# ASSURING E-COMMERCE BUSINESS ACTIVITIES

Dorothy M. Fisher
Computer Information Systems
California State University, Dominguez Hills
Carson, California 90747
EMAIL: DFISHER@soma.csudh.edu

Steven A. Fisher
Department of Accountancy
California State University, Long Beach
Long Beach, California 90840-8504
EMAIL: SFISHER@csulb.edu

Wang-chan Wong
KBquest Group, Inc
18662 MacArthur Blvd, Suite 200
Irvine, California 92747
EMAIL: WCWONG@kbquest.com

**ABSTRACT**

Trust is imperative for conducting online transactions. To reduce online risks and foster trust, assurance service providers, such as TRUSTe, BBBonline, and WebTrust, audit online businesses to assure their compliance with principles and criteria for e-commerce business activities. Of these assurance service providers, WebTrust offers the most comprehensive services, including programs for business to consumer and business to business transactions, certification authorities (CA) and service providers. WebTrust jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) offers best practices and a framework of measurable controls for electronic businesses, and thus, fosters online trust and confidence that are critical to the success of electronic commerce. As e-commerce matures, WebTrust will play an increasingly important role in CA-based e-commerce as well as in the applications service provider industry.

Keywords: E-commerce, Trust, Assurance Services, CAs, WebTrust

**INTRODUCTION**

Despite of the recent demise of many dot-com companies, e-commerce is here to stay. However, its future success is greatly dependent on trust of all parties involved in online transactions. "Confidentiality, authentication, integrity, and nonrepudiation are the four most important ingredients required for trust in e-commerce transactions" (http://ftp.webtrust.org/webtrust_public/certauth_fin.doc). Confidentiality protects user privacy and proprietary information. Authentication ensures the authenticity of an e-commerce retailer or a consumer by using digital signatures or certificates. Data integrity ensures that data is not altered during transmission. Nonrepudiation is protection from denial of a transaction by either party. Confidentiality can be provided through encryption. Authentication, data integrity, and nonrepudiation can be provided through digital signatures, and public key certificates. However. without face-to-face contact, a "bricks and mortar" facility, and direct physical exchange of goods and credit information, online commerce faces significant hurdles in developing trust.

To reduce risk and build trust and confidence online, principles and criteria for key areas critical to companies operating in e-commerce marketplaces must be established. Web site assurance services, such as those provided by the American Institute of Certified Public Accountants member firms (www.aicpa.org), the Better Business Bureau (www.bbbonline.org), MasterCard, and TRUSTe (www.truste.org), ensure online businesses comply to the established principles and criteria. Of these assurance service providers, the AICPA's WebTrust offers the most comprehensive principles and criteria for business-to-consumer and business-to-business e-commerce, for services providers, as well as for certificate authorities

The purpose of this paper is to examine the role of WebTrust in assuring e-commerce business activities and explore its potential in providing consumer confidence and entrust in e-commerce. Section one briefly discusses risks associated with e-commerce. Section two gives an overview of WebTrust. Second three discusses certificate authorities (CA) and explores the role of WebTrust in CA-based e-commerce. Section four concludes paper.

## RISKS OF E-COMMERCE

Conducting commerce over the Internet entails unique risks. In order to provide a trusted environment for consumers, e-commerce businesses must ensure some fundamental security for transactions over the Internet that includes the elements of confidentiality, authentication, data integrity, and nonrepudiation[3]. Confidentiality protects user privacy and proprietary information. Authentication ensures the authenticity of an e-commerce retailer or a consumer by using digital signatures or certificates. Data integrity ensures that data is not altered during transmission. Nonrepudiation refers to assurance that an e-commerce retailer or a consumer will not repudiate having participated in a transaction after the fact.

Gray and Debreceny [5] categorizes these security risks into three areas including:

*Business Practices and Information Privacy:* A well-constructed web page may be effective in enticing consumers to purchase goods and services. Yet, behind the web page facade the entity may be engaging in deceptive practices. Additionally, consumers need information concerning the entity's ability to fill consumers' orders, product specifications, product warranties, return policies, and the resolution of consumer complaints. A lack of such information may lead to increased risk of losses and lower satisfaction for consumers.

*Transaction Integrity:* Without proper controls over the web site Internet transactions can easily be incorrectly processed and altered. The result may be incorrect orders, improper billing, problems with returns and a series of other problems that undermine the integrity of retail e-commerce. Consumers want assurance that the entity has the effective security controls in place.

*Information Protection:* A recent Yanklevich Partners survey of 1,003 American consumers commissioned by the AICPA indicates that 85% of online users would not give out their credit card numbers when shopping online (AICPA, 4/27/98). To gain consumer confidence in the web site it is important that the entity takes appropriate steps to protect customer information. This protection includes security measures such as digital certificates to guard against the intentional or unintentional leakage of private information.

## HOW WEBTRUST SERVICES REDUCE RISKS AND FOSTER TRUST

Certified Public Accountants (CPA) have long been concerned with the integrity of corporate financial reporting and the strength of an entity's internal controls to safeguard assets and to accurately process transactions in their roles as independent auditors. Independent audits provide investors and creditors with assurance of the integrity and fairness of financial reporting and, thereby, greatly contribute to the efficiency of capital markets. In fact, United States financial reporting is considered the best and most trustworthy in the World due in part to the independent audits conducted by CPA's [8].

Recently, the CPA profession through the joint efforts of the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have ventured into a new direction offering assurance services to business-to-consumer and business-to-business e-commerce, service providers, and certificate authorities (CAs). These services termed WebTrust provide assurance to consumers and online concerns that e-commerce web sites meet WebTrust Principles and Criteria for privacy, security, integrity, availability and confidentiality, and consumer redress for complaints, and business practices online. The key areas included in WebTrust program are a site's privacy policies and procedures to protect personal information, its security practices and control and the availability of the site's system, disclosures about its business practices and transaction integrity, non-repudiation and confidentiality of information and data. WebTrust assurance is intended to reduce risks and, thus, increase trust and confidence in e-commerce.

Similar to other forms of assurance services, WebTrust assurance services are provided by specially licensed CPA firms and practitioners. In conducting a WebTrust assurance process a practitioner audits an online business and its web site to verify if it meets WebTrust Principles and Criteria. Once the WebTrust practitioner has completed the assurance process, a WebTrust Seal is awarded to the web site. Customers and business partners can click on the WebTrust seal to learn about the site's business practice disclosures, Report of the Independent Accountant, and Management's Assertions. An example of the WebTrust Seal may be viewed at http://cert.webtrust.org/verisign.html. The WebTrust practitioner continuously monitors the web site to verify its compliance with the WebTrust Principle, i.e., business practice disclosure, transaction integrity, and information protection. If the web site fails to comply with the Principles and Criteria, the seal will be revoked.

WebTrust Criteria are the basis for practitioners to assess if the principle has met at a Website. The WebTrust Privacy Principle requires the business "discloses its privacy practices, complies with such privacy practices, and maintains effective controls to provide reasonable assurance that personally identifiable information obtained as a result of electronic commerce is protected in conformity with its disclosed privacy practices." (http://www.cpawebtrust.org/privacy_fin.htm). The WebTrust Confidentiality Principle requires that the business "discloses its confidentiality practices, complies with such confidentiality practices, and maintains effective controls to provide reasonable assurance that access to information obtained as a result of electronic commerce and designated as confidential is restricted to authorized individuals, groups of individuals, or entities in conformity with its disclosed

confidentiality practice" (http://www.cpawebtrust.org/confidentiality_exp.htm). The WebTrust Security Principle states that business "discloses its key security practices, complies with such security practices, and maintains effective controls to provide reasonable assurance that access to the electronic commerce system and data is restricted only to authorized individuals in conformity with its disclosed security practices" (http://www.cpawebtrust.org/Security_fin.htm). Business Practices/Transaction Integrity Principle states that "the entity discloses its business practices for electronic commerce, executes transactions in conformity with such practices, and maintains effective controls to provide reasonable assurance the electronic commerce transactions are processed completely, accurately, and in conformity with its disclosed business practices" (http://www.cpawebtrust.org/BusPracTrans_fin.htm). The Availability Principle states the business "discloses its availability practices, complies with such availability practices, and maintains effective controls to provide reasonable assurance that electronic commerce systems and data are available in conformity with its disclosed availability practices" (http://www.cpawebtrust.org/avail_fin.htm). WebTrust for Certification Authorities (CA) establishes universal standards for issuance of digital certificates so that users of these certificates can feel confident that the certificate is valid, credible, and trustworthy. These standards surrounding security, confidentiality, authentication, integrity, and nonrepudiation are designed to increase confidence in the public key infrastructure (PKI) used by Certification Authorities. The WebTrust for Certification Authorities Principle for CA Business Practices Disclosure states "The Certification Authority discloses its key and certificate life cycle management business and information privacy practices and provides its services in accordance with its disclosed practices. The principle for service integrity is "The Certification Authority maintains effective controls to provide reasonable assurance that subscriber information was properly authenticated, the integrity of keys and certificates it manages is established and protected throughout their life cycles." (http://www.cpawebtrust.org/CertAuth_fin.htm)

The specific areas of the Webtrust criteria for each of the above principles include disclosures, policies, procedures, and monitoring. For each criterion, there are illustrative disclosures for business to consumer, business to business, CAs and Service Providers when applicable.

## CA-BASED E-COMMERCE

As e-commerce matures, certification authorities (CAs) will assume an increasingly important role in securing e-commerce[7]. CA service is based on a Public Key Infrastructure (PKI). PKI uses public/private-key pairs to provide confidentiality, authentication, integrity and nonrepudiation required for trust in e-commerce. Keys are mathematically related so that the data encrypted by a private key can be decrypted and read only by the related public key and vice-versa. These keys allow one to sign and verify signature. The signer keeps the private key and deposits the public key in an electronic directory of public keys used to verify digital signature. Using the public key, anyone can verify that a signature of a particular signer of a document. A digital signature is more difficult to forge and cannot be transfer from one document to another document. Although someone can use your public key to verify your signature, it prevents him from signing documents in your name.

However, the logistics of maintaining a directory of public keys used to verify digital signature is formidable. The so-called certification authorities (CAs) offer digital signature service. For instance, VeriSign is one such certification authority [9]. CAs verify the identity of a subscriber, say an online business, and issue and digitally sign a digital certificate that includes the subscriber's public key, identify information, and an expiration date. Once the online business receives the certificate, the business can post the certificate in the web page of his Privacy Policy. Consumer can check the authenticity certificate. The certificate can be used to identify the merchant and the key bound in the certificate can be used to encrypt message from consumer to an online business. According to the Aberdeen Group, a Boston-based research firm, the number of global companies using digital certificates will surge from 20% in 2001 to 98 percent by 2003.

Unfortunately, the proliferation of CAs offering digital signature services has resulted in a system that is disorganized and fragmented. Standards are needed for the management of certificates and the policies and practices of CAs. The WebTrust Program for Certification Authorities established universal standards for issuance of digital certificates so that users of these certificates may feel confident that the certificate is valid, credible, and trustworthy. These standards surrounding security, confidentiality, authentication, integrity, and nonrepudiation are designed to increase confidence in the public key infrastructure used by Certification Authorities. Microsoft recently required that all certification authority companies, which provide security systems for enterprises transacting commerce online, be certified by WebTrust or its equivalent in order utilize "public key" security programs embedded in Microsoft's Internet Explorer Web browser.

## CONCLUSION

Confidentiality, authentication, integrity, and nonrepudiation are the four most important ingredients required for trust in e-commerce transactions. To reduce online risk and foster trust and confidence, we need a trusted third party to police the e-commerce business activities in order to reduce risks. WebTrust assurance services are provided by a trusted third party such as a licensed CPA firm or practitioner based on WebTrust principles and criteria. WebTrust principles and criteria

developed by AICPA and CICA are perhaps the most comprehensive and for conducting trustworthy e-Commerce.

Currently, WebTrust is being offered by public accounting professionals in Argentina, Australia, Austria, Canada, Denmark, England, France, Germany, Hong Kong, Ireland, Italy, Netherlands, Puerto Rico, Scotland, Spain, the US and Wales. As e-commerce matures, WebTrust Program for Certificate Authorities will play an increasingly important role. However, it remains to be seen if WebTrust Program for Certification Authorities will be the de facto standard in the future.

**REFERENCE**

[1] American Institute of Certified Public Accountants, "Electronic Commerce Assurance," http://www.aicpa.org/assurance/about/newsvc/elec.htm.

[2] American Institute of Certified Public Accountants, *WebTrust Principles and Criteria*, Version 2, October 1999, http://webtrust.org/princritb.htm.

[3] Bhimani, Anish, "Securing the Commercial Internet," *Communications of the ACM*, 39(6), June, 1996, pp. 29-35.

[4] Friedman, B., Kahn, P.H., Jr., and Howe, D.C. "Trust Online," *Communications of the ACM*, 43(12), December 2000, p. 34-40.

[5] Gray, G. and Debreceny, R. "The Electronic Frontier," *Journal of Accountancy*, May, 1998, pp. 32 - 38.

[6] Koreto, "WebTrust: A New Approach to E-Commerce," Journal of Accountancy, May 1998, p. 38.

[7] Patterson, T., "Establishing Electronic Commerce via Certificate Authorities," http://www.se-com.com/secom/wp/cyberguard-ecom.html

[8] Rittenberg, Larry J. and Bradley J. Schweiger, *Auditing*, Harcourt, Brace, & Company, 1999

[9] VeriSign, "VeriSign Secure Server IDs for the WebTrust Program", 1999, http://www.verisign.com/webtrust/siteindex.html