1999

WebTrust principles and criteria for business-to-consumer electronic commerce, Version 2.0, October 15, 1999

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

AICPA/CICA

WebTrust SM/TM Principles and Criteria

for

Business-to-Consumer Electronic Commerce

October 15, 1999

Version 2.0

These Principles and Criteria are effective for examination periods beginning after December 31, 1999 for all new and existing seals. Earlier adoption is encouraged.

COMMITTEE AND TASK FORCE MEMBERS

AICPA
Assurance Services Executive Committee

Robert L. Bunting, Chair

Ronald S. Cohen

Louis Grabowski

Everett C. Johnson, Jr.

George Lewis

Alfonse M. Mattia

Don Pallais

Edward F. Rockman

Susan C. Rucker

Albert E. Trexler

Gordon A. Viere

Wendy E. Visconty

Darwin Voltin

William E. Zimmerman

Staff Contact:
Anthony J. Pugliese,
Director of Assurance Services

CICA
Assurance Services Development Board

John W. Beech, Chair

Kenneth W. Chase

Mark C. Davies

Richard Flageole

Douglas C. Isaac

Ivan Lavine

Manon Leclair

Joanne R. Rogers

Steven E. Salterio

David W. Stephen

Staff Contacts:
Karen Duggan,
Principal, Assurance Standards

Bryan Walker
Principal, Research Studies

AICPA / CICA Electronic Commerce
Assurance Services Task Force

Everett C. Johnson, Jr., Chair

Yogen Appalraju

Bruce R. Barrick

Joseph G. Griffin

David Holyoak

Christopher J. Leach

Patrick J. Moriarty

Walter Primoff

Gary W. Riske

Kerry L. Shackelford

Donald E. Sheehy

Christian R. Stormer

Staff Contacts:
Bryan Walker, CICA
Principal, Research Studies

Sheryl Weiner, AICPA
WebTrust Team Leader

CONTENTS

	Page
Introduction	**5**
Background	**6**
What Is E-commerce?	6
What Are the Risks in E-commerce?	7
Consumer Recourse	9
The WebTrust Seal of Assurance	**9**
The CPA and the CA as Assurance Professionals	**9**
Obtaining and Keeping the WebTrust Seal Of Assurance	**10**
The Assurance Process	10
Obtaining the Seal	11
Keeping the Seal	11
The Seal Management Process	12
Seal Authentication	12
WebTrust Principles and Criteria	**14**
The WebTrust Principles	14
The WebTrust Criteria	15
Appendix A —Examples of Practitioner Reports	**47**
Appendix B - WebTrust SM/TM Self-Assessment Questionnaire (Version 2.0)	**50**
Appendix C - Consumer Arbitration	**63**
Addendum 1 – United States	65
Addendum 2 – Canada	68

INTRODUCTION

The Internet provides consumers with a new means for obtaining useful information and for purchasing goods 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 this set of principles and criteria for business-to-consumer e-commerce, referred to as the WebTrust℠ Principles and Criteria, and the related WebTrust Seal of assurance, also referred to as CPA WebTrust℠ and CA 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 these principles and criteria. 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 Version 2.0 of the WebTrust Principles and Criteria. Its focus is business-to-consumer e-commerce transactions. The principal changes to Version 1.1 (June of 1999) of the WebTrust Principles and Criteria include, but are not limited to, the following:

1. Expansion of the Business Practices Disclosures Principle to include new disclosures related to an on-line business's information privacy practices. These new disclosures include such items as the specific kinds of information being collected by an on-line business and the use and distribution of that information. Additional criteria require that an on-line business disclose to the consumer his or her choices regarding how information collected may be used or distributed and requires that a consumer be given the option to opt out of transactions that use information in a way they do not want.

2. Expansion of the Business Practices Disclosure Principle to include information on how to resolve complaints. These complaints may relate to any part of a customer's e-commerce transaction, including complaints related to the quality of services and products, accuracy, completeness, and distribution of private customer information[1] and the consequences for failure to resolve such complaints. Version 2.0 requires that this resolution process include management's commitment to use a third-party dispute resolution service whose procedures meet WebTrust dispute resolution standards in the event a consumer is not satisfied with an on-line business's resolution of such a complaint. A third-party dispute resolution service

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

would be used unless there is a program mandated by a regulatory body.

3. Expansion of the Information Protection Principle to require that an on-line business maintains controls over the collection of data and provides consumers with a choice as to how information collected from them on-line will be used and provides the option to opt out of any undesired use of that information.

4. Expansion of the Information Protection Principle to require that an on-line business maintain controls to ensure that information collected from consumers is accurate and complete for its intended use and that consumers can review and arrange for the correction of any incorrect data maintained by the on-line business.

5. Expands the Information Protection Principle to require that an on-line business maintain controls to determine the integrity and security policies of third parties to which information is transferred.

We anticipate that future revisions will be needed to update these criteria and related materials. Additional principles and criteria also may be developed to expand the focus to include business-to-business transactions and other aspects of e-commerce.

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 by the AICPA Assurance Services Executive Committee and the CICA Assurance Services Development Board.

The public accounting profession has developed a set of WebTrust Principles and Criteria and the related WebTrust Seal of assurance to assist entities and their customers in assessing the risks of doing business electronically. This document explains e-commerce, the risks that are addressed by the e-commerce principles and criteria, and the seal of assurance, and presents the principles and the related measurement criteria.

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 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.

What Are the Risks in E-commerce?

The following are broad areas of risk associated with e-commerce.

Business Practices and Information Privacy Practices

E-commerce often involves transactions between strangers. Appearances can be deceiving. How can a consumer know whether an entity that presents a well-constructed Web page will really fill its orders for goods and services as it claims? How can a consumer know whether the entity will allow the return of goods, or whether there are product warranties? How are customer complaints regarding the accuracy, completeness and distribution of private customer information resolved? The anonymity of e-commerce and the ease with which the unscrupulous can establish—and abandon—electronic identities make it crucial that people know that those entities with which they are doing business disclose and follow certain business practices. Without such useful information and the assurance that the entity has a history of following such practices, consumers could face an increased risk of loss, fraud, inconvenience, or unsatisfied expectations.

Information privacy can be a two-edged sword. One the one hand, merchants need certain information in order to process a customer order. On the other hand, the customer does not want this information provided to others without customer permission. 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.

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 at their site they may be prohibited or restricted in the manner in which they are able to do business.

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

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

Transaction Integrity

Without proper controls, electronic transactions and documents can be easily changed, lost, duplicated, and incorrectly processed. These attributes may cause the integrity of electronic transactions and

documents to be questioned, causing disputes regarding the terms of a transaction and the related billing. Potential participants in e-commerce may seek assurance that the entity has effective transaction integrity controls and a history of processing its transactions accurately, completely, and promptly, and billing its customers in accordance with agreed-upon terms.

Information Protection

It is important for consumers to have confidence that they have reached a properly identified Web site and that the entity takes appropriate steps to protect private customer 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 confidentiality 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, private customer 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. Security breaches may also include unauthorized access to corporate networks, Internet/Web servers, and even access to the consumer's Internet connection (for example, his or her home computer). Potential participants in e-commerce may seek assurance that the entity has effective information protection controls and a history of protecting private customer information.

The Year 2000 Issue

The Year 2000 Issue has attracted substantial publicity and all entities should be aware of it. Responses are varied, with some entities still doing little. The issue is simple to explain; it has arisen because computerized systems identify the year using two digits only, the digits *00* may be misinterpreted, for example, as 1900 or a special code or an error condition, potentially causing errors or operational failure of computerized systems. In addition, a number of computerized systems do not properly perform calculations with dates beginning in 1999, because these systems use the digits *99* in date fields to represent something other that the year 1999. It is also important to recognize that the 2000 is a leap year and not all systems recognize February 29, 2000, as a valid date. The Year 2000 Issue may manifest itself before, on, or after January 1, 2000, and its effects on financial reporting and operations may range from inconsequential errors to business failure.

It is the responsibility of an entity's management to assess and remediate the effects of the Year 2000 Issue on an entity's systems. This responsibility extends beyond systems that produce financial information. It encompasses all systems, including those that are part of the entity's operational activities, such as safety, environment, production, machine control, service, and security activities. Management also is responsible for considering the effect that other entities' noncompliant systems may have on its operations and financial information system. The board of directors (or others with equivalent responsibility) has a responsibility to oversee the activities of management to ensure that the Year 2000 Issue is receiving appropriate attention from management.

It is important to recognize that it is not and will not be possible for any entity to represent that it has achieved complete Year 2000 compliance and guarantee its remediation. The problem is simply too complex for such a claim to have legitimacy. Accordingly, no assurance regarding Year 2000 compliance is provided as part of the WebTrust service.

Consumer Recourse

Due to the unique nature of e-commerce, customers to a website 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 for some of their e-commerce processes, those companies would continue to use their current mechanism and must use other dispute resolution mechanisms to cover the entire e-commerce transaction. 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 transaction integrity, control, authorization, confidentiality, 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) or 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 the Web site's business practices and controls to determine whether they are in conformity with the WebTrust Principles and Criteria for Business-to-Consumer E-commerce, and has issued a report with an unqualified opinion indicating that such principles are being followed in conformity with the WebTrust Criteria. See Appendix A, "Examples of Practitioner Reports." These principles and criteria reflect fundamental standards for business practices, transaction integrity, and information protection.

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, 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 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, 199x through Yyyy yy, 2000—

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

in conformity with the AICPA/CICA WebTrust Criteria.

A self-assessment questionnaire has been provided as Appendix B, "WebTrust$^{SM/TM}$ Self-Assessment Questionnaire (Version 2.0) to assist the entity's management in forming a basis for its assertions.

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[2] for its e-commerce transactions. Helpful guidance on appropriate control

[2] Certain WebTrust clients 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 client. 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 nonauthoritative 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.)

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 processing e-commerce transactions. 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[3] and provide a professional opinion, which adds to the credibility of management's representations.

Obtaining the Seal

To obtain the WebTrust Seal of assurance, the entity must meet all the WebTrust Principles as measured by the WebTrust Criteria associated with each of these principles. 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 entity's assurance 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 Web site.
   c) The relative effectiveness of the entity's monitoring and change management controls for ensuring continued conformity with the WebTrust Criteria as such changes are made.

---

[3] 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.

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 three 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 undertakes to inform the practitioner of any significant changes in its business and information privacy policies, practices, processes, and controls particularly if such changes might affect the entity's ability to continue meeting the WebTrust Principles and 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 was completed and the updated auditor's report is issued.

The Seal Management Process

The WebTrust Seal of assurance will be managed using a trusted-third-party service organization (the seal manager) along the following lines.

- Upon receiving an unqualified report, the practitioner obtains an Enrollment Identification (EID) from the AICPA, CICA, or appropriate licensed association.
- The practitioner will provide to the entity an EID number used for registration at the Seal manager site.
- Using this EID, the entity will need to apply for and receive a special Class 3 Certificate (the WebTrust digital certificate) from the Seal manager.
- The Seal manager also will provide the materials needed to install the Seal and a special WebTrust-digital certificate to the entity.
- If, for an appropriate reason, the practitioner determines that the Seal should be removed from the entity's Web site, he or she will notify the entity and request that the Seal and the related practitioner's report be removed from the Web site. The practitioner also will send notification to the Seal manager that the Seal should be revoked. This will electronically revoke the digital certificate.
- Digital certificates expire one year after their date of issue; therefore the practitioner and the entity will need to renew the digital certificate annually.

Seal Authentication

To verify whether the seal displayed on a Web site is authentic, the customer can click on the seal and a graphic display, which looks like a certificate, will appear. This display will provide the customer with directions on how to view the special WebTrust digital certificate issued by the seal manager using the

browser. This digital certificate provides the customer with evidence that the WebTrust Seal is valid. The digital certificate will indicate (1) that it is an RSA certificate, (2) that it was issued as a result of a WebTrust examination, (3) who it was issued to, and (4) where the company awarded the seal is located. Without this digital certificate, the WebTrust Seal should *not* be considered valid. Also, VeriSign includes on its Web site (at www.verisign.com/webtrust/siteindex.html) a listing of all Web sites that have received the WebTrust Seal.

WEBTRUST PRINCIPLES AND CRITERIA[4]

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

The following principles have been developed with the consumer-user in mind and, as a result, are intended to be practical and somewhat nontechnical in nature.

The WebTrust Principles[5]

Business and Information Privacy Practices

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

To enhance customer confidence in e-commerce, it is important that the customer is informed about the entity's business practices for e-commerce transactions. The entity should properly disclose its business practices for dealing with such matters as orders and any subsequent returns and warranty claims. The entity should also follow its disclosed practices. This includes management's agreeing to third-party arbitration to settle customer complaints. The entity also needs to disclose its practices relating to the manner in which in uses, protects and maintains private customer information along with the site's consumer recourse provisions.

This principle relates to the e-commerce transaction processes that the entity uses and management's method for settling third-party complaints. However, it does not include any representation as to the quality of its goods or services or their suitability for any customer's intended purpose (as such matters are outside the scope of the WebTrust Principles and Criteria).

Transaction Integrity

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

These controls address matters such as: (1) transaction validation; (2) the accuracy, completeness, and

---

[4] 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).

[5] The WebTrust Principles meet or exceed the standards of the Online Privacy Alliance (OPA) and the European Union (EU) Privacy Directives as of October 1999.

timeliness of transaction processing and related billings; (3) the disclosure of terms and billing elements and, if applicable, electronic settlement; and (4) appropriate transaction identification. Such controls are essential in helping to establish consumer confidence in doing business electronically over the Internet.

Information Protection

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

These controls address privacy and security matters such as encryption or other protection of private customer information (such as credit card numbers and personal and financial information) transmitted to the entity over the Internet, protection of such information once it reaches the entity and requesting permission of customers to use their information for purposes other than those related to the entity's business, and for obtaining customer permission before storing, altering, or copying information on the customer's computer. In connection with safeguarding this information, consumers are concerned about being able to correct or update information provided to a site. The process by which a site allows this process to occur can greatly enhance its e-commerce activity. Consumer concern about the safeguarding of private information traditionally has been one of the most significant deterrents to undertaking e-commerce transactions.

The WebTrust Criteria

In order to provide more specific guidance, a number of 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.

A four-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 through fourth columns provide illustrative disclosures and controls for retail goods and other nonfinancial services, online banking and online securities trading, respectively. 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.

The entity must be able to demonstrate over a period of time (at least two months or more) that (1) it executed transactions in accordance with the business practices it discloses for e-commerce transactions, (2) its controls operated effectively, (3) it maintains a control environment that is conducive to reliable business practice disclosures and effective controls, and (4) it maintains monitoring procedures to ensure that such business practices remain current and such controls remain effective in conformity with the WebTrust Criteria. These concepts are an integral part of the WebTrust Criteria.

A. **Business and Information Privacy Practices**—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
A1	**Description of goods and/or services** The entity discloses descriptive information about the nature of the goods that will be shipped or the services that will be provided, including, but not limited to, the following:			
A1.1.	Condition of goods (meaning, whether they are new, used, or reconditioned).	• You can purchase new and used books on our site; used books are clearly labeled as such.		
A1.2.	Description of services (or service contract).		• Our Internet Services are as follows: – Twenty-four -hour access to your bank accounts. – Pay bills including heat, water, phone, cable TV, credit and department store cards, taxes, and gas. – Transfer funds between your accounts. – Check account balances on your bank accounts. – Keep track of the entries that have gone through	• ABC Trading Inc. provides various trading accounts, including cash accounts, margin accounts, options accounts, and short sell accounts. All pay interest so your money earns even when it is idle. • Our Internet Services are as follows: – U. S. and Canadian Equities – Buy or sell securities listed on the AMEX, NASDAQ, NYSE, TSE, ME, VSE, ASE. – Options Trading - Buy puts and calls or write (sell) covered puts and calls on any exchange in the

A. Business and Information Privacy Practices—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
			your accounts. – Make payments or draw down on your Credit Line. – Obtain balances and make payments on most loans.	United States or Canada. – Short Selling - Short selling involves us borrowing the stock on the investor's behalf to cover the short-sale initially. The short sale of securities involves high degree of risk and therefore may not be suitable for every investor.
			• You may access your checking account, savings account, money market accounts, and home equity line of credit through our on-line service.	– Foreign Equities - Trade in most foreign exchanges around the world, including: Hong Kong, Shanghai, Shenzhen, Jakarta, Thailand, Kuala Lumpur, London, Tokyo, Paris, Frankfurt, Geneva, Sydney, Johannesburg, Zurich, Singapore, Manila, and many more. – Mutual Funds - Over 1000 North American mutual funds are available. • You can view your investment account, send trade requests, see the status of your trades and the value of your portfolio twenty-four hours a day, every day.
A1.3.	Sources of information (meaning, where it was obtained and how it was	• This report was compiled by us based on scientific evidence from research done at ten universities,	• The Federal Reserve Bank provides prime lending rate information. Bond rating	• ABC Trading Inc. uses a computerized routing system to obtain pricing information. Orders

A. Business and Information Privacy Practices—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
	compiled).	which are listed in the report. An analysis prepared by our scientists also is included. Further reproduction or dissemination of all or portions of this report without our written permission is prohibited under copyright law.	information is provided by Standard and Poors.	are directed to the market based on price and liquidity.
A2	**Terms and Conditions** The entity discloses the terms and conditions by which it conducts its e-commerce transactions including but not limited to the following:			
A2.1.	Time frame for completion of transactions (transaction means fulfillment of orders where goods are being sold and delivery of service where a service is being provided).	• Our policy is to ship orders within one week of receipt of a customer-approved order. Our experience is that over 90% of our orders are shipped within 48 hours, the remainder is shipped within one week.	• A transfer of funds before 5PM (Pacific Time) on a business day is posted to your account the same day. All transfers completed after 5PM (Pacific Time) on a business day or on a Saturday, Sunday or banking holiday will be posted on the next business day.	• Market orders placed when the markets are open are typically executed and confirmed in a matter of seconds. For limit orders placed during market hours, our Best Market Determination Module will determine where the order gets placed. If the market is closed, your order is transmitted to the exchange before the start of the next trading day. • The real-time status of your order is

A. **Business and Information Privacy Practices**—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
				provided on our Web site. In addition, if you have provided us with your email address, you can choose to be notified by email when your order is filled. You will also receive written confirmation of the trade in the mail. • We process your order with the same efficiency as an institutional order, with all the trade execution resources of ABC Trading Inc. • You can enter an order at any time, seven days a week, twenty-four hours a day, on our Web site or through our automated telephone system. If the market is closed when you place your order, it will be reflected at market open on the next trading day. • You will be notified within five (5) business days prior to expiration of your sell order.
A2.2.	Time frame and process for informing customers of exceptions to normal processing of orders or service requests	• We will notify you by email within twenty-four hours if we cannot fulfill your order as specified at the time you placed it and will provide you the option	• In the unlikely event we are unable to process your transaction, we will notify you within one hour by email and/or telephone.	• The current status of your order is provided on our Web site. In addition, if you have provided us with your email address, you can choose to be notified by email when

A. **Business and Information Privacy Practices**—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
		of canceling the order without further obligation. You will not be billed until the order is shipped.		your order is filled. If, for whatever reason, your order cannot be fulfilled, the status of your order will show an error (Status="ERR") and notify you immediately by email if you have provided us with your email address.
A2.3.	Normal method of delivery of goods or services, including customer options, where applicable.	• You have the option of downloading the requested information now or we will send it to you on CD-ROM by UPS 2-day or Federal Express overnight delivery.	• In order to sign-in and perform on-line financial transactions, you should use a browser that supports 128 bit encryption.	• In order to sign-in and perform on-line financial transactions, you should use a browser that supports 128 bit encryption.
A2.4.	Payment terms, including customer options, if any.	• Your credit card will be charged at the time of shipment or you can send us a check or money order.	• All bill payments will be withdrawn from the account on the day the payment is scheduled to be sent to the payee whether these payments are made electronically or by check.	• To open an account at ABC Trading, Inc., a minimum of $500 equity is required. This initial deposit can be made with your personal check, securities, or any combination of the two. All subsequent equity transferred into your account can be made by a check payment, electronic transfer of funds from your banking account, or by transferring your assets from another broker.
A2.5.	Electronic settlement practices and related	• Your bank account will be charged $12.95 monthly for our	• Your account will be immediately debited $30 for	• All stock transactions are settled three days after the trade and option

A. Business and Information Privacy Practices—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
	charges to customers.	service fee.	each stop payment order requested.	trades are settled one day after the trade. You will be charged a commission of $20 per trade regardless of the size of your transaction.
A2.6.	How customers may cancel recurring charges, if any.	• To cancel your monthly service fee, send us an e-mail at Subscriber@ABC.COM or call us at 800-555-1212. Be sure to include your account number.	• We will charge you monthly fee of $5 once you sign-up for online banking. Contact our Customer Service Department at any time should you want to cancel online banking services.	• There are no monthly or recurring fees associated with your account.
A2.7.	Product return policies and/or limited liability, where applicable.	• Purchases can be returned for a full refund within thirty days of receipt of shipment. Call our 800 number or email us for a Return Authorization Number, which should be written clearly on the outside of the return package.	• If your online password has been compromised and you tell us within two business days after you learn of the loss or theft, your losses are limited to $100 if someone used your online password without your permission. If you do not tell us within two business days after you learn of the loss or theft your losses are limited to $1,000. • If your statement shows withdrawals, transfers, or purchases that you did not	• The Securities Investors Protection Corporation (SIPC) currently protects the assets in each account up to $500,000, of which no more than $100,000, may be in cash. This protection does not cover fluctuations in the market value of your investments.

A. **Business and Information Privacy Practices**—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
		• Transactions that occur at this site are in accordance with the laws and business practices of Alberta, Canada	authorize and you do not notify us within sixty days after the online statement was sent to you, you may not recover any money lost after the sixty-day period. • Transactions that occur at this site are in accordance with the laws and business practices of Canada, for example, Office of the Superintendent of Financial Institutions (OSFI) and the Canadian Payments Association.	• Transactions that occur at this site are in accordance with the laws and business practices of Alberta, Canada, for example, Alberta Securities Commission
A3	<u>Customer support & service</u> The entity discloses on its Web site (and/or in information provided with the product) where customers can obtain warranty, repair service, and support related to the goods and services purchased on its Web site.	• Warranty and other service can be obtained at any one of our 249 worldwide locations that are listed on this Web site. A list of these locations also is provided with delivery of all of our products. • For service and other information, contact one of our customer service representatives at 800-555-1212 between 7:00A.M. and 8:00P.M. (Central	• For service and other information, such as your specific rights and responsibilities and for the applicable laws and regulations that govern your transaction send us an e-mail at <u>OnlineServicie@bank.com</u> or call our Customer Service representatives at 1-800-666-8787.	• Feel free to contact our Customer Service via email, telephone, or regular mail twenty-four -hours a day regarding your specific rights and responsibilities and for the applicable laws and regulations which govern your transaction: – To contact ABC Trading Inc. via email: Send your message to Customer Service at service@abctrading.com. Email messages sent during market

A. Business and Information Privacy Practices—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
		Standard Time) or you can write to us as follows: Customer Service Department ABC Company 1234 Anystreet Anytown, Illinois 60000 or CustServ@ABC.COM		hours are responded to on a timely basis by dedicated online Customer Service representatives. – To contact ABC Trading Inc. via telephone: dial 800-555-1212 between 7:00 A.M.. and 8:00 P.M. (Central Standard Time) or you can write to us as follows: Customer Service Department ABC Trading Inc. 1234 Anystreet Anytown, Illinois 60000
A4	**Customer communications** The entity discloses information to enable customers to file claims, ask questions and register complaints, including, but not limited to, the following:			
	• Street address (not a post office box or email address) • Telephone number (a number to reach an	• If you wish to file a claim or have questions or complaints about our products, you can call one of our customer service representatives at 800-555-1212 between 7:00	• In case of errors or if you have questions or complaints about our services, you can call one of our customer service representatives at	• In case of errors or if you have questions or complaints about our services, you can call one of our customer service representatives at 800-555-1212 between 7:00 A.M.

A. **Business and Information Privacy Practices**—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
	employee on a reasonably timely basis and not only a voice mail system or message machine) • Days and hours of operation • If there are several offices or branches, the same information for the principal office	A.M. and 8:00 P.M. (Central Standard Time) or you can write to us as follows: Customer Service Department ABC Company 1234 Anystreet Anytown, Illinois 60000 or CustServ@ABC.COM • If you have any questions about our organization or our privacy statement or our practices at this site, please contact CustServ@ABC.COM.	800-666-8787 between 7:00 A.M. and 8:00 P.M. (Central Standard Time) or you can write to us as follows: Customer Service Department ABC Bank 1234 Anystreet Anytown, Illinois 60000 You must notify us no later than sixty days after we have sent you the first paper or online statement on which the problem or error occurred. When contacting us with a request, please have the following information available: – Name, account number, transaction date, description of error or transaction you are unsure about, and why you believe it is an error, the dollar amount of the suspected error – For a bill payment the	and 8:00 P.M. (Central Standard Time) or you can write to us as follows: Customer Service Department ABC Trading Inc. 1234 Anystreet Anytown, Illinois 60000 ▪ If you have any questions about our organization or our privacy statement or our practices at this site, please contact CustServ@ABC.COM.

A. Business and Information Privacy Practices—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
			checking account number used to pay the bill, payee name, date the payment was authorized, payment amount, reference number, and payee account number for the payment in question • If you have any questions about our organization or our privacy statement or our practices at this site, please contact CustServ@ABC.COM.	
A4.1.	In the event outside dispute resolution is necessary, the process by which these disputes are resolved. These complaints may relate to any part of a customer's e-commerce transaction, including complaints related to the quality of services and products, accuracy,	• 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	• 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.	• 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

A. **Business and Information Privacy Practices**—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
	completeness, and distribution of private customer 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	here".	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-xxx.	here".

A. Business and Information Privacy Practices—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
	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.			
A5	**Information Privacy** The entity discloses on its Web site its information privacy practices. These practices include but are not limited to the following disclosures.			
A5.1.	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 obtain information from TRW Credit Reporting/Equifax Consumer Reporting as well as personal information you provide, for example, social security/insurance number and salary to evaluate your credit worthiness in processing your mortgage application.	• 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

A. **Business and Information Privacy Practices**—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
		• 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 zip 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 that required by law.	• 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 zip code are also used to tailor the content displayed to correspond to your preferences	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 zip code are also used to tailor the content displayed to correspond to your preferences
A5.2.	Choices regarding how individually 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	• 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.	• 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.	• 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. **Business and Information Privacy Practices**—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
	to parties not involved with the transaction.			
A5.3.	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.	• Without providing the information requested and highlighted by an asterisk, you will be unable to establish an account.
A5.4.	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 can request a copy of your customer record by sending an email to CustServ@ABC.COM. We will then send you a copy of your record via the postal service. You can then make any needed changes and provide any documentation to authenticate the change, for example, copy of social security card/social insurance registration.	• 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.
A5.5.	If the Web site uses cookies, how they are used and the consequences, if any, of an individual's refusal to accept a cookie.	• 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,	• 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	• 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

A. **Business and Information Privacy Practices**—The entity discloses its business and information privacy practices for e-commerce transactions and executes transactions in accordance with its disclosed practices.

	Criteria	Illustrative Disclosures for Retail Goods and Other Non-financial Services	Illustrative Disclosures for Online Banking	Illustrative Disclosures for Online Securities Trading
		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.	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 our marketing purposes. Our cookies expire in thirty days.	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.
A6.	**Monitoring** The entity maintains monitoring procedures that provide reasonable assurance of the following: • Its business practice disclosures on its Web site remain current. • Reports of noncompliance are promptly addressed and corrective measures taken.	• Management regularly receives and reviews information that permits monitoring of business disclosures and transaction integrity (such as complaint rates, return rates, customer surveys, warranty and replacement rates).	• Management regularly receives and reviews information that permits monitoring of business disclosures and transaction integrity (such as transaction rejected reports, complaint rates, customer surveys).	• Management regularly receives and reviews information that permits monitoring of business disclosures and transaction integrity (such as transaction rejected reports, complaint rates, customer surveys).

B **Transaction Integrity**—The entity maintains effective controls to provide reasonable assurance that customers' transactions using e-commerce are completed and billed as agreed.

	Criteria	Illustrative Controls for Retail Goods and Non-financial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
B1	**Requesting goods and/or services** The entity maintains controls to provide reasonable assurance that:			
B1.1.	Each request or transaction is checked for accuracy and completeness.	• Web scripts contain error checking for invalid inputs. • The entity's computer system automatically checks each order for accuracy and completeness of information before processing.	• Web scripts contain error checking for invalid inputs. • The entity's computer system automatically checks each financial transaction for accuracy and completeness of information before processing.	• Web scripts contain error checking for invalid inputs. • The entity's computer system automatically checks each trade for accuracy and completeness of information before processing.
B1.2.	Positive acknowledgment is received from the customer before the transaction is processed	• All customer-provided information for the order is displayed to the customer. Customer accepts an order, by clicking *yes*, before the order is processed. • Customer receives a confirming email and can correct or cancel order prior to fulfillment	• All financial transactions are displayed to the customer to accept, by clicking *yes*, before the transaction is processed.	• All trades are displayed to the customer to accept, by clicking *yes*, before the transaction is processed.
B2	**Processing requests for goods and/or services**			

B **Transaction Integrity**—The entity maintains effective controls to provide reasonable assurance that customers' transactions using e-commerce are completed and billed as agreed.

	Criteria	Illustrative Controls for Retail Goods and Non-financial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
	The entity maintains controls to provide reasonable assurance that:			
B2.1.	The correct goods are shipped in the correct quantities in the time frame agreed, or services and information are provided to the customer as requested.	• Packing slips are created from the customer sales order and checked again as order is picked and packed. • Commercial delivery methods are used that reliably meet expected delivery schedules. • Shipping manifests are retained. • Entity retains customer orders or contract information. • Service delivery targets are maintained and actual services provided are monitored against such targets. • The entity uses a "feedback" questionnaire to confirm customer satisfaction with completion of service or delivery of information to the customer.	• The entity's computer system has controls (for example, balancing controls, daily reconciliation controls) to ensure that submitted transactions are processed completely, accurately and in a timely manner.	• We provide current status of your order on our Web site. Customers know immediately if their order was processed correctly. • The entity's computer system has controls (for example, order tracking, balancing controls, daily reconciliation controls) to ensure that submitted orders are processed completely, accurately and in a timely manner.
B2.2.	Transaction exceptions are promptly communicated to the customer.	• Computerized backorder records are maintained and are designed to notify customers of backorders within twenty-four hours. Customers are given the option to cancel a	• The entity's staff investigates all rejected transactions and escalates unresolved problems to the customer services manager. Customers are notified via email or telephone	• The entity's staff investigates all rejected transactions and escalates unresolved problems to the customer services manager. Customers are notified via email or telephone

B **Transaction Integrity**—The entity maintains effective controls to provide reasonable assurance that customers' transactions using e-commerce are completed and billed as agreed.

	Criteria	Illustrative Controls for Retail Goods and Non-financial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
		backorder or have an alternate item delivered.	of potential problems related to online transactions.	of potential problems related to online transactions.
B3	**Processing bill/payment** The entity maintains controls to provide reasonable assurance that:			
B3.1.	Sales prices and all other costs/fees are displayed for the customer before processing the transaction.	• Customer has the option of printing, before order is processed, an "order confirmation" on line for future verification with payment records (such as credit card statement) detailing all information of the order (such as item(s) ordered, sales prices, costs, sales taxes, shipping charges, and so on). • All costs, including taxes and shipping, and currency used are displayed to the customer. Customer accepts an order, by clicking *yes*, before the order is processed.	• All financial services fees are displayed on the Web site describing the financial services and the fee options available to the customer. • Each fee option for financial services describes fully the fees (transaction fee, monthly fee, and so on) including any transaction limits in amount and number placed on the customer. • All deposit and loan interest rates are displayed to the customer. • All foreign exchange rates are displayed to the customer before performing a transaction involving foreign currency. • The transaction details (for example, amount, account numbers, bill payment vendor,	• All fees (fixed and transaction based) are displayed on the Web site describing the service and the fee options to the customer.

B **Transaction Integrity**—The entity maintains effective controls to provide reasonable assurance that customers' transactions using e-commerce are completed and billed as agreed.

	Criteria	Illustrative Controls for Retail Goods and Non-financial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
			foreign currency rate, interest rate, transaction fee) are displayed before the customer accepts the transaction. Customer accepts transaction, by clicking *yes*, before the transaction is processed.	
B3.2.	Transactions are billed and electronically settled as agreed.	• Billing and settlement experiences are monitored on a daily basis against policy as disclosed at Web site. • Total costs and the expected shipping and billing dates are displayed for the customer before the customer accepts the order.	• A transfer of funds before 5 P.M. (PST) on a business day is posted to your account the same day. All transfers completed after 5 P.M. (PST) on a business day or on a Saturday, Sunday, or banking holiday will be posted on the next business day. • All bill payments will be withdrawn from the account on the day the payment is scheduled to be sent to the payee whether these payments are made electronically or by check. • Standard procedures exist for establishing the vendor bill payment process and the authorized vendor list.	• All trades are settled from your cash account. Market orders placed when the markets are open are typically executed and confirmed in a matter of seconds. For limit orders placed during market hours, our Best Market Determination Module will determine where the order gets placed. If the market is closed, your order is transmitted to the exchange before the start of the next trading day.
B3.3.	Billing or settlement errors are promptly corrected.	• Billing or settlement errors are	• Posting errors are followed up	• Posting errors are followed up

B **Transaction Integrity**—The entity maintains effective controls to provide reasonable assurance that customers' transactions using e-commerce are completed and billed as agreed.

	Criteria	Illustrative Controls for Retail Goods and Non-financial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
		followed up and corrected within twenty-four hours of reporting by the customer.	and corrected within twenty-four hours of reporting by the customer.	and corrected within twenty-four hours of reporting by the customer.
B4	**Transaction history** The entity maintains controls that allow for subsequent follow-up of transactions.	• The company maintains a transaction history for each order. • Each order has a unique identifier that can be used to access order information. Such information also can be accessed by customer name and dates of ordering, shipping or billing. • The entity maintains this identifier and detailed order records that enable customers to contact the entity about details of orders for at least ninety days from order fulfillment. • Order history information is maintained for six months from the date of shipment and is available for immediate access by customer service representatives. After six months, this information is	• The entity's computer system maintains a transaction history for each service requested and related transaction. • Upon completion of a transaction, the entity's computer system issues a unique identifier (for example., confirmation number) confirming that the transaction has been processed successfully, and displays the number to the customer together with the date and time of the transaction. Each transaction can be accessed by customer name or account number or date of transaction. • All transactions are also recorded on the customer statement that can be accessed by the customer. • Two years of customer transaction history is available	• The entity's computer system maintains a transaction history for all trades requested and related transaction. One year's transaction history can be viewed on line. • Upon completion of a transaction, the entity's computer system issues a unique identifier (for example, confirmation number) confirming that the transaction has been processed successfully, and displays the number to the customer together with the date and time of the transaction. Each transaction can be accessed by customer name or account number or date of transaction. • We mail out monthly statements for each month in which your account shows activity, and quarterly statements for inactive

B **Transaction Integrity**—The entity maintains effective controls to provide reasonable assurance that customers' transactions using e-commerce are completed and billed as agreed.

	Criteria	Illustrative Controls for Retail Goods and Non-financial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
		maintained in a form that can be accessed by customer service representatives within three days.	to the entity to make inquiries and answer any client questions.	accounts. • Two years of customer transaction history is available to the entity to make inquiries and answer any client questions.
B5	**Entity monitoring of its transaction integrity** The entity maintains monitoring procedures that provide reasonable assurance of the following: • Its transaction integrity controls remain effective. • Reports of noncompliance are promptly addressed and corrective measures taken.	• Noncompliance situations are corrected when discovered and remedial actions taken are closely monitored for thirty days to prevent recurrence.	• Noncompliance situations are corrected when discovered and remedial actions taken are closely monitored for thirty days to prevent recurrence.	• Non-compliance situations are corrected when discovered and remedial actions taken are closely monitored for thirty days to prevent recurrence.

C **Information Protection**—The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce is protected from uses not related to the entity's business.[6]

	Criteria	Illustrative Controls for Retail Goods and Other Nonfinancial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
C1.	**Transmission of private customer information** The entity maintains controls to protect transmissions of private customer information over the Internet from unintended recipients.	• Private customer information is protected during transmission by using encryption technology, meaning, Secure Sockets Layer (SSL) technology. The customer has the option of calling the entity's 800 number to provide his or her name, address, and credit card information to protect transmission of this information over the Internet. • The entity has registered its Domain Name and Internet IP address to protect its Internet identity. The address is unique and no more than one company can have the same address. • The entity's Web site has a digital certificate, which can be checked using features in a standard Web browser. • The entity's Webmaster updates the site and reviews and tests key	• Private customer information is protected during transmission by using 128-bit encryption technology SSL technology). • The entity has registered its Domain Name and Internet IP address to protect its Internet identity. The address is unique and no more than one company can have the same address. • The entity's Web site has a digital certificate, which can be checked using features in a standard Web browser. • The entity's Webmaster updates the site and reviews and tests key Web pages at least daily to ensure that improper content or links have not been added. • The entity provides guidance	• Private customer information is protected during transmission by using 128-encryption technology SSL technology). • The entity has registered its Domain Name and Internet IP address to protect its Internet identity. The address is unique and no more than one company can have the same address. • The entity's Web site has a digital certificate, which can be checked using features in a standard Web browser. • The entity's Webmaster updates the site and reviews and tests key Web pages at least daily to ensure that improper content or links have not been added. • The entity provides guidance

[6] *See footnote 1.*

C **Information Protection**—The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce is protected from uses not related to the entity's business.[6]

	Criteria	Illustrative Controls for Retail Goods and Other Nonfinancial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
		Web pages at least daily to ensure that improper content or links have not been added. • The entity provides guidance (for example, Security FAQs) on its Web site outlining the customers' responsibilities to ensure customer information is transmitted securely. • The entity provides a customer confirmation of the transaction via email which is unencrypted. The customer has the ability to "opt out" of receiving this receipt.	(for example, Security FAQs) on its Web site outlining the customers' responsibilities to ensure customer information is transmitted securely. ▪ All transactions and confirmations are done on-line and in a secure, encrypted session.	(for example, Security FAQs) on its Web site outlining the customers' responsibilities to ensure customer information is transmitted securely. ▪ Upon completion of the transaction a confirmation screen is displayed with the details of the customer transactions. The customer can print this screen as receipt.
C2	**Collecting customer information** The entity maintains controls over the collection of data and has policies which provide customers with the following: ▪ A choice as to whether individually identifiable			

C **Information Protection**—The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce is protected from uses not related to the entity's business.[6]

	Criteria	Illustrative Controls for Retail Goods and Other Nonfinancial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
	information collected from them online may be used for purposes other than completing the transaction in progress (an internal secondary use or external third-party use[7]) • The opportunity to opt out of any particular internal secondary or external third- party usage of that information except those required by law or other regulatory agency	• If the customer wishes that the information not be used for one or more of these purposes, they can click a box on the screen to opt out of providing such data to third parties.	• If the customer wishes that the information not be used for one or more of these purposes, they can click a box on the screen to opt out of providing such data to third parties.	• If the customer wishes that the information not be used for one or more of these purposes, they can click a box on the screen to opt out of providing such data to third parties. If you previously did not opt out of providing information to an outside vendor or individual and wish to be removed for lists we sell to these third parties, please send an email to custserv@abc.com with your request, or you can always telephone or write customer service.
C3	**Protection and use of private customer information**			

[7] Internal secondary would be defined as another department or service offered by an entity not directly involved with the customer transaction, for example a credit card service offered by an institution that offers mortgage services. An external third party company is defined as an unrelated entity to the company that receives information from the company directly involved with the customer transaction, for example a mailing house that buys mailing lists from companies seeking prospective buyers of other goods or services.

C **Information Protection**—The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce is protected from uses not related to the entity's business.[6]

	Criteria	Illustrative Controls for Retail Goods and Other Nonfinancial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
	The entity maintains controls to protect private customer information obtained as a result of e-commerce and retained in its system from outsiders.			
C3.1.	Systems that retain private customer 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 customer information is processed and stored on servers protected with access control rules to prevent unauthorized access	• Commercial firewalls are used. They are updated regularly and tested periodically for susceptibility to security weaknesses. • Edit checks exist on all Web page input screens to disable unauthorized data that could trigger the unauthorized processing execution of system programs on the Web Server. • All private customer information is processed and stored on servers protected with access control rules to prevent unauthorized access. • Directory browsing has been disabled on the Web Server to prevent outsiders from browsing a list of files (especially if no default index file has been defined).	• Commercial firewalls are used. They are updated regularly and tested periodically for susceptibility to security weaknesses. • All private customer information is processed and stored on servers protected with access control rules to prevent unauthorized access. • Edit checks exist on all Web page input screens to ignore unauthorized data that could trigger the unauthorized processing execution of system programs on the Web Server.

C **Information Protection**—The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce is protected from uses not related to the entity's business.[6]

	Criteria	Illustrative Controls for Retail Goods and Other Nonfinancial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
C3.2.	Customers entering through the Web page cannot access other customers' private information.	• All system access from outside the entity, other than for customary e-commerce transactions through the Web page, (through the Internet, dial up, or other connections) is restricted by one-time passwords and/or smart cards.	• All access to customer accounts is restricted to the customer through the use of a unique digital certificate associated with each customer. • Customer sessions between the browser and e-commerce systems are protected to avoid other users from hijacking a customer's session (for example, use of unique digital certificates or cookies checking for random unique identifiers before the start of each session). • All system access from outside the entity, other than for customary e-commerce transactions through the Web page, (through the Internet, dial up, or other connections) is restricted by authentication systems using one-time passwords.	• All access to customer accounts is restricted to the customer through the use of a unique user ID and secret password. • Customer sessions between the browser and the e-commerce systems are protected to avoid other users from hijacking a customer's session (for example, use of unique digital certificates or cookies checking for random unique identifiers before the start of each session). • All system access from outside the entity, other than for customary e-commerce transactions through the Web page, (through the Internet, dial up, or other connections) is restricted by authentication systems using one-time passwords.
C3.3.	Private customer information obtained as a result of e-commerce is not intentionally disclosed to parties not related to the	• Policy restricts the entity staff from disclosing private customer information to any third party without the express consent of the customer or as otherwise	• Policy restricts the entity staff from disclosing private customer information to any third party without the express consent of the customer or as	• Policy restricts the entity staff from disclosing private customer information to any third party without the express consent of the customer or as

C **Information Protection**—The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce is protected from uses not related to the entity's business.[6]

	Criteria	Illustrative Controls for Retail Goods and Other Nonfinancial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
	entity's business unless (1) customers are clearly notified prior to their providing such information or (2) customer permission is obtained after the customer has provided such information.	provided by law.	otherwise provided by law.	otherwise provided by law.
C3.4.	Private customer information obtained as a result of e-commerce is used by employees only in ways associated with the entity's business	• All private customer information is restricted to only authorized persons within the entity and protected through effective authentication systems and/or encryption technology. • The entity has *strict* policies and monitoring procedures to ensure that only certain employees can access private customer information. These policies also set forth ways that customer information can and cannot be used. Policy enforcements are made possible through conditions of employment statement.	• All private customer information is restricted to only authorized persons within the entity and protected through effective authentication systems and/or encryption technology. • The entity has policies and monitoring procedures to ensure that only certain employees can access private customer information. These policies also set forth ways that customer information can and cannot be used. Policy enforcements are made possible through conditions of employment statement.	• All private customer information is restricted to only authorized persons within the entity and protected through effective authentication systems and/or encryption technology. • The entity has policies and monitoring procedures to ensure that only certain employees can access private customer information. These policies also set forth ways that customer information can and cannot be used. Policy enforcements are made possible through conditions of employment statement.

C **Information Protection**—The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce is protected from uses not related to the entity's business.[6]

	Criteria	Illustrative Controls for Retail Goods and Other Nonfinancial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
C4	**Accuracy and completeness of information** The entity maintains controls so that individually identifiable information collected, created or maintained by it is accurate and complete for its intended use	• The entity 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.	• The entity 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.	• The entity 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.
C5	**Entity responsibility for third party information** The entity maintains controls and carries out 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 transfer data to the outsource provider. The entity obtains representation as to the controls that are followed by the outsource provider.	• The entity provides information from credit applications to an outside credit reporting agency. The entity's contract with the credit reporting agency sets forth the manner in which such information is protected. .	• The entity outsources the stock market quoting function of the entity's Web site. The entity obtains the policies of this provider regarding the information protection and privacy of the data shared.

C **Information Protection**—The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce is protected from uses not related to the entity's business.[6]

	Criteria	Illustrative Controls for Retail Goods and Other Nonfinancial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
C6	**Protection of customers' computers and files** The entity maintains controls to protect against its unauthorized access to customer's computers and its unauthorized modification of customer's computer files:			
C6.1.	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.	• 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.	• 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.
C6.2.	Transmission of malicious computer code to customers is prevented.	• The entity maintains antivirus software on its systems, updates its virus signatures at least monthly, and takes reasonable precautions to protect both its systems and the customer's computer from viruses during the	• The entity maintains antivirus software on its systems, updates its virus signatures at least monthly, and takes reasonable precautions to protect both its systems and the customer's computer from	• The entity maintains antivirus software on its systems, updates its virus signatures at least monthly, and takes reasonable precautions to protect both its systems and the customer's computer from

C **Information Protection**—The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce is protected from uses not related to the entity's business.[6]

	Criteria	Illustrative Controls for Retail Goods and Other Nonfinancial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
		e-commerce session. • The entity implements programming standards and conducts software testing to ensure Web pages using active content technologies (for example. Java applets, Active X, JavaScripts) are not susceptible to security weaknesses.	viruses during the e-commerce session. • The entity implements programming standards and conducts software testing to ensure Web pages using active content technologies (for example. Java applets, Active X, JavaScripts) are not susceptible to security weaknesses.	viruses during the e-commerce session. • The entity implements programming standards and conducts software testing to ensure Web pages using active content technologies (for example, Java applets, Active X, JavaScripts) are not susceptible to security weaknesses.
C7	**Monitoring** The entity maintains monitoring procedures that provide reasonable assurance regarding the following:			
C7.1.	Its information protection controls remain effective.	• Management receives and reviews information that permits monitoring of information protection (such as attempts to bypass security controls, security violations, firewall and antivirus updates, virus incident reports, version release number of currently installed security and encryption software and most recent version release number of	• Management receives and reviews information that permits monitoring of information protection controls (such as attempts to bypass security controls, security violations, firewall and antivirus updates, virus incident reports, version release number of currently installed security and	• Management receives and reviews information that permits monitoring of information protection controls (such as attempts to bypass security controls, security violations, firewall and antivirus updates, virus incident reports, version release number of currently installed security and

C **Information Protection**—The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce is protected from uses not related to the entity's business.[6]

	Criteria	Illustrative Controls for Retail Goods and Other Nonfinancial Services	Illustrative Controls for Online Banking	Illustrative Controls for Online Securities Trading
		software from the software vendor, and actions taken to correct published security weaknesses).	encryption software and most recent version release number of software from the software vendor, and actions taken to correct published security weaknesses).	encryption software and most recent version release number of software from the software vendor, and actions taken to correct published security weaknesses).
C7.2.	Reports of non-compliance are promptly addressed and corrective measures taken.	• Noncompliance situations are corrected when discovered and remedial actions taken are closely monitored for thirty days to prevent recurrence.	• Noncompliance situations are corrected when discovered and remedial actions taken are closely monitored for thirty days to prevent recurrence.	• Noncompliance situations are corrected when discovered and remedial actions taken are closely monitored for thirty days to prevent recurrence.

APPENDIX A —EXAMPLES OF PRACTITIONER REPORTS

This appendix presents two illustrative reports for WebTrust 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 2.0 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 Certified Public Accountant's Report

To The Management of ABC Company, Inc.:

We have examined the assertion **[hot link to management's assertion]** by the management of ABC Company, Inc. (ABC) regarding the disclosure of its e-commerce business and information privacy practices on its Web site and the effectiveness of its controls over transaction integrity and information protection for e-commerce (at WWW.ABC.COM) based on the AICPA/CICA WebTrust Criteria **[hot link]**, during the period Xxxx xx, 1999 through Yyyy yy, 2000.

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 business and information privacy practices and its controls over the processing of e-commerce transactions and the protection of related private customer information, (2) selectively testing transactions executed in accordance with disclosed business and information 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.

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, or (3) changes required because of the passage of time, such as to accommodate dates in the year 2000, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

In our opinion, during the period Xxxx xx, 1999 through Yyyy yy, 2000, ABC Company, in all material respects—

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

based on the AICPA/CICA *WebTrust* Criteria.

The CPA *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.

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

[*Name of CPA firm*]

Certified Public Accountants

[*City, State*]

[*Date*]

Illustration No. 2 for Use in Canada

Auditor's Report

To The Management of ABC Company, Inc.:

We have audited ABC Company's disclosure of its e-commerce business and information privacy practices on its Web site and the effectiveness of its controls over transaction integrity and information protection for e-commerce (at WWW.ABC.COM) during the period Xxxx xx, 1999 through Yyyy yy, 2000. These e-commerce disclosures and controls are the responsibility of ABC Company's management. Our responsibility is to express an opinion on the conformity of those disclosures and controls with the AICPA/CICA WebTrust Criteria **[hot link]** 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 business and information privacy practices and its controls over the processing of e-commerce transactions and the protection of related private customer information, (2) selectively testing transactions executed in accordance with disclosed business and information 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 business and information privacy practices for e-commerce transactions and executed transactions in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that customers' orders placed using e-commerce were completed and billed as agreed
- Maintained effective controls to provide reasonable assurance that private customer information obtained as a result of e-commerce was protected from uses not related to ABC Company's business

in accordance with the AICPA/CICA WebTrust 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, or (3) changes required because of the passage of time, such as to accommodate dates in the year 2000, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The CA 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.

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

[Name of CA firm] *[City, Province]*

Chartered Accountants *[date of report]*

Appendix B - WEBTRUST[SM/TM] SELF-ASSESSMENT QUESTIONNAIRE (VERSION 2.0)

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

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

based on the AICPA/CICA WebTrust[SM/TM] Criteria."

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

I General Information

A. E-commerce Activities to Be Covered

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

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

   b) Who is the typical customer?

   c) What is the typical form of payment?

2. What is the Web site URL?

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

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

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

B. Information Systems Used to Support E-commerce Activities

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

   a) Provide a description.

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

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

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

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

   a) Give a description.

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

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

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

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

a) Provide a description.

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

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

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

C. Web Site Server Technology

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

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

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

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

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

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

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

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

5. Identify the WebServer package used.

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

D. Control Environment

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

   a) Management's "tone at the top"

   b) Hiring, development, and retention of competent personnel

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

   d) Supervising business activities and control procedures

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

   f) Other factors

II Business and Information Privacy Practices

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

A. Description of Business Practices.

1. Describe the entity's business practices and how such practices are

disclosed to customers for each of the following.

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

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

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

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

   (4) Other relevant descriptive information.

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

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

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

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

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

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

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

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

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

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

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

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

   (2) Telephone number (a number to reach an employee on a reasonably timely basis and not only a voice mail system or message machine).

(3) Days and hours of operation.

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

(5) Other relevant information for customers,

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

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

(2) The use of that information.

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

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

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

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

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

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

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

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

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

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

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

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

2. Describe who is responsible for controlling these activities.

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

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

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

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

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

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

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

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

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

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

III Transaction Integrity Controls

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

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

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

   a) How the entity provides reasonable assurance that—

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

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

   b) How the entity provides reasonable assurance that—

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

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

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

   c) How the entity provides reasonable assurance that—

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

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

      (3) Billing or settlement errors are promptly corrected.

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

2. Describe who is responsible for controlling these activities.

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

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

1. Its transaction integrity controls remain effective.

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

   b) Reports of noncompliance are promptly addressed and corrective

measures taken.

IV Information Protection Controls

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

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

A. Description of the controls over the collection of data

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

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

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

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

2. Describe the controls maintained by the entity to protect private customer information obtained as a result of e-commerce and retained in its system from outsiders, as follows.

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

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

about their own transactions).

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

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

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

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

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

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

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

4. Who is responsible for controlling these activities?

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

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

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

C. Describe the processes management uses to monitor the continuing effectiveness of its controls over information protection to provide reasonable assurance that—

1. Its information protection controls remain effective.

2. Its information protection controls continue to meet the WebTrust Criteria.

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

V Change Management and CPA/CA Notification

A. Description of the Change Management Process

1. Describe the entity's controls over changes to its electronic business practices, its transaction integrity controls, its information protection controls, and its e-commerce systems and supporting technology, which are designed to provide reasonable assurance that—

   a) All such changes are approved by management.

   b) Changes in business practices are reflected in modified disclosures of such practices.

   c) Changes in the manner in which e-commerce transactions are executed are reflected in modified business practice disclosures.

   d) Modified business practice disclosures continue to conform to the WebTrust Criteria.

   e) Controls over transaction integrity and information protection continue to function effectively and to conform to the WebTrust Criteria.

B. Description of the Process to be Used to Notify CPA or CA of Changes

1. Describe the entity's policies and procedures to notify the CPA or CA in advance of making changes to the following:

   a) E-commerce activities

   b) E-commerce systems and supporting technology

   c) Business practices and disclosures of business practices

d) Controls over transaction integrity

e) Controls over information protection

f) Monitoring procedures over the foregoing

g) Control environment

2. Who is responsible for notifying the CPA or CA of such changes?

3. Has the entity changed those controls, procedures, or responsibilities designed to provide reasonable assurance that the CPA or CA is notified of all relevant changes in the last three months? If so, describe such changes and when each was made.

VI Other Matters

A. Describe below any other matters that would be relevant to the CPA or CA in evaluating the Web site's conformity with the WebTrust Criteria. Examples might include the following:

1. Significant changes in the entity's business or its organizational structure

2. Significant problems in meeting demand for its goods and services, meeting its customer commitments or continuing its historical level of customer satisfaction (for example., as might be evidenced by unusual levels of customer complaints).

3. Significant processing or controls problems with the entity's e-commerce systems or supporting infrastructure.

4. Instances of fraud and breaches of transaction integrity, security and information protection controls involving the following:

   a) Employees with e-commerce responsibilities

   b) Contractors and others who provide services to the entity related to its e-commerce activities

   c) Unauthorized third parties

   d) Systems and supporting infrastructure used for executing e-commerce transactions.

5. Significant changes in management and other key personnel with e-commerce responsibilities.

6. Significant changes in legal or regulatory requirements affecting the entities business or the operation of its Website

7. Other relevant information.

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 addendi 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[8] 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.

[8] 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 for claims <$1,000. The cost for claims >$1,000-$15,000 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 – Canada

In Canada, an e-commerce merchant is not obliged to choose NAF or its Canadian affiliate (name to be confirmed) 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 client should refer to NAF's Code of Procedure to gain a full understanding of the intent of the principles.