2000

WebTrust Program for On-Line Privacy, Version 3.0, August 15, 2000; Exposure draft (American Institute of Certified Public Accountants), 2000, August 15

American Institute of Certified Public Accountants (AICPA)

Canadian Institute of Chartered Accountants

The CPA. Never Underestimate The Value.℠

Chartered Accountants of Canada

Comptables agréés du Canada

Exposure Draft

AICPA/CICA

WebTrust SM/TM Program for On-Line Privacy

August 15, 2000

Version 3.0

Comments on this exposure draft should be sent to Sheryl Martin, WebTrust Team Leader, Assurance Services, AICPA, 1211 Avenue of the Americas, New York, NY 10036-8775 or Bryan Walker, Canadian Institute of Chartered Accountants, 277 Wellington Street West, Toronto, Canada M5V 3H2 in time to be received by September 30, 2000. Responses also may be sent by electronic mail via the Internet to sweiner@aicpa.org or bryan.walker@cica.ca.

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 (see Appendix E).

COMMITTEE AND TASK FORCE MEMBERS

AICPA
Assurance Services Executive Committee

Robert L. Bunting, Chair

Gari Fails

Ted Horne

Everett C. Johnson, Jr.

John Lainhart

George Lewis

Edward F. Rockman

Susan C. Rucker

J. W. Mike Starr

Wendy E. Visconty

Darwin Voltin

Neal West

Staff Contact:

Alan Anderson,
Senior Vice President, Technical Services

Anthony J. Pugliese,
Director of Assurance Services

CICA
Assurance Services Development Board

John W. Beech, Chair

Douglas C. Isaac

Marilyn Kuntz

Doug McPhie

Steven E. Salterio

David W. Stephen

Doug Timmins

Keith S. Vance

Staff Contacts:

Cairine M. Wilson,
Vice President, Innovation

Gregory P. Shields
Director
Assurance Services 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, referred to as the WebTrust℠ Privacy Program, and the related WebTrust 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 exposure draft of the WebTrust Privacy Program, 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 (update coming soon)
   - Business Practices and Transaction Integrity (update coming soon)
   - Availability (update coming soon)
   - Confidentiality NEW
   - Non-Repudiation NEW
   - Customized Disclosures NEW
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 (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 service providers (e.g., Application Service Providers) in addition to Internet Service Providers.

The new modules will be 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 Principles and Criteria has been approved for exposure by the AICPA Assurance Services Executive Committee and the CICA Assurance Services Development Board. Early adoption guidelines are set out in Appendix E.

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 individuals and its subsequent exchange with other entities. Some consumers like this as it allows for 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 and dissemination of personally identifiable information. Personally identifiable 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 personally identifiable information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or sexual preferences.

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 provided to others 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 impact the consumer.

It is important for consumers to have confidence that they have reached a Web site that takes appropriate steps to protect personally identifiable 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, personally identifiable 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) 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 personally identifiable information is disclosed to third parties. For sensitive information, the entity should provide an explicit (opt in) choice if information is to be disclosed to a third party or for a purpose other then those 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 personally identifiable 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, updates 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 market place may find that without adequate privacy standards and disclosures at their site they may be prohibited or restricted in the manner in which they are able to do business.

Consumers from other areas in the world are also concerned about how their information will be used, how it is protected, what process is in place that will allow them to correct erroneous information, and who will have access to this information. Without proper 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

Due to the unique nature of e-commerce, website customers are concerned about how their complaints are addressed. If a website 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. For companies that currently have a dispute resolution mechanism covering their e-commerce processes (or the privacy aspects thereof), those companies would continue to use their current mechanism. All such mechanisms should conform to the Principles of Arbitration in Appendix C, 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 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) and demonstrated through the display of a secured WebTrust Seal.

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

- Disclosed its privacy practices for e-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 is protected in conformity with its disclosed privacy practices

based on the WebTrust Privacy Criteria.

See Appendix A, for "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 CPA AND THE CA AS ASSURANCE PROFESSIONALS

CPAs and CAs 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 CPA or CA 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. CPAs and CAs 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 CPA or CA. CPAs and CAs 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 CPA or CA 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 along the following lines:

> ABC Company, on its Web site for e-commerce (at WWW.ABC.COM), during the period Xxxx xx, 200x through Yyyy yy, 200x:
> - Disclosed its privacy practices for e-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 is protected in conformity with its disclosed privacy practices
>
> based on the AICPA/CICA WebTrust Privacy Criteria.

For an initial representation, the historical period covered should be at least two months, or more, as determined by the practitioner. 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[1] 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 US, and the Criteria of Control (CoCo) in Canada. However, 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 electronic 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.

An independent, objective and knowledgeable practitioner will perform tests of these representations under AICPA or CICA professional standards[2] and provide a professional opinion, which adds to the credibility of management's representations.

---

[1] 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 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).

[2] 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.

Scope of Work

WebTrust Privacy focuses on private and/or sensitive customer information obtained as a result of electronic 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.

If the entity passes personally identifiable information on to third parties, it needs to consider whether the privacy practices and controls of such third parties provide appropriate protection for such information in conformity with the entity's disclosed privacy practices. Likewise, the practitioner also needs to consider the privacy practices and controls of such third parties.

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 CPA or CA 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.

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:
   a) The nature and complexity of the entity's operation.
   b) The frequency of significant changes to its 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 WebTrust Privacy Criteria as such changes are made.
   d) The practitioner's professional judgment.

   For example, an update will be required more frequently for a financial institution's fast-changing Web site for securities transactions than for an on-line 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.
2. During the period between updates, the entity should undertake to inform the practitioner of 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 the manner in which they are met. 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 updated auditor's report is issued.

The Seal Management Process

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

- Upon becoming a WebTrust Licensee, the WebTrust practitioner obtains a registration number (ID and password) from the WebTrust licensing authority. With this the practitioner can issue a WebTrust Seal to the entity.
- When the practitioner is prepared to issue a WebTrust Seal, the practitioner accesses the WebTrust secure server system. Upon payment of the registration fee, the practitioner receives passwords and IDs unique to the engagement. The Seal Manager would issue these to the practitioner in pairs. One set would allow the practitioner to read and write to the secure server (see below) and the other would permit the entity to preview the presentation.
- The practitioner would prepare a draft of the practitioner's report and provide it along with management's assertions for posting to the preview site.
- The Seal Manager will then deliver the Seal to the entity with the appropriate links to the preview site. Notification of delivery is provided to the practitioner.
- When the practitioner and entity have agreed that the Seal should become active, the practitioner notifies the seal manager to transfer the information from the preview site to the active WebTrust site and provides the appropriate expiration date.
- 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 engagement and other open items. (For example, if the seal expires on June 30, xxxx, the practitioner has 30 days to complete open items and prepare new documents for posting with the Seal Manager. The subsequent 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 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 30 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 provides links to the appropriate Principle(s), the practitioner's report 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 combination of the WebTrust Principles, the list will also identify the specific Principles for which a WebTrust Seal has been issued.

WEBTRUST PRIVACY PRINCIPLE AND CRITERIA[3]

Although e-commerce can be conducted through a number of means, including electronic bulletin boards and formalized EDI arrangements, all of which can impact 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 non-technical in nature.

The WebTrust Privacy Principle[4]

> *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 personally identifiable information. Additionally, the entity should also disclose management's agreeing 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 four broad areas – 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.

---

[3] 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).

[4] The WebTrust Principles meet or exceed 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.

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.

The entity must be able to demonstrate over a period of time (at least two months or more) 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.

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.	We will need certain information - such as name, Internet address or screen name, billing address, type of computer, 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 let you know of additional products and services from our company, and to send promotional material from some of our partners about which you might be interested. 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 gathered from you to any other third parties except as required by law.	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 let you know of additional products and services from our company, and to send promotional material from some of our partners about which you might be interested. 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
A.1.2	Choices regarding how personally identifiable information collected from an individual online may be used and/or distributed. Individuals should be 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.	
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 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 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 individually identifiable information collected can be reviewed and, if necessary, corrected or removed.	This site provides you with 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 (e.g., web bugs, 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, other than cookies, to analyze patterns and paths through this site.	
A.3	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.	
A.4	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 personally identifiable information be removed from the system after 3 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 5 years.
A.5	The entity discloses the process used to resolve disputes.	Transactions at this site 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 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 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-

Criteria	Illustrative Disclosures for Business to Consumer e-commerce	Illustrative Disclosures for Service Providers

xxx.

A.6	The entity discloses changes or updates to its practices.	During the period May 31 – August 31, 2xxx, we collected customer telephone numbers. From September 1 to the present time 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 allows the distribution of collected personally identifiable information to third parties. Since our previous policy did not allow for the distribution of such personally identifiable information, we will obtain your permission prior to the distribution of such information collected before September 30, xxxx.

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, goals and objectives regarding the protection of personally identifiable information consider 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 • Access by the customer to his or her private information for update and corrective purposes • Security of the customer's private information • Enforcement and consumer recourse policies regarding customer privacy.	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 under goes 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 are aware of and follow the entity's published privacy policy.	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.	
B.3	Accountability for the privacy policy has been assigned.	Management has assigned responsibility for enforcement of the company privacy policy to the CIO. Others on the executive committee assist in the review and update of the policy as outlined in the executive committee handbook.	Management has assigned responsibilities for the enforcement of the company privacy policy to the Chief Legal Officer. Others on the executive committee assist in the review and update of the policy as outlined in the executive committee handbook.
B.4	The entity provides for adequate security of the programs and data during the backup, offsite storage and restoration processes.	During the daily backup routine, the data is secured from both physical and logical access by unauthorized personnel. During any restoration process, no access is allowed by unauthorized personnel.	
B.5	Documented privacy objectives, policies, and standards are consistent with disclosed privacy requirements.	Management reviews it's 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 5 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. Security criteria that relate to privacy		
C.1.1 The entity has procedures to establish new users.	New users are given a secure session in which to provide new user information and select an appropriate user ID and password.	New users provide information in a secure (SSL) session. User IDs and passwords are provided to the user and must contain non-alphanumeric characters.
C.1.2 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 (UNIX and Windows NT) is provided via a strong identification and authentication mechanism (digital signature, one-time password, Secure-ID 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.
C.1.3 The entity has procedures in place to allow users to change, update or delete their own user information.	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 personally identifiable information or deletions must be processed in writing.
C.1.4 The entity has procedures to	Remote access is	The remote access to

Criteria	Illustrative Controls for Business to Consumer e-commerce	Illustrative Controls for Service Providers
limit remote access to the internal network to only authorized personnel.	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.	and use of the computing resources are restricted by the implementation of an authentication mechanism of identified users and resources associated with access rules. User IDs and passwords are stored in an encrypted database, with the associated encryption key stored off-line.
	Logical access control procedures (e.g., firewalls, routers, password controls) are maintained by the IT department. These controls are tested on a periodic basis by performing penetration testing from both within the internal network and from the internet.	
C.1.5 The entity has controls in place to prevent customers, groups of individuals, or other entities from accessing other than their own private or confidential information.	Customers are required to enter a user ID and password to access their personally identifiable information and orders. A challenge word or phrase (e.g., 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.	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.
	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.	

	Criteria	Illustrative Controls for Business to Consumer e-commerce	Illustrative Controls for Service Providers
C.1.6	The entity provides encryption capability for sensitive or private information that is passed across an unsecured electronic network.	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.1.7	Systems that retain private information obtained as a result of e-commerce are protected from unauthorized outside access.	Commercial firewalls are used. They are updated regularly and tested periodically for susceptibility to security weaknesses. All private information is processed and stored on servers protected with access control rules to prevent unauthorized access.	
	Privacy specific criteria		
C.2	Private information obtained as a result of e-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.	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.

	Criteria	Illustrative Controls for Business to Consumer e-commerce	Illustrative Controls for Service Providers
C.3	Private information obtained as a result of e-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.	
C.4	The entity maintains procedures so that individually identifiable information collected, created or maintained by it is accurate and complete for its intended use.	The company only accepts data from you 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.5	The entity maintains procedures to determine the adequacy of information protection and privacy policies of third parties to whom information is transferred.	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.6	Customer permission is obtained before storing, altering or copying information in the customer's computer or the customer is notified with an option to prevent such activities.	The entity requests the customer's permission before it intentionally stores, alters or copies information (such as cookies and other similar files) in the customer's computer. The entity requests the customer's permission before it performs any diagnostic or inventory on the customer's computer.	
C.7	In the event that a disclosed privacy policy is changed or deleted to be **less** restrictive, the entity maintains procedures to protect personally identifiable 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 personally identifiable 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/Performance Measures**		
D.1	The entity maintains procedures for monitoring the security of its e-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 – a real time monitor which is used to detect intruders; and SATAN -- this software is run monthly and provides a security analysis of	Commercial and other monitoring software (COPS, SATAN, 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.

	Criteria	Illustrative Controls for Business to Consumer e-commerce	Illustrative Controls for Service Providers
		the system. In addition the group maintains and analyzes the server logs.	
D.2	The entity has procedures in place to keep its disclosed privacy policy current with laws and regulations and to monitor adherence to its current privacy policy practices.	Staff meetings are held on a regular basis to address current privacy concerns and their findings are discussed at quarterly management meetings.	Legal Counsel for the entity reviews the policy on an annual basis to assess whether modifications are required. The entity is active in current public policy forums and monitors these forums for possible impact on its privacy policy.
D.3	The entity has procedures in place to test its security incident policy and update it as needed due to technology changes, changes in the structure of the e-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 in place to effectively monitor and follow up on 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 email and pager should any incident be in progress. If an incident occurs, a report is filed within 24 hours for follow up and analysis. Customers are directed to an area of the web site to post a message about security breaches or possible breaches as soon as they become concerned. These customer comments are followed up within 24 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 two illustrative reports for WebTrust Privacy Program engagements. Illustration No. 1 is prepared in accordance with the AICPA's attestation standards. Illustration No. 2 is prepared in accordance with the CICA's assurance standards.

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.

Under the U. S. *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.

Illustration No. 1 for Use in the United States

Independent Auditor's Report

To The Management of ABC Company, Inc.:

We have examined management's assertion [hot link to management's assertion] regarding ABC Company, Inc.'s (ABC) disclosed privacy practices for e-commerce transactions, compliance with such privacy practices and the effectiveness of its controls over privacy for e-commerce during the period XXX, 2000 through YYY, 2000, based on the AICPA/CICA WebTrust Criteria [hot link to privacy principle and criteria].

These e-commerce disclosures 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 e-commerce disclosed privacy practices and its controls over privacy for e-commerce, (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, during the period Xxxx xx, 2000 through Yyyy yy, 2000, ABC Company, in all material respects:

- Disclosed its privacy practices for e-commerce transactions
- 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

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's Web site for e-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 Canada

Direct Report Based on CICA Standards
Unqualified Opinion

Auditor's Report

To The Management of ABC Company, Inc.:

We have audited ABC Company's disclosure of its privacy practices, and compliance with these practices, for e-commerce transactions and the effectiveness of its controls over privacy for e-commerce (at WWW.ABC.COM) during the period Xxxx xx, 2000 through Yyyy yy, 2000. These e-commerce disclosures, practices and controls are the responsibility of ABC Company's management. Our responsibility is to express an opinion on the conformity of those disclosures, practices and controls with the AICPA/CICA *WebTrust* Privacy Criteria [hot link to privacy principle and criteria], based on our audit.

We conducted our audit 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 e-commerce disclosed privacy practices and its controls over privacy for e-commerce, (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, during the period Xxxx xx, 2000 through Yyyy yy, 2000, ABC Company, in all material respects:

- Disclosed its privacy practices for e-commerce transactions
- 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

in accordance with AICPA/CICA *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 e-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 CA firm*] [*City, Province*]
Chartered Accountants

APPENDIX B – WEBTRUST SM/TM PRIVACY SELF-ASSESSMENT QUESTIONNAIRE

[To be completed during the exposure period]

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 website.

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 is organization based in the United States that 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:

1. **FUNDAMENTALLY FAIR PROCESS** — All parties in an arbitration process 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.

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 has established an effective arbitration and mediation process. While 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 and suggested that the organization apply the NAF Code of Procedure[5] as well.

This section provides additional information about the arbitration process as followed by The National Arbitration Forum.

NAF has a simple and cost effective method of filing a complaint. Complaints can be initiated on-line, 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 pp. 42-43 of the *Code of Procedure*). This "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.

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

Frequently Asked Questions:

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

2. Q: How much does it cost?
   A: The cost is $49 dollars (USD) for claims <$1,000. The cost for claims >$1,000-$15,000 (USD) range between $49- $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 10 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 U.S., the courts can not 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 dealing with 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 12 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 website or you may visit the Forum's site at www.arb-forum.com for more information.

Addendum 2 – Non NAF

For example in Canada, an e-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 Appendix C. 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. The guidance is in normal 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 where the entity's disclosures outside the scope of the engagement are known by the practitioner to be misleading, where there are known major problems with controls not directly affecting privacy, or where 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 non-conformity 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

The period of coverage for an initial WebTrust engagement should be at least two months or more as determined by the practitioner.

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:

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 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. If the practitioner is notified of such changes, the practitioner should determine whether these changes have an affect on the WebTrust Criteria included in the scope of the engagement and whether:

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, or
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, 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:

- Disclosed its privacy practices for e-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 is 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.6. If the client appropriately discloses such changes, no mention of such change needs to be made in the practitioner's 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 report.*

Seal Requirements

- Privacy Designation
- Link to Secure Site, etc.
- Firm Name Optional

TO BE ADDED DURING EXPOSURE PERIOD

Subsequent Events

The practitioner should consider the effect of subsequent events up to the date of the practitioner's report. When the practitioner becomes aware of events that materially affect the subject matter (e.g., 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 electronic commerce.
- The company has complied with all contractual agreements that would have a material effect on the transaction of electronic commerce.
- There have been no breeches to the security of the website.
- 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 website since July 1, 200X.
- Management has disclosed to you all organizations to whom we sell our customer data base 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 electronic commerce controls, practices and disclosures
- Notify you regarding changes affecting our electronic commerce activities, including:
  - Changes to our electronic commerce controls, practices and disclosures or the manner in which they achieve the *WebTrust* Electronic Commerce Principles
  - Changes in the nature of the products, information or services we offer through electronic commerce
  - Changes in the system(s) we use to support electronic commerce

  - To permit you to unilaterally remove the *WebTrust* Seal if:
    - You find that changes, such as those above, have been made but not communicated to you by us
    - A subsequent examination has not been made within ____ days for any reason
    - During the course of performing the engagement you discover that changes we have made result in practices 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 1st to March 31st, the next update report would cover January 1st to June 30th, etc. 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.

APPENDIX E- EARLY IMPLEMENTATION

Early implementation for privacy assurance using the draft WebTrust Privacy Program is allowed. If a client wants a WebTrust examination, the practitioner needs to address the following issues:

- Status of draft Principle and Criteria;
- Reporting considerations;
- Issuing a WebTrust seal;
- Situations where significant changes are made to the draft principles.

Status of Draft Principle and Criteria

The WebTrust Privacy Principle and Criteria contained in this document have been issued for exposure on August 15, 2000 for a 45-day comment period. During this comment period and until final approval and issuance by the AICPA and CICA, the Task Force believes that the draft WebTrust Privacy Criteria are suitable for a WebTrust Privacy engagement that could result in the issuance of a WebTrust Privacy Seal.

Reporting Considerations

Due to the current draft status of the WebTrust Privacy Criteria, any report issued using such stated criteria should include presentation of the criteria along with the practitioner's report. A hyperlink from the electronic version of the Auditor's Report to the exposure draft should be made. Since the Principle and Criteria have not yet been established through AICPA/CICA approval, a written copy of the draft principle and criteria may need to be attached to any paper version of the Auditor's Report.

Until the principle and criteria is approved, management should modify its assertion and the auditor should modify the audit opinion to state that the entity:

- "Disclosed its privacy practices for e-commerce transactions
- Complied with such privacy practices
- Maintained 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

based on the accompanying draft of the AICPA/CICA WebTrust Privacy Criteria."

Issuing A WebTrust Privacy Seal

Since it will be permissible to issue a WebTrust seal on this draft version of WebTrust Privacy Principles and Criteria, a client may have a WebTrust Privacy seal displayed on its site prior to the draft WebTrust Privacy Program being approved by AICPA and CICA.

Significant Changes to Principle and Criteria

There is a possibility that significant changes could be made to this draft of the WebTrust Privacy Principle and Criteria as a result of comments received during the exposure process. For clients who have been audited under the a draft of the WebTrust Principle(s) and Criteria, the changes may impact in one of the two following ways:

- For clients who have completed engagements and have a WebTrust seal on its site – they will be allowed a grace period (not to exceed six months), during which they can continue to display the seal and the related Auditor's Report and other information. The update examination will be undertaken using the final WebTrust Principle and Criteria.
- In situations where the examination commenced using the draft Principle and Criteria, but the Principle and Criteria are approved prior to the release of the Auditor's Report, the auditor will need to issue the Auditor's Report using the approved Principle and Criteria as the benchmark for the examination. In order to do so, the auditor will need to assess the impact of any changes in the final Principle and Criteria on the client before such issuance.