Electronic Commerce Assurance

The Special Committee on Assurance Services identified Electronic Commerce Assurance as an assurance service CPAs can provide. To consider whether you want to provide this service, you can read this service description.

Background

The First Wave - EDI. Doing business electronically became a way of life for certain companies in the 1980s. Many larger companies required their vendors to use electronic data interchange (EDI) to place orders, notify them of shipments and send invoices.

As the use of EDI grew, standards began to develop into a full body of standards, known as ANSI X12. This allowed vendors to deal with their customers using common electronic transaction formats. ANSI X12 is widely used by many organizations, but the standard is ignored by some industry giants such as WalMart and Kmart. The most powerful player in the distribution chain often dictates the standard for all of its vendor and customer relationships. This means that at least some of the participants in the distribution chain must accommodate multiple EDI systems mandated by their more powerful business partners.

This trend also helped grow a new service business called value added networks (VANs), which specialized in receiving electronic transactions, translating them to/from ANSI X12 or other proprietary formats if needed, transmitting them to the intended recipient, and providing acknowledgment of receipt to the sender.

Although the use of EDI was driven by large companies, many smaller suppliers, transportation companies, and banks rapidly adopted it. EDI has enabled many companies to achieve business efficiencies through the use of techniques like just-in-time inventory management, rapid response to changing customer buying patterns, and lower cost through the elimination of paper and its related processing activities. Microcomputer software has enabled smaller organizations to participate fully in the use of EDI. Some organizations have used EDI as a technology enabler to completely reengineer how they do business.

For purposes of this discussion, EDI refers to inter-company execution of transactions electronically and substantially without supporting paper documentation. Examples of EDI include:

- Electronic linkage between manufacturers, wholesalers, and retailers which allows retailers' computer systems to order and release goods from manufacturers' or wholesalers' inventories and make direct electronic funds transfers to the sellers' accounts without paper-based purchase orders, receiving reports, or invoices.
- Electronic claims filing, processing, and payment systems between primary and secondary health care providers and third-party payers.

In more advanced EDI systems, retailers may be able to directly examine or adjust manufacturers' production schedules to effect the timely delivery of the desired goods. EDI systems are increasingly common in manufacturing, retailing, wholesale distribution, healthcare, financial institutions, and investments.

Electronic commerce is a broader term and may involve individual consumers as well as small and large companies engaging in a variety of transactions electronically without paper documents.

The Second Wave - Increased Breadth of Transactions and Diversity of Users. The second wave of electronic commerce is now upon us. During this wave, we will see many more types of electronic transactions and a volume of business conducted electronically. This wave already includes retail
consumers who use it for electronic shopping. The second wave also involves a broad range of banking and financial transactions, and expanding network services, such as the Internet.

As businesses move toward paperless systems and electronic commerce, the number and types of electronic transactions and documents will explode dramatically. However, electronic transactions and documents can be easily altered, deleted, and duplicated. This attribute may cause the integrity of electronic transactions and documents to be later questioned, causing disputes regarding the terms of a transaction, such as a purchase, or the content of the document, such as a contract.

The anonymity of electronic commerce makes it crucial that people know with whom they are doing business. Without this assurance, the authenticity of the transaction may be questioned, fraud might occur, and payments for certain transactions might be lost or diverted. In the first wave, traditional EDI transactions were typically conducted between parties who were acknowledged business partners and are usually covered by an overall contract specifying key transaction and dispute-resolution principles. However the second wave often involves transactions between virtual strangers conducted over an unsecured network, such as the Internet. The potential for fraud, dispute, and other business risks in this new environment obviously is much greater.

The growth of electronic commerce requires the reduction or elimination of the barriers that companies normally employ to bar unauthorized outside access to critical company information and resources. Literally hundreds of persons outside of the company may be able to authorize or influence changes in production levels, shipments of goods, and funds transfers. The promise of electronic commerce is best fulfilled through the relatively unrestricted flow of information and decentralization of authority. The new system of commerce requires new concepts of control, authorization, confidentiality, and anonymity.

This suggests new markets for CPAs to provide assurance and other services related to electronic commerce. Participants in electronic commerce will not only require assurance that their own systems are secure, but also that appropriate controls exist in supplier and customer organizations to limit access to authorized users and to protect an organization's confidential information. In addition, the broad use of electronic commerce introduces the need for new privacy controls.

A Peek at The Third Wave - A New Electronic Society. The third wave of electronic commerce will probably have attributes along the following lines:

- **Ubiquitous** - Virtually all business transactions will be documented electronically.
- **Cashless** - Transactions will be settled electronically using digital cash. This may involve different concepts of money and different roles (or no role) for banks.
- **High Integrity** - The supporting systems must provide high transaction integrity and security or they will not be accepted.
- **Intelligent Agents** - The use of these kinds of tools to automatically search for the best options and execute transactions on behalf of their clients will become widespread.
- **Continuous Testing** - Third Wave systems will allow the CPA to perform continuous testing procedures as transactions are being processed.

**Risks in Electronic Commerce - The Need for Assurance.** The second and third wave growth of electronic commerce will create many abuses and concerns that can be addressed by CPA assurance services. Some of the potential abuses and concerns caused by this new environment include:

- **Intentional attacks** - Hackers and/or competitors may actively attack a system to obtain access to confidential data (such as credit card numbers), impersonate legitimate customers, steal and resell proprietary information, intentionally corrupt information, set-up "back doors" for future passive surveillance of transaction activity, or similar acts.
- **Transmission failures** - As transactions travel through a network, they generally are subject to
numerous processing steps, translations, and store-and-forward processes. These activities introduce risks such as unintentional errors, lost transactions, and duplication of transactions.

- **Lack of authentication** - A fundamental requirement of all commerce (electronic and otherwise) is knowing with whom one is dealing. In paper-based commerce, this requirement is met through the use of letterheads, logos, authorizing signatures, face-to-face contact, and other cues. Electronic messages lack these traditional identifiers and increase the risk that you may unintentionally deal with the wrong party, or deal with someone impersonating another party. The use of public networks heightens this risk substantially.

- **Loss of trust** - The authentication risks may be mitigated through the use of digital signatures and other encryption technology. These technologies often require services of a trusted individual or trusted system to verify that keys and digital signatures actually belong to a designated individual (similar to a notary public function or a securities signature guarantee). There is obvious risk of abuse of this trusted relationship and a related need for assurance regarding the activities of the trustee (organization, individual, system, etc.).

- **Theft of identity** - Without proper authentication techniques, it will be relatively easy for criminals to assume the identity of a party and conduct a variety of transactions in that party's name.

- **Window dressing** - Some of the control and security procedures provided by electronic commerce vendors will be offered primarily to encourage use. They will be viewed as cosmetic marketing-oriented features rather than true controls and might not be seriously adhered to. The markets will require assurance that claimed security and control procedures are being followed religiously.

- **Inappropriate use of individual and organizational profiles** - As more company and individual transactions are processed electronically, it will be possible to accurately and intimately profile individuals and companies based upon the pattern and content of their transactions. There will be a tremendous appetite among commercial enterprises, government agencies, and unscrupulous individuals for this information. There will be both legitimate and illegitimate markets for the collection and resale of this information. Companies and individuals within companies will be tempted to sell information captured in the context of confidentiality. Many companies will claim to have constructed Chinese walls to prevent unauthorized distribution of information. Users will require assurance that effective procedures are in place. The markets will also require generally accepted control and security standards against which vendors can be measured. This may become a mandated service for companies engaged in electronic commerce.

- **Effects of economic pressures** - Third party security and control providers will emerge to provide confidential, secure, verified, encrypted intermediary services to electronic commerce vendors. Their stock in trade will be the protections they provide to users. This will become a competitive service area very quickly, and cost will be a driving force in determining the market winners. Cost containment increases the risk that control and security will be short changed, which leads to the need for assurance by the customers and transaction originators who rely on these services.

Various players in the electronic commerce arena can benefit from additional assurance regarding these kinds of risks. The current EDI software providers, and organizations that use it, are currently candidates for controls and security assurance services. As electronic commerce extends to retail consumers, this area will grow in importance and the market for assurance will grow accordingly.

**Overview of Potential New CPA Services**

**Nature and Benefits of the Service.** CPAs can provide a valuable service by helping to address the risks and promoting the integrity and security of electronic transactions, electronic documents, and the supporting systems. The CPA would provide assurance to electronic commerce participants that the electronic commerce service providers and the tools and systems in use are functioning in accordance with accepted criteria for electronic commerce integrity and security. This would be similar to today's attest engagement regarding management's assertions that its internal control
structure conforms with COSO.

*Integrity services* provide assurance that (1) the elements of a transaction or document are as agreed among the parties and (2) the systems that process and store transactions and documents do not alter those elements.

*Security services* provide assurance that (1) the parties to transactions and documents are authentic and that such transactions and documents are protected from unauthorized disclosure and (2) the systems that support transaction processing and storage provide appropriate authentication and protection.

<table>
<thead>
<tr>
<th>Transactions and documents</th>
<th>Integrity</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elements were as agreed.</td>
<td>Parties are authentic. Transactions and documents are protected.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supporting systems</th>
<th>Integrity</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elements not altered through processing or storage.</td>
<td>Appropriate authentication and protection systems exist.</td>
<td></td>
</tr>
</tbody>
</table>

**Example 1 - The Value-Added Network Service Provider.** In this example, a CPA reviews, evaluates and tests the control, integrity, and security procedures of a value-added network provider and would provide assurance to third parties regarding the provider's compliance with appropriate criteria. This is similar to the service-auditor report concept, set forth in SAS No. 70, *Reports on Processing of Transactions by Service Organizations*, except that: (1) there are no recognized measurement criteria for reporting under SAS No. 70 and (2) a service auditor's report is designed as an auditor-to-auditor communication and is not particularly well suited for a broad range of third parties.

**Example 2 - The Internet Electronic Commerce Software Package.** In this example, the CPA reviews, evaluates and tests the control, integrity and security procedures incorporated into a software package used for electronic commerce and provides assurance to third parties (for example, purchasers and users of the software) regarding compliance with appropriate criteria. For example, Intuit's Quicken software provides electronic banking services. The CPA could test the integrity and security features of this package to provide assurance that only the designated user can initiate transactions against his or her bank account. Netscape’s Internet software provides secure electronic commerce capabilities. The CPA could provide assurance that credit card and other personal information sent over the Internet using this software, is protected from manipulation and disclosure. The CPA's report could be an important feature to software users.

**Example 3 - The Trusted Key and Signature Provider.** Several organizations verify that a particular key to be used for encryption or digital signature actually belongs to the intended party. The CPA could provide assurance that the "trusted provider" follows appropriate procedures in establishing the identity of key holders and provides appropriately secure systems on which to maintain and distribute such keys.

**Example 4 - The Digital Bank Electronic Payment Card.** Several forms of digital electronic payment systems are being developed. Under one system, the user purchases an electronic "smart card" containing payment units that could be used for electronic purchases (such a system has been in use for several years in France to replace coin telephone calls). Visa and Mastercard have recently announced agreement on a standard for protecting electronic credit card transactions. The CPA could provide assurance to the issuers of such cards that they cannot be tampered with and to the users of such cards that the electronic payment systems and transactions are secure.
Other Related Services
There are many additional examples of assurance services that could be provided. There are also high potential consulting and service provider opportunities for CPAs in the electronic commerce marketplace. For example:

- **Consulting services** - Consulting services would be directed toward assisting clients in (1) designing, developing, implementing, and monitoring electronic commerce systems and tools that provide high integrity and security and (2) developing ways to use electronic commerce effectively to achieve business objectives.

- **Electronic commerce service provider** - Rather than provide assurance or consulting services, the CPA could become a provider of electronic commerce services. Examples of these services include:
  1. Directly processing electronic transactions using high-integrity systems (that is, providing a value-added network service).
  2. Obtaining and storing complete copies of the electronic transactions and documents.
  3. Developing and storing a digital signature of electronic transactions and documents that indicates their authenticity and detect alterations.
  4. Providing authentic keys to be used for encryption, or digital signatures, by operating the systems used to generate, process, and maintain such keys (that is, operating a "trusted key server").

Market Considerations

**Potential Customers/Payers.** Electronic commerce assurance services could be provided to any or all parties entering into, or related to, an electronic transaction. For example, any transaction could have parties such as a buyer, a seller, a broker, an agent, a banker, a transaction processor, a network service provider, one or more lawyers, or a transfer or escrow agent. In addition, developers of software (EDI software, Web browsers, Internet security tools) and providers of electronic commerce services are also potential customers.

There are several possible payers for electronic commerce assurance services. They include, at minimum, the companies that may specify an electronic commerce system for use by their vendors or customers as a condition of the business relationship. The party imposing a system on other business entities may wish to have assurance that the specified system contains inherent controls to avoid any liability to its captive users. It also may require independent assurance regarding system integrity and reliability as a source of reassurance to their current or potential vendors/customers. Vendors of electronic commerce systems and services may require independent assurances from CPAs to give credibility to their marketing efforts.

CPA providers of electronic commerce assurance services may arrange non-traditional payment schemes for their services. For example, CPAs might not charge the party mandating the use of an EDI or other electronic commerce system. They might be paid a fee by the software vendor/installer for each customer who agrees to use the system. Or, the CPA might receive a variable fee based upon the volume of transactions which ultimately pass through the system. Additionally, the CPA might be hired by the system user(s) to provide additional assurance services with respect to controls and security within the users organization relative to the system.

Transaction-based or volume based pricing, rather than the traditional fee-for-service pricing, provides an opportunity for the CPA to price assurance services in relation to the risk being assumed. As in the case of an insurance company where the risk increases with the number of policy holders and the size of policies, the risk in providing electronic commerce assurance is related to the number of third parties assurance is provided to and the related volume of electronic commerce. CPAs could adopt pricing structures for these services that are responsive to the risks involved.
Marketplace Permission. The CPA is uniquely positioned to provide these services. It is a logical extension of the CPA's existing competencies in systems and control environments. Existing client relationships and the CPA's reputation for integrity, confidentiality, and objectivity help ensure access to the parties whose cooperation may be necessary to carry out these engagements. While additional competencies may be required, CPAs may already be the most qualified to offer these services.

Market Size and Growth Potential. There are two primary potential markets for electronic commerce services: retail and commercial.

Retail marketplace - According to Woolford Marketing, an Internet marketing organization:

- Current users of retail electronic commerce (nobody knows for sure): 40 million.
- Projected users in 2000 (from Microsoft, Sun, and others): 500 million worldwide.
- Average age: 35.
- Average household income: $55,000.
- Expected primary Internet use:
  1. shopping.
  2. education and entertainment.
  3. business.

- Primary transaction medium: credit card.

These users might pay for assurance that their transactions will not subject them to financial risk, invasion of privacy, and harassment from unwanted solicitors. At present the average annual credit card fee is $35 and the average credit card annual volume of business is over $1,000. Most individuals have and use more than one credit card. Assume consumers are willing to pay $.50 to $5 per year to assure that the most intimate details of their financial life are not abused and that the commercial environment they use is secure. On this basis the worldwide assurance market for Internet retail is $500 million to $5 billion over the next few years.

Commercial marketplace (U.S.) - It is expected that electronic commerce will eventually become ubiquitous and that a high percentage of business transactions will be carried out electronically. Participating organizations will want assurance regarding the integrity, security, confidentiality, and anonymity of the electronic marketplace. Some pertinent statistics regarding the U.S. portion of this marketplace include:

- Total Business Enterprises > 20 Employees: 440,000.
- Total Business Enterprises < 20 Employees: 4,500,000.
- Gross Domestic Product: $7 trillion.

The foregoing excludes governmental enterprises which could also be major users of assurance services. Assuming that virtually all businesses with over 20 employees and 50 percent of businesses with under 20 employees will become involved in electronic commerce yields about 2,500,000 users representing more than 80 percent of the country's GDP. If these enterprises are willing to pay an average of $50 to $250 a year for the integrity of their electronic marketplace, then the market is worth $1.25 to $6.25 billion.

Competition. Other providers have begun to enter this market. But no one dominates it or has developed a set of measurement standards that are universally accepted.

Why CPAs Should Provide This Service
CPAs provide the objectivity and integrity needed for this kind of service. Others might be able to
provide the technology, skills, and the investment; but when independent assurance is needed or when disputes arise, the CPA profession's ethical standards and traditions should be very valuable to the parties involved. Access to existing clients and knowledge of their systems and integrity assurance needs would most likely create an initial marketing advantage.

CPAs may have a head start on other possible competitors because of the focus on internal controls in the historical financial statement audit. The competencies required for control assessment relative to historical financial statements are much the same as those required for the integrity and security control assurance service. There is a natural extension of these into the transaction-related and other electronic commerce assurance services described above. While many CPAs lack the computer literacy and related tools necessary to perform these services, most nonCPA competitors lack the CPA’s knowledge of internal controls and assessment techniques.

**Competency Considerations**

**Application of Current Skills and Knowledge.** CPAs have the ethical standards and principles needed to ensure the integrity of electronic transactions and documents. They have skills in evaluating evidence, planning the extent of validation as a function of the effectiveness of the system of internal controls, and reporting to third parties on the results of their work.

**New Skills and Knowledge Required.** CPA firms wishing to offer electronic commerce assurance services will require additional competencies. To provide this service at a low cost, automated techniques will be needed. Firms will have to develop or acquire software agents, sensors, and other technology based tools. Some additional skills and knowledge will include information technology and digital communications, encryption and digital-signature principles, and high-volume information storage and retrieval.

Smaller practitioners may offer services to their clients who are required to use one or more EDI systems to satisfy mandating vendors or customers. Because many small practitioner clients will need to use multiple EDI systems, a single firm will not be able to provide significant assurance services to everyone in the information chain. This will have the effect of requiring special skills provided by niche players for each EDI system. EDI segments of the electronic commerce assurance market should therefore become available to any firm that is willing to develop the competencies necessary to deliver the service.

**Initial Investments (Other than New Skills and Knowledge).** The CPA providing certain of these services (for example, those involving continuous testing) will probably have to invest in hardware, network connections, and software applications. These resources will need to be highly secure and ensure high-integrity processing on a 24-hour basis. This technology infrastructure is likely to involve a high initial investment and continuing investments for maintenance and upgrades.

**AICPA Actions Needed to Initiate and Support This Service**
The AICPA has established a [service development task force](#) to further develop this service. Its efforts include:

- Developing measurement criteria for use in this service - Criteria for Integrity and Security over Electronic Commerce (CISEC).
- Developing guidance for practitioners who want to provide electronic commerce assurance.