

Appendix B

WebTrustsm Self-Assessment Questionnaire

Version 1.0 - December 1997

This questionnaire is for use by electronic commerce service providers in documenting their electronic 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 _____, 199__ through _____, 199__ the entity:

- disclosed its business practices for electronic commerce transactions and executed transactions in accordance with its disclosed business practices,
- maintained effective controls to provide reasonable assurance that customers’ orders placed using electronic commerce were completed and billed as agreed, and
- maintained effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce was protected from uses not related to its business

based on the AICPA/CICA *WebTrustsm* Criteria.”

Entity Name _____

Entity Location _____

Web Site URL _____

Server Location _____

Period Covered: From _____

Through _____

Date Prepared _____

Prepared By _____

I. General Information

A. Electronic Commerce Activities to Be Covered

1. Describe the entity's electronic commerce activities that are asserted/represented to meet the *WebTrust* Principles and Criteria.
 - a) What goods / services are being sold / 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 organization reporting relationship to the entity's management?
4. How long has the entity been selling such goods and services through this form of electronic commerce?
5. If the electronic commerce activities have changed in the last 90 days, describe the nature of such changes and when each change occurred.

B. Information Systems Used to Support the Electronic Commerce Activities

1. Web Site or Other Customer Interface Systems
 - a) Description
 - b) 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. Telecommunications & Network Systems
 - a) Description
 - b) 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. Other Supporting Systems and Technology
 - a) Description
 - b) 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. 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 electronic commerce transaction integrity and the protection of related private customer information. Such factors might include, but not be limited to:
 - 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 electronic commerce activities.
 - f) Other factors.

II. Business Practice Disclosures

- A. Principle - *The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed practices.***

B. 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) The terms and conditions by which electronic commerce transactions are conducted
 - (1) Time frame for fulfillment of orders for goods or services.
 - (2) Time frame and process for informing customers of backorder or other order exceptions and available customer options.
 - (3) Normal method of delivery, including customer options, if any.
 - (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, if any.
 - (8) Other relevant terms and conditions, if any.
 - b) 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 (i.e., whether they are new, used, or reconditioned).
 - (2) Description of services (or service contract).
 - (3) Sources of information (i.e., where it was obtained and how it was compiled).
 - (4) Other relevant descriptive information.
 - 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 its Web site.

- d) Information to enable customers to file claims, ask questions and register complaints, including 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.
- 2. Describe who is responsible for controlling these activities.
- 3. Has the entity changed its business practices or the related disclosures in the last 90 days?
 - a) If so, describe the nature of such changes and when each change occurred.

C. Where there are local, national, or other laws or requirements affecting business terms and conditions (e.g., customer 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.

D. 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.

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

- 1. The electronic 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.

F. Self-Assessment Questions (Yes / No / Not Applicable)

1. Does the entity disclose the time frame for fulfillment of orders for goods and services?
2. Does the entity disclose the time frame and process for informing customers of backorder or other order exceptions and the available customer options?
3. Does the entity disclose its normal method of delivery and customer options, if any?
4. Does the entity disclose its payment terms and customer options, if any?
5. Does the entity disclose its electronic settlement practices and related charges to customers?
6. Does the entity disclose how the customer may cancel recurring charges, if any?
7. Does the entity disclose its return policies or that there are no return practices?
8. Does the entity disclose 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:
 - a) Condition of goods (i.e., whether they are new, used, or reconditioned)?
 - b) Description of services (or service contract)?
 - c) Sources of information (i.e., where it was obtained and how it was compiled)?
9. Does the entity disclose (on its Web site and/or in information provided with the product) where customers can obtain warranty, service and support related to the goods and services purchased on its Web site?
10. Does the entity disclose information to enable customers to file claims, ask questions and register complaints, including:
 - a) Street address (not a post office box or E-mail address)?
 - b) Telephone number (a number to reach an employee on a reasonably timely basis and not only a voice mail system or message machine)?
 - c) Days and hours of operation?
 - d) If there are several offices or branches, is the same information disclosed for the principal office?

III. Transaction Integrity Controls

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

B. Description of steps taken to ensure the integrity of electronic commerce transactions

1. Describe the controls maintained by the entity to ensure the integrity of electronic commerce transactions:
 - a) How the entity provides reasonable assurance that:
 - (1) Each order is checked for accuracy and completeness.
 - (2) Positive acknowledgment is received from the customer before the order 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 on the order.
 - (3) Back order and other exceptions are promptly communicated to the customer.
 - c) How the entity provides reasonable assurance that:
 - (1) Sales prices and all other costs are displayed for the customer before requesting acknowledgment of the order.
 - (2) Orders are billed and electronically settled as agreed.
 - (3) Billing or settlement errors are promptly corrected.
 - d) How entity maintains controls that allow for subsequent follow-up of orders.
2. Describe who is responsible for controlling these activities.
3. Has the entity changed its controls over transaction integrity in the last 90 days?
 - a) If controls over transaction integrity have changed, describe the nature of such changes and when each change occurred.

C. 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.
2. Its transaction integrity controls continue to meet the *WebTrust* Criteria.
3. Reports of noncompliance are promptly addressed and corrective measures taken.

D. Self-Assessment Questions (Yes / No / Not Applicable)

1. Does the entity maintain controls to provide reasonable assurance that:
 - a) Each order is checked for accuracy and completeness?
 - b) Positive acknowledgment is received from the customer before the order is processed?
2. Does the entity maintain controls to provide reasonable assurance that:
 - a) The correct goods are shipped in the correct quantities in the time frame agreed?
 - b) Services and information are provided to the customer as agreed to on the order?
 - c) Back order and other exceptions are promptly communicated to the customer?
3. Does the entity maintain controls to provide reasonable assurance that:
 - a) Sales prices and all other costs are displayed for the customer before requesting acknowledgment of the order?
 - b) Orders are billed and electronically settled as agreed?
 - c) Billing or settlement errors are promptly corrected?
4. Does the entity maintain controls that allow for subsequent follow-up of orders?

5. Does the entity maintains monitoring procedures that provide reasonable assurance that:
 - a) Its business practice disclosures on its Web site remain current?
 - b) Its transaction integrity controls remain effective?
 - c) Reports of noncompliance are promptly addressed and corrective measures taken?
6. Does the entity have a control environment that is generally conducive to reliable business practice disclosures on its Web site and effective controls over electronic commerce transaction integrity?

IV. Information Protection Controls

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

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

- 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 electronic commerce and retained in its system from outsiders:
 - a) How systems that retain private customer information obtained as a result of electronic commerce are protected from outside access.

- b) How the entity ensures that customers entering through the Web page can only perform inquiries, execute transactions, and obtain information about their transactions.
 - c) How private customer information obtained as a result of electronic commerce is protected from intentional disclosure to parties not related to the entity's business unless:
 - (1) customers are clearly notified prior to their providing such information, or
 - (2) customer permission is obtained after they have provided such information.
 - d) How the entity ensures that private customer information obtained as a result of electronic 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:
- a) 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) How the entity ensures that transmission of computer 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 90 days?
- a) If so, describe the nature of such changes and when each change occurred.

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 transaction integrity controls continue to meet the *WebTrust* Criteria.
- 3. Reports of noncompliance are promptly addressed and corrective measures taken.

D. Self-Assessment Questions (Yes / No / Not Applicable)

1. Does the entity maintain controls to protect transmissions of private customer information over the Internet from unintended recipients?
2. Does the entity maintain controls to protect private customer information obtained as a result of electronic commerce and retained in its system from outsiders:
 - a) Are systems that retain private customer information obtained as a result of electronic commerce protected from outside access?
 - b) Are customers entering through the Web page restricted to only performing inquiries, executing transactions, and obtaining information about their transactions?
 - c) Is private customer information not intentionally disclosed to parties not related to the entity's business unless:
 - (1) customers are clearly notified prior to their providing such information, or
 - (2) customer permission is obtained after they have provided such information?
 - d) Is private customer information used by employees only in ways associated with the entity's business?
3. Does the entity maintain controls to protect against its unauthorized access to customer's computers and its unauthorized modification of customer's computer files:
 - a) 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?
 - (1) Does this include obtaining permission or providing customer notification before using "cookies"?
 - b) Transmission of computer viruses to customers is prevented?
4. Does the entity maintain monitoring procedures that provide reasonable assurance that:
 - a) Its information protection controls remain effective?
 - b) Reports of non-compliance are promptly addressed and corrective measures taken?

5. Does the entity have a control environment that is generally conducive to effective controls over protection of private customer information?

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 commerce business practices, its transaction integrity controls, its information protection controls, and its electronic 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 electronic 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 its:
 - a) electronic commerce activities,
 - b) electronic 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, and
 - 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 3 months?
 - a) 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:

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 (e.g., as might be evidenced by unusual levels of customer complaints).
3. Significant processing or controls problems with the entity's electronic commerce systems or supporting infrastructure.
4. Instances of fraud and breaches of transaction integrity, security and information protection controls involving: (1) employees with electronic commerce responsibilities, (2) contractors and others who provide services to the entity related to its electronic commerce activities, (3) unauthorized third parties, or (4) systems and supporting infrastructure used for executing electronic commerce transactions.
5. Significant changes in management and other key personnel with electronic commerce responsibilities.
6. Other relevant information.