any open items or causes for concern.	The service provider meets with its technology vendors on a regular basis (for example, SUN, Cisco and Microsoft). 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.

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Service Providers
	Privacy Specific Criteria		
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.	Company procedures require that customers are given the clear and conspicuous option as to the sharing of the customer's information with other parties not associated with the transaction and has controls in place to track those options within the company's database.	Company policy prohibits the sharing of any information gathered as a result of an e-commerce transaction to be shared or disclosed to individuals or other entities for any purpose.
C.10	The entity has procedures to ensure that private information obtained as a result of electronic commerce is used by employees only in ways associated with the entity's business.	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.	

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Service Providers
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.	The company only accepts data from the customer or other reliable sources and uses reliable collection methods. Prior to completing the transaction, the customer is 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.	Individuals may request a copy of their confidential profile via email. The profile will be mailed to the customer of record. Should any changes need to be made, an update form will be included with the profile. Some Information will need to be verified with other documents that will be requested when needed.
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.	The entity outsources technology support or service and transfers data to the outsource provider. The entity obtains representation as to the controls that are followed by the outsource provider and obtains a report on the effectiveness of such controls from the outsource provider's independent auditor.	

Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Service Providers
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 permission to store, alter, or copy information (other than cookies) in the customer's computer.	The company requests the customer's permission before it intentionally stores, alters, or copies information in the customer's computer. The company requests the customer's permission before it performs any diagnostic or inventory on the customer's computer. The consumer registration page notifies and requests permission from consumers to utilize cookies to expedite site registration and logon. Customers are prompted when files are to be downloaded as part of the service.	
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.	The entity maintains copies of all versions of the privacy policy. The entity attorney summarizes the key changes to this policy statement. Data collected before and after each privacy policy change are tracked in the entity's database. The entity sends notification of such changes and deletions to all affected customers and requests that the customers **opt-in** to the new policy. Customers who do not **opt-in** to the new policy will continue to be protected under the old policy.	

Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Service Providers
D	**Monitoring and Performance Measures**	
D.1 The entity has procedures to monitor the security of its electronic commerce systems.	The Information Security group uses the following monitoring tools: • COPS – This software provides a snap shot of the system which is analyzed on a monthly basis. • Tripwire – This is a real time monitor which is used to detect intruders. • SATAN – This software is run monthly and provides a security analysis of the system. In addition, the group maintains and analyzes the server logs.	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 in place to keep its disclosed privacy and related security policies current with laws and regulations and to monitor adherence to its current privacy and security policy practices.	Staff meetings are held on a regular basis to address current privacy concerns and their findings are discussed at quarterly management meetings. The company 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.	Legal counsel for the company reviews the privacy policy on an annual basis to assess whether modifications are required. The company is active in current public policy forums and monitors these forums for possible impact on its privacy policy.

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Service Providers
D.3	The entity has procedures in place to test its privacy and security incident policy and update it as needed due to technology changes, changes in the structure of the electronic commerce system(s), or information gained from tests of its plan.	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 biannual 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.	All system logs are monitored and evaluated on a routine 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 back to the customer and CIO or the customer may contact the Incident Response hot-line by telephoning (888) 911-0911 24x7.	

APPENDIX A - ILLUSTRATIVE PRACTITIONER REPORTS

This Appendix presents four illustrative reports for WebTrust Privacy Program engagements. Illustrations No. 1 and No. 2 are prepared in accordance with the AICPA's attestation standards. Illustration No. 3 and No. 4 are prepared in accordance with the CICA's assurance standards.

Under the United States *Attestation Standards*, the first paragraph of the practitioner's report will state that the practitioner has performed an examination of management's assertion about compliance with the WebTrust criteria. The practitioner may opine (1) on management's assertion or (2) directly on the subject matter. Illustration No. 1 is a report in which the practitioner opines directly on the subject matter and Illustration No.2 is a report in which the practitioner opines on management's assertion.

Both attest and direct engagements and reporting are supported in Canada. The practitioner's communication will vary 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. The assertion evaluates, using suitable criteria, the subject matter for which the accountable party is responsible. In a direct reporting engagement, the practitioner's conclusion will evaluate directly, using suitable criteria, 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.

The reports presented in this Appendix A are for illustrative purposes and should be modified in accordance with the applicable professional standards as the specific engagement facts and circumstances warrant.

Reporting Examples Based on AICPA Standards

Illustration No. 1 for Use in the United States
Direct Report Based on AICPA Standards

Independent Auditor's Report

To the Management of ABC Company, Inc.:

We have examined management's assertion [*hot link to management's assertion*] that ABC Company Inc. (ABC Company), during the period Xxxx xx, 2000 through Yyyy yy, 2000 —

- Disclosed its privacy practices for electronic commerce,
- Complied with such privacy practices, and
- Maintained effective controls to provide reasonable assurance that personally identifiable information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices

based on the AICPA/CICA WebTrust Criteria [*hot link to privacy principle and criteria*]. These practices, disclosures, compliance and controls are the responsibility of ABC Company'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 ABC Company's disclosed privacy practices and the related controls over privacy, (2) testing compliance with its disclosed 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, ABC Company in all material respects—

- Disclosed its privacy practices for electronic commerce,
- Complied with such privacy practices, and
- Maintained effective controls to provide reasonable assurance that personally identifiable information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices

during the period Xxxx xx, 2000 through Yyyy yy, 2000 based on the AICPA/CICA WebTrust Privacy 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 (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) the degree of compliance with the policies or procedures may alter the validity of such conclusions.

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

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

Illustration No. 2 for Use in the United States

Report on Management's Assertion Based on AICPA Standards

Independent Auditor's Report

To the Management of ABC Company, Inc.:

We have examined management's assertion [*hot link to management's assertion*] that ABC Company Inc. (ABC Company), during the period Xxxx xx, 2000 through Yyyy yy, 2000—

- Disclosed its privacy practices for electronic commerce,
- Complied with such privacy practices, and
- Maintained effective controls to provide reasonable assurance that personally identifiable information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices

based on the AICPA/CICA WebTrust Criteria [*hot link to privacy principle and criteria*]. These practices, disclosures, compliance and controls are the responsibility of ABC Company'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 ABC Company's disclosed privacy practices and the related controls over privacy, (2) testing compliance with its disclosed 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, ABC Company's management assertion referred to above is fairly stated, in all material respects, based upon AICPA/CICA Web Trust Privacy 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 (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) the degree of compliance with the policies or procedures may alter the validity of such conclusions.

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

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

Reporting Examples Based on CICA Standards

Illustration No. 3 for Use in Canada

Direct Report Based on CICA Standards

Auditor's Report

To the Management of ABC Company, Ltd.:

We have audited —

- The disclosed privacy practices for electronic commerce of ABC Company, Ltd. (ABC Company),
- Compliance with such privacy practices, and
- The effectiveness of its controls to provide reasonable assurance that personally identifiable information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices,

during the period Xxxx xx, 2000, through Yyyy yy, 2000. These policies, disclosures, compliance, and controls are the responsibility of ABC Company's management. Our responsibility is to express an opinion, based on our audit, on the conformity of those disclosures, compliance, and controls with the CICA/AICPA WebTrust Privacy Criteria, [hot link to privacy principle and criteria].

Our audit was conducted in accordance with standards for assurance engagements established by the Canadian Institute of Chartered Accountants (CICA). 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 ABC Company's disclosed privacy practices and the related controls over privacy, (2) testing compliance with its disclosed 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, ABC Company, in all material respects—

- Disclosed its privacy practices for electronic commerce,
- Complied with such privacy practices,
- Maintained effective controls to provide reasonable assurance that personally identifiable information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices

during the period Xxxx xx, 2000, through Yyyy yy, 2000, in accordance with CICA/AICPA WebTrust Privacy Criteria.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) the degree of compliance with the policies or procedures may alter the validity of such conclusions.

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

[City, Province]
{Date of report}

[Name of CA firm]
Chartered Accountants

Illustration No. 4 for Use in Canada

Attest Report Based on CICA Standards

Auditor's Report

To the Management of ABC Company, Ltd.:

We have audited management's assertion [hot link to management's assertion] that ABC Company Ltd. (ABC Company), during the period Xxxx xx, 2000 through Yyyy yy, 2000—

- Disclosed its privacy practices for electronic commerce,
- Complied with such privacy practices, and
- Maintained effective controls to provide reasonable assurance that personally identifiable information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices

in accordance with the AICPA/CICA WebTrust Criteria [hot link to privacy principle and criteria]. These practices, disclosures, compliance, and controls are the responsibility of ABC Company's management. Our responsibility is to express an opinion based on our audit.

Our audit was conducted in accordance with standards for assurance engagements established by the Canadian Institute of Chartered Accountants (CICA). 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 ABC Company's disclosed privacy practices and the related controls over privacy, (2) testing compliance with its disclosed 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, management's assertion for the period Xxxx xx, 2000 through Yyyy yy, 2000, is fairly stated, in all material respects, in accordance with the CICA/AICPA Web Trust Privacy 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 (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) the degree of compliance with the policies or procedures may alter the validity of such conclusions.

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

[*City, Province]* *[Name of CA firm]*
{Date of report} *Chartered Accountants*

APPENDIX B - WEBTRUST SM/TM SELF-ASSESSMENT QUESTIONNAIRE FOR ON LINE PRIVACY

This questionnaire is for use by electronic commerce service providers in documenting their electronic commerce privacy practices, disclosures and related controls and in documenting a basis for their assertion or representation that "on its Web site at www.___.____ during the period _____, 200_ through _____, 200_ the entity—

- Disclosed its privacy practices for electronic commerce transactions
- Complied with such privacy practices
- Maintained effective controls to provide reasonable assurance that personally identifiable customer information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices

based on the AICPA/CICA WebTrust SM/TM Criteria.

Entity Name _____ Entity Location _____
Web Site URL _____ Server Location _____
Period Covered: From _____ Through _____
Date Prepared _____ Prepared By _____

General Information

Electronic commerce Activities to Be Covered

1. Describe the entity's electronic commerce activities that are asserted and represented to meet the WebTrust Principles and Criteria for On-Line Privacy.

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

   b) Who is the typical customer?

   c) What is the typical form of payment?

2. What is the Web site URL?

3. Who is responsible for controlling the disclosure of the entity's on-line privacy policies and its adherence to these policies and what is their reporting relationship to the entity's management?

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

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

Information Systems Used to Support Electronic commerce Activities

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

    a) Provide a description.

    b) Indicate who, in this entity, is responsible for each customer interface system

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

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

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

    a) Give a description.

    b) Indicate, who, in this entity, is responsible for the telecommunications and network systems.

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

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

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

    a) Provide a description.

    b) Indicate who, in this entity, is responsible for the supporting systems and technology identified.

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

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

Web Site Server Technology

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

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

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

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

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

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

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

    d) Install a Java Applet on the appropriate Web page

5. Identify the WebServer package used.

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

Control Environment

1. Describe the factors in the entity's organization that contribute to a control environment that is generally conducive to reliable privacy practice disclosures on its Web site and effective controls over monitoring the entities compliance with its disclosed privacy policies. Such factors might include, but are not limited to the following:

    a) Management's "tone at the top"

    b) Hiring, development, and retention of competent personnel

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

    d) Supervising its privacy activities and control procedures

    e) Employing a suitable internal auditing function that periodically audits matters related to the entity's electronic commerce privacy policies

    f) Other factors

Specific Privacy Online Criteria

A) Description of Information Privacy Practices

1) Describe the entity's information privacy and related security practices and how such practices are disclosed to customers for each of the following.

   a) What are the specific kinds and sources of information being collected such as:

      (i) Name

      (ii) Address

      (iii) Type of computer

      (iv) Credit Card Number

      (v) E-mail address

      (vi) Other relevant information

   b) How is the information collected used:

      (i) To send information about our company

      (ii) To bill for the customers order

      (iii) To send promotional material from/about our partners

      (iv) Other uses of private customer information, if any

   c) Possible third-party distribution of information collected. Disclosure might include any limitations on the reliance on the third party's privacy practices and controls. Possible third-parties might include:

      (i) Parties who participate in completing the transaction (for example, credit card processors, delivery services, and fulfillment)

      (ii) Parties not related to the transaction (for example, marketing organizations to whom information is provided)

   d) Choices regarding how personal information collected from an individual online may be used and/or distributed.

      (i) Opt-out of providing information

      (ii) Deny distribution to parties not involved with the transaction

(iii)Other

e) How do individuals “opt-in” before sensitive information needed for the electronic commerce transaction is gathered and transmitted?

f) The consequences, if any, of an individual's refusal to provide information or to opt-out of a particular use of such information.

g) How erroneous or incomplete personally identifiable information collected can be reviewed by the consumer and, if necessary, corrected or removed.

2) If the Web site uses cookies, or other tracking methods (for example, Web bugs), describe how they are used and the consequences, if any, of an individual's refusal to accept a cookie.

3) Describe the information the entity discloses to enable individuals, companies or other users to inform it about breaches or possible breaches to the privacy and security of its electronic commerce system(s).

4) Describe the information the entity discloses in order to enable customers to contact it for questions or support.

5) Describe the process the entity uses to resolve disputes including, at a minimum, the following:

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

b) How to resolve complaints related to the accuracy, completeness, and distribution of private customer information.

c) What use or other action will be taken with respect to the private information, which is the subject of the complaint, until the complaint is satisfactorily resolved.

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

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

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

6) Describe the entity’s process to identify and disclose changes or updates to its privacy and related security practices to comply with applicable laws or regulations or any self-regulatory programs in which the entity participates.

7) The entity discloses to the site’s visitors when they have left the site covered by the entity’s privacy policy.

B) Policies, Goals and Objectives

1) Describe the entity's policies regarding the protection of personally identifiable information including but not limited to the following:

   a) Notice to the customer regarding the information collected.

   b) Choice to the customer regarding the type(s) of information gathered and any options the customer has regarding the collection of this information.

   c) The procedures to add new users, modify access levels of existing users, and remove users who no longer need access.

   d) Access by employees based upon responsibilities and who authorizes that access.

   e) Access by the customer to his or her private information and corrective purposes

   f) How complaints about privacy can be addressed.

   g) Procedures to handle security incidents.

   h) Record retention and distribution practices.

   i) The commitment to use third-party dispute resolution processes

2) Describe how employees responsible for the privacy of personally identifiable information are made aware of the entity's published privacy and related security policies, and what actions are taken to ensure that employees follow such policies.

3) Identify to whom accountability for the privacy and related security policies has been assigned.

4) Describe the training and resources allocated to support its privacy and related security policies.

5) Describe the procedures used to assess whether the entity's privacy and related security policies are consistent with its disclosed privacy practices and applicable laws and regulations.

C) Procedures and Technology Tools

Security Criteria that Relate to Privacy

1) Describe the entity's security criteria that relate to privacy:

   a) The entity's procedures to establish new users.

   b) The entity's procedures to identify and authenticate authorized users.

c) The entity's procedures to allow users to change, update or delete their own user information.

d) The entity's procedures to limit remote access to the internal network to only authorized personnel.

e) The entity's procedures to prevent customers, groups of individuals, or other entities from accessing other than their own private or sensitive information.

f) The entity's procedures to limit access to personally identifiable information to only authorized employees based upon their assigned roles and responsibilities.

g) The entity's utilization of, at a minimum, 128-bit encryption to protect transmission of user authentication, verification, and sensitive or private information that is passed over the Internet from unintended recipients.

h) The entity's procedures to maintain system configurations that minimize security exposures potentially affecting private or sensitive information.

Privacy Specific Criteria

2) Describe the entity's privacy specific controls and procedures to:

a) Ensure that private information obtained as a result of electronic commerce is not disclosed to parties not essential to the transaction unless customers are clearly notified prior to providing such information. If the customer was not clearly notified when he/she submitted the information, customer permission is obtained before such information is released to third parties.

b) Ensure that private information obtained as a result of electronic commerce is used by employees only in ways associated with the entity's business.

c) Subject personally identifiable information collected, created or maintained by it to reasonable edit and validation checks as it is collected.

d) Determine 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 third party's disclosed privacy practices.

e) Ensure that customer permission is obtained before storing, altering or copying information on a customer's computer or the customer is notified with an option to prevent such activities.

(i) Ensure that cookies are not stored on a customer's computer if the customer has rejected the use of cookies.

(ii) Ensure permission is received from the customer to store, alter, or copy information (other than cookies) in the customer's computer.

f) Protect personally identifiable information in accordance with the privacy policies in place when such information was collected in the event that a disclosed privacy policy is deleted or changed to be **less** restrictive,. Clear and conspicuous customer notification and choice are required to allow the entity to follow the new privacy policy with respect to their personally identifiable information.

D) Monitoring and Performance Measures

1) Describe the entity's procedures to monitor the security of its electronic commerce systems.

2) Describe the entity's procedures to keep its disclosed privacy and related security policies current with laws and regulations and to monitor adherence to its current privacy and security policy practices.

3) Describe the entity's procedures to test its privacy and security incident policy and update it as needed due to technology changes, changes in the structure of the electronic commerce system(s), or information gained from tests of its plan.

4) Describe the entity's procedures to monitor and act upon privacy and security breaches.

APPENDIX C - CONSUMER ARBITRATION

This Appendix applies to engagements that use an arbitration program. Should a program mandated by a regulatory body be in effect, that program would be followed and disclosed. This Appendix provides additional information about the arbitration process. It outlines the process that would meet the WebTrust criteria. The attachments to this Appendix provided additional comments relative to the various countries where WebTrust services are offered.

The Arbitration Process – Background

Before arbitration can take place, two parties must agree to it. An agreement may take many forms other than a written contract. Both parties show their agreement by some reasonable, affirmative act. The Web site may invite acceptance by conduct, such as a check box or other means, and may propose limitations on the kind of conduct that constitutes acceptance. For example, consumers may find the following language at a site, which would constitute acceptance of an agreement:

BY ACCESSING THIS WEB SITE OR ORDERING PRODUCTS DESCRIBED ON THIS SITE, YOU AGREE TO BE BOUND BY CERTAIN TERMS AND CONDITIONS. PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY.

The terms and conditions would elaborate arbitration, consumer recourse and other issues for both the consumer and Web site.

WebTrust endorses the twelve principles noted below that form the basis of the arbitration process. These principles have been developed by The National Arbitration Forum (NAF). NAF, an organization based in the United States, has developed an arbitration process that is widely used. It is the model adopted for WebTrust regardless of whether NAF, or an affiliate of NAF, is retained for the arbitration process or an alternate organization is selected.

Under the model adopted for WebTrust, arbitration must be based on the rules of law, applied consistently. The twelve principles of the arbitration process are the following.

1. **FUNDAMENTALLY FAIR PROCESS** — All parties in an arbitration process are entitled to fundamental fairness.

2. **ACCESS TO INFORMATION** — Information about arbitration should be reasonably accessible before the parties commit to an arbitration contract.

3. **COMPETENT AND IMPARTIAL ARBITRATORS** — The arbitrators should be both skilled and neutral.

4. **INDEPENDENT ADMINISTRATION** — An arbitration should be administered by someone other than the arbitrator or the parties themselves.

5. **CONTRACTS FOR DISPUTE RESOLUTION** — An agreement to arbitration is a contract and should conform to the legal principles of contract.

6. **REASONABLE COST** — The cost of an arbitration should be proportionate to the claim. The prevailing party will recover the cost of initiating arbitration (if in fact the initiator of the complaint was the prevailing part) once the decision is final.

7. **REASONABLE TIME LIMITS** — A dispute should be resolved with reasonable promptness.

8. **RIGHT TO REPRESENTATION** — All parties have the right to be represented in an arbitration, if they wish, for example, by an attorney or other representative.

9. **SETTLEMENT & MEDIATION** — The preferable process is for the parties themselves to resolve the dispute.

10. **HEARINGS** — Hearings should be convenient, efficient, and fair for all.

11. **REASONABLE DISCOVERY** — The parties should have access to the information they need to make a reasonable presentation of their case to the arbitrator.

12. **AWARDS AND REMEDIES** — The remedies resulting from an arbitration must conform to the law.

Addendum 1 – United States

Overview of the National Arbitration Forum's Arbitration Process

In the United States, the National Arbitration Forum (NAF) has established an effective arbitration and mediation process. Although it is not mandatory for WebTrust clients to select NAF for its third-party arbitration service provider, it is required that the organization selected for the role follow the principles identified in Appendix C, "Consumer Arbitration," and suggested that the organization apply the NAF Code of Procedure[7] as well.

This section provides additional information about the arbitration process as followed by NAF

NAF has a simple and cost-effective method of filing a complaint. Complaints can be initiated online, over the telephone or through the postal service. In each case, complaints are tracked and monitored. The following is an overview of the arbitration process.

- A Party begins an arbitration by filing with the Director, at an office of NAF, or electronically, a properly completed copy of the Initial Claim Documents described in Rule 12 of the *Code of Procedure*, accompanied by the appropriate filing fee (see pages 42-43 of the *Code of Procedure*). The *Code of Procedure* must also be applied fairly and without prejudice to either of the parties involved in a dispute.
- NAF reviews the documents, administratively opens a file, assigns a file number, and notifies the Claimant.
- The Claimant then serves the Respondent in accord with Rule 6 of the *Code of Procedure*.
- A Respondent may file a Response as explained in Rule 13 of the *Code of Procedure*.
- There is no fee for filing a Response, unless the Response includes a Counter Claim.
- If there is no Response, the arbitration proceeds in accord with Rule 36 of the *Code of Procedure*.
- A Party may Request a Document Hearing or a Participatory Hearing and pay the fee listed in the Fee Schedule.
- The Arbitrator schedules an arbitration hearing after an Arbitrator is selected.
- The Arbitrator conducts the hearing and promptly issues an Award.

7 For a complete copy of the NAF *Code of Procedure*, visit the National Arbitration's Web site – www.arb-forum.com, or you may download the document from the AICPA Web site at www.aicpa.org/webtrust/index.htm.

Frequently Asked Questions

1. Q: How do I file a complaint?
   A: Complaints may be initiated online, over the telephone, or through the postal service.
   .

2. Q: How much does it cost?
   A: The cost is US$49 dollars for claims less than US$1,000. The cost for claims greater than US$1,000 up to US$15,000 range between US$49 and US$150.

3. Q. How long does the process take?
   A: Typically, most disputes are resolved in 45-60 days.

4. Q: If I am not happy with the decision, may I still go to court?
   A: You always have the right to go to court.

5. Q: Who pays for the proceedings?
   A: The losing party pays.

6. Q: Will my case be confidential?
   A: Yes, arbitration proceedings are completely private.

7. Q: Who makes the decision?
   A: A neutral and impartial legal expert who will render a decision based solely on the law.

8. Q: Is there a limitation on the award?
   A: Arbitrators may award all remedies allowed by law up to the amount of the claim.

9. Q: If after the decision is made, the other party refuses to abide by the decision what can I do?
   A: You may take the arbitration decision to court approximately ten days later, and the court will turn the decision into a judgment. Then the decision becomes enforceable.

10. Q: If I need to go to court, where is the hearing held?
    A: The company's arbitration clause will state where the hearing is to be held, (often the parties will agree to the location). For consumers in the United States, the courts cannot force the consumer to travel. With respect to a business, WebTrust arbitration rules provide that arbitration will take place where the defendant does business. If a consumer and business are involved in a dispute, the hearing will typically occur where the consumer resides.

11. Q: Can I have legal representation at an arbitration hearing?
    A: Yes, an attorney or other qualified individual may represent you at an arbitration hearing.

12. Q: Why was the NAF chosen?

A: NAF was chosen because of their expertise in addressing consumer complaints as well as their ability to process claims online at a reasonable cost.

13. Q: We already have a consumer recourse and arbitration process at our site, do we need to change arbitration organizations?
A: No, however, in order to ensure a consistent application of the WebTrust Principles and Criteria the arbitration organization must use the arbitration principles developed for WebTrust.

14. Q: My company currently has a dispute resolution process that covers the privacy policy at our site. Do we need any additional process to assure compliance with WebTrust?
A. Yes. If the current process only covers your privacy policy you will need to put a process in place that will cover all aspects of a transaction at your site. You may use your current arbitrator or may use another arbitration association, but in all cases the arbitrator must apply the Principles of Arbitration developed specifically for WebTrust.

15. Q: Where can I learn more about the NAF and its *Code of Procedure*?
A: You may down load NAF's *Code of Procedure* from the AICPA Web site or you may visit their site at www.arb-forum.com for more information.

Addendum 2 – Non-NAF

For example in Canada, an electronic commerce merchant is not obliged to choose NAF or its Canadian affiliate as its third-party arbitrator for the purposes of WebTrust.

Any third-party arbitrator must, however, agree to follow the twelve principles listed in this Appendix. In considering whether a selected arbitration organization can meet these principles, the entity should refer to NAF's *Code of Procedure* to gain a full understanding of the intent of the principles.

APPENDIX D - PRACTITIONER POLICIES AND GUIDANCE FOR WEBTRUST PRIVACY ENGAGEMENTS

Introduction

This section includes Practitioner Policies (as defined in the WebTrust Business License, Appendix A, "Defined Terms," "Policies Statement"), which set forth practices that practitioners must follow when conducting a WebTrust engagement. These policies are in *italic* typeface. This section also includes additional practitioner guidance on implementing these policies. This guidance is in non-italicized typeface.

Client/Engagement Acceptance

The practitioner should not accept an engagement where the awarding of a WebTrust Seal would be misleading.

The WebTrust Seal implies that the entity is a reputable site that has reasonable disclosures and controls in a broad range of areas, including privacy. Accordingly, the practitioner would avoid accepting a WebTrust engagement in which the entity's disclosures outside the scope of the engagement are known by the practitioner to be misleading, there are known major problems with controls not directly affecting privacy, or the entity is a known violator of laws or regulations.

Procedures to provide WebTrust services resulting in the awarding of a WebTrust Seal should be performed at a high level of assurance (i.e., audit or examination level).

Although a practitioner can provide a variety of services related to WebTrust, such as a preliminary review of a Web site to identify potential areas of nonconformity with the WebTrust Criteria, any engagement leading to a WebTrust Seal would need to include procedures to provide a high level of assurance (i.e., audit or examination level) as a basis for an unqualified opinion.

Initial Period of Coverage

Typically, an initial report would need to cover a period of two months or more. However, an initial report covering a period of less than two months (including a point-in-time) report can be issued in certain circumstances by a practitioner:

a. *When an entity begins the WebTrust program, or*

b. *When an entity wishes to restore the WebTrust Seal following a significant event that caused the entity to no longer comply with the criteria (that necessitated removal of the auditor's report and the WebTrust Seal from the entity's site).*

In determining the initial period of coverage, the practitioner would consider what length of period would be required to obtain sufficient competent evidential matter as a basis for his or her opinion.

Frequency of Updates

The interval between updates for the WebTrust Privacy Program should not exceed six months and this interval often may be considerably shorter.

In determining the interval between updates, the practitioner would consider the following—

a. The nature and complexity of the entity's operation.
b. The nature and frequency of significant changes to privacy disclosures, policies and related privacy and security controls.
c. The relative effectiveness of the entity's monitoring and change management controls for ensuring continued conformity with the applicable WebTrust Criteria included in the scope of the engagement as such changes are made.

During the period between updates, the entity is responsible for notifying the practitioner of: (1) any significant changes that are made to the privacy policies and/or related privacy and security controls from those that were in place at the time of the last WebTrust engagement, (2) of any failure to comply with its disclosed privacy practices, and (3) of any failure in the effectiveness of such controls. If the practitioner is notified of such circumstances, the practitioner should determine whether these have an effect on the entity's conformity with those WebTrust Criteria included in the scope of the engagement and whether one or more of the following is called for—

a. An update examination would need to be performed.
b. The seal would need to be removed until an update examination is completed and an updated auditor's report is issued.
c. No action is required at that time because of the nature of the change and/or the effectiveness of the entity's monitoring and change management controls.

Management Assertions

Management should provide an appropriate written assertion on its Web site.

Management's assertion would ordinarily identify the Web site covered and the period covered (which ordinarily would be same as that covered by the practitioner's report), and include a statement along the following lines, for example, for privacy—

During the period covered by the examination, the entity, in all material respects—

- Disclosed its privacy practices for electronic commerce,
- Complied with such privacy practices,
- Maintained effective controls to provide reasonable assurance that personally identifiable customer information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices

based on the AICPA/CICA WebTrust Privacy Criteria.

Changes in Client Privacy Policies and Disclosures

Changes in an entity's disclosed privacy policies need to be disclosed on its Web site in accordance with WebTrust Privacy Criterion A.7. If the client appropriately discloses such changes, no mention of such change needs to be made in the practitioner's report. If the client does not make such changes, the practitioner is precluded from issuing an unqualified report.

Sufficient Criteria for Unqualified Opinion

*In order to obtain an unqualified opinion, the entity should meet, in all material respects, **all** of the applicable WebTrust Criteria included in the scope of the engagement during the period covered by the report and each update period.*

Subsequent Events

The practitioner should consider the effect of subsequent events up to the date of the practitioner's report. If the practitioner becomes aware of events that materially affect the subject matter (for example, the entity's privacy disclosures, privacy practices, and privacy and related security controls), and the practitioner's conclusion, the practitioner should consider whether the disclosed privacy policies reflect those events properly or whether those events are addressed properly in the practitioner's report.

Representation Letter

Prior to conclusion of the engagement and before the practitioner issues a report, the client will be required to provide to the practitioner a Representation Letter.

This Letter might include the following representations—

- Company's privacy practices are followed consistently and as disclosed to the auditor.
- There have been no changes in the company's privacy practices during the period of review, or since the last review.
- There are no violations or possible violations of laws or regulations whose effects should be considered as to their effect on the transaction of e-commerce.
- The company has complied with all contractual agreements that would have a material effect on the transaction of e-commerce.
- There have been no breeches to the security of the Web site.
- Management subscribes to and follows the WebTrust Principle(s).
- Management represents that the privacy practices disclosures for www.abc.com are current, accurate, complete and have been on our Web site since July 1, 200X.
- Management has disclosed to you all organizations to whom we sell our customer database information.

- The company agrees to—
  - Permit you to conduct subsequent examinations at such times as you may deem appropriate, but not to exceed three months from the date of this report.
  - Maintain e-commerce controls, practices and disclosures.
  - Notify you regarding changes affecting our e-commerce activities, including the following—
    - Changes to our e-commerce controls, practices and disclosures or the manner in which they achieve the WebTrust Electronic Commerce Principles.
    - Changes in the nature of the products, information or services we offer through e-commerce.
    - Changes in the system(s) we use to support e-commerce.
  - Permit you to unilaterally remove the WebTrust Seal if—
    - You find that changes, such as those above, have been made but not communicated to you by us.
    - A subsequent examination has not been made within [specified number] days for any reason.
    - During the course of performing the engagement, you discover that changes we have made result in practices which no longer meet the WebTrust Principles and Criteria.
- Management has advised you of all actions taken at meetings of stockholders, board of directors, and committees of the board of directors (or other similar bodies, as applicable) that may affect our transacting business electronically.
- Management has responded fully to all inquiries made to us by you during your examination.

Report

Some practitioners have followed the practice of covering a cumulative reporting period with each update report. For example, if the practitioner's initial report covered the period from January 1 to March 31, the next update report would cover January 1 to June 30, and so on. This approach can be continued under the WebTrust Privacy Program, but any cumulative period should begin with the starting date of the period in the first report issued under this version of the WebTrust Privacy Program.

Practitioners that have previously issued reports with cumulative reporting periods (under WebTrust Principles and Criteria Version 2.0 and prior) will need to restart such a cumulative period as indicated above.