

eFraud in Online Commerce: Impact on Business Reputation & Consumer Confidence

Kerry G. (Kwasi) Holman

President, Prince Georges County Economic Dev. Corp.

**1st Annual Web Services Security
Conference**

College Park, Maryland

May 25 – 26, 2006

Abstract

- The scope and target of Internet fraud in online commerce has seen an exponential growth in recent time. For this, there are unexpected consequences – which are not clearly discernable.
- By their basic nature, Internet fraud involves the use of the Internet as the target or as the means of perpetrating economic crimes of deception.
- Therefore, this keynote will examine the nature and extent of some of the principal types of business Internet fraud with concrete examples. The keynote will also highlight the impact on business reputation and consumer confidence.

Forms of eFraud

- Internet fraud manifest in several forms.
- Generally, they involve the Internet as the target or as the means of perpetrating economic crimes of deception.

Forms of eFraud Cont.

- Most frauds involving business transactions carried out on the **Internet** relate to misleading and deceptive practices which mirror similar activities conducted using traditional paper-based techniques.
- On the **Internet**, however, fraudsters now enjoy direct access to millions of prospective victims around the world, instantaneously, and at minimal cost.
- Examples include so-called advance fee schemes, such as pyramid and Ponzi schemes, the use of chain letters and bulk electronic mail, business opportunity schemes, and fraudulent online auctions, prizes and lotteries.
- Even the endemic West African advance fee letter scams are now being conducted electronically (Smith, Holmes, and Kaufmann 1999).

Forms of eFraud Cont.

- **Online Funds Transfer Fraud**
- The **Internet** may also be used in connection with the commission of various forms of theft of funds electronically.
- Sometimes, security information such as passwords and account details can be obtained by gaining access to databases held by businesses or financial institutions.
- On other occasions, insiders may move funds electronically by sending instructions via electronic mail.
- When the use of electronic commerce becomes more widespread, abuses relating to the transfer of funds electronically can be expected to increase.
- In one case, for example, two individuals who worked for a computer training company, Aptech, in India, allegedly sent electronic mail messages in the name of Microsoft and Videsh Sanchar Nigam (India's overseas telephone service provider) that contained an attachment which, when opened, sent messages back to the accused containing passwords and other data from the State Bank of India.
- Both were arrested and charged under India's *Information Technology Act 2000* with hacking which carries a maximum penalty of three years' imprisonment and 200,000 rupees fine (US\$4,300)(Bloomberg News 2001).

Forms of eFraud Cont.

Securities and Investment Fraud

- The **Internet** is now regularly being used for corporate activities that extend from offering and trading in securities to lodging official documents electronically with regulatory agencies.
- Already instances have begun to emerge of fraudulent conduct involving the sharemarket that have used the **Internet** to disseminate false information in order to attract investors, or to manipulate sharemarkets.
- In 1998, for example, a worldwide clean-up operation, involving the Office of Fair Trading in Britain and its counterparts in 22 other countries, identified 1,159 potential 'get rich quick' schemes being advertised on **Internet** sites (Office of Fair Trading 1998).
- The possibility of insider trading also exists in the digital world of sharetrading in much the same way as in the traditional sharemarket. Already instances have begun to emerge. In Australia, for example, beginning in 1999, a number of small speculative mining companies began to diversify into **Internet**-related activities, hoping to ride the wave of high technology on the Australian and United States stockmarkets. Regulatory authorities observed a surge in stock price and trading volume of these companies *prior to* the announcement of their proposed metamorphosis, and expressed concern about future potential for false and misleading statements in this area (Phillips 1999).

Forms of eFraud Cont.

- **Identity-related Fraud**
- One of the most frequently used strategies to perpetrate **fraud** is the creation of false documents for misrepresenting one's identity. Once a convincing identity has been fraudulently established, it is then possible to steal money or otherwise to act illegally and then to evade detection, investigation and arrest (Smith 1999).
- The technology of the **Internet** makes it relatively simple to disguise one's identity. Electronic mail and **Internet** addresses may be manipulated by including details which are misleading or the source of a message may be made anonymous or changed so that it appears to be coming from another user. Similarly, there is no way of knowing the commercial affiliations of those on the **Internet**. Referees for organizations might, in fact, be individuals employed specifically to indicate their approval of the organization in question.
- It is also possible to choose legitimate-sounding names in order to improve one's credibility or include domain names which are misleading (see Bachner and Jiang 2000). There has recently developed a practice in the United States and Canada, for example, of some organisations adopting domain names containing the names of Australian cities in order to improve their credibility, despite the fact that they have no connection at all with Australia.

Forms of eFraud Cont.

- **Identity-related Fraud Cont.**

- An example of a recent identity theft case that made use of the Internet concerned 200 of America's richest people who were victimized by a 32 year-old New York chef, Abraham Abdallah.
- Abdallah was alleged to have used computers in a public library to obtain millions of dollars from the accounts of billionaires such as George Soros, Steven Spielberg, talk show host Oprah Winfrey, former presidential candidate Ross Perot, George Lucas and Ted Turner.
- Abdallah allegedly obtained information from credit reference companies by forwarding letters, purporting to be from major banks, requesting information. He used answering machines, courier drop-offs and email accounts to discover enough information to take over the electronic identity of his victims.
- He was only detected when he sent an email message to Merrill Lynch pretending to be billionaire Thomas Siebel, asking for US\$10 million to be transferred to an Australian account. Merrill Lynch was concerned that the transfer would overdraw his account and contacted Siebel (Ringin 2000).

Forms of eFraud Cont.

Procurement Fraud

There are considerable savings to be had from organizations carrying out purchasing and procurement activities electronically. Tenders can be widely disseminated and documents downloaded electronically, while contracts can be negotiated and settled more quickly and easily than in pre-electronic times. This should lead to higher levels of openness, trust and cooperation being established between those involved in the procurement process (Department of Public Works and Services, New South Wales 1999).

In Pakistan, for example, the Electronic Government Program aims to generate transparency and savings in procurement costs for the government through the introduction of a complete system of electronic procurement from supplier management and tendering to the award of contracts. A database of suppliers and the latest market prices of items purchased will be maintained. Each department in the government will have access to the system and a database of suppliers and item prices maintained, thus enabling them to select the supplier of choice and the price to generate a purchase order. The system will be linked directly with the government's finance and budget system to ensure that expenditure on government procurement is subject to audit (Pakistan Information Technology Commission 2001).

Forms of eFraud Cont.

Procurement Fraud Cont.

- Electronic procurement, however, carries risks of **fraud** and abuse as internal controls may be removed when new electronic procurement systems are introduced.
- Government agencies are particularly vulnerable in view of the extensive procurement activities in which they engage, and the large sums of money involved.
- In one Australian case, for example, a sub-contractor to a local Council in New South Wales allegedly gained access to the Council's database of tendering information and was able to secure numerous contracts through the use of this information (Bell 2000, p. 31).

Forms of eFraud Cont.

- **Outsourcing Risks**

- Various opportunities also exist for economic crimes to take place in connection with the outsourcing of services, particularly those relating to information technology and data management (Bell 2000).
- The use of Application Service Providers (ASPs) who provide space for the storage of digital information belonging to other entities on a commercial basis, creates risks that the information may be used for fraudulent purposes or sold-on without authority.
- The outsourcing of information technology services generally also creates risks of **fraud** and corruption where contractors abuse the trust that they are given in managing confidential and sensitive data.

Forms of eFraud Cont.

- **Public Sector Fraud**

- As government benefits programs continue to be administered electronically, the opportunities for **fraud** against public sector agencies will increase.
- In Australia, for example, Electronic Benefits Transfer (EBT) systems are being used for the delivery of social security benefits and, unfortunately, have been subject to abuse.
- The system operates on a national scale and assists in the electronic delivery of limited social security benefits in cases previously addressed using the traditional counter cheque. Plastic cards can be used to obtain cash from ATMs by authorized recipients.
- In Australia a number of prosecutions have taken place in respect of internal **fraud** carried out by government employees fraudulently using the EBT computer system in December 1997 and January 1998. EBT cards were issued in fictitious names enabling the offenders to obtain cash at ATMs. In one case, the proceeds of the **fraud** were used to purchase heroin in the same street as the location of the ATM and within 10 minutes of the **fraud** occurring (Warton 1999).

Forms of eFraud Cont.

- **Others:**
- **Theft of Services/Non-provision of Services:** As with other types of telecommunications, it is possible to steal **Internet-** related services by entering into a contract with an ISP and a telecommunications carrier, and then failing to pay for the services provided.
- **Information Piracy:** The **Internet** can also be used to make illegal copies of data in breach of copyright laws.
- **Page Jacking:** Page jacking involves the appropriation of web site descriptions, key words, or meta-tags from other sites. Page-jackers insert these items into their own sites in an attempt to draw individuals to a particular site. The victim is then able to be defrauded in various ways, sometimes by having modem connections re-directed to international premium paid numbers, such as the Moldovan scam referred to above.
- **Digital Extortion:** The **Internet** is also being used to carry out acts of criminal extortion which, although on the borderline of **Internet fraud**, can have substantial consequences for individual businesses. In one case, two individuals from Kazakhstan were arrested in London on 20 August 2000, for allegedly having broken into the computer network of Bloomberg LP, in Manhattan, in an attempt to extort money from the company.

RISKS Inherent in Fraudulent Online Business Practices

Although **Internet**-based technologies can greatly enhance the speed and efficiency of business transactions, they also create new business risks.

Often the speed with which online transactions take place facilitates acts of **fraud** as there may be no 'cooling-off' period during which the parties to transactions can reflect on the terms of a proposed agreement and obtain verifying evidence about the subject matter or identity of the other contracting party.

Sometimes, necessary internal controls that are designed to prevent **fraud**, may not operate in the case of **Internet** transactions, in which agreements may be struck and payments made instantaneously.

RISKS Inherent in Fraudulent Online Business Practices Cont.

- In addition, electronic transactions entail a loss of collateral information about those involved, such as key social and business cues that are used to establish trust in commercial transactions.
- These include appearance, facial expression, body language, voice, dress, and demeanor which may all not be apparent when one transacts business online.
- The absence of such cues greatly enhances the ability of fraudsters to disguise their true identities or to make use of other people's identities which is often an essential precursor to committing a crime.
- The development of effective user authentication technologies may provide a solution to this problem.

RISKS Inherent in Fraudulent Online Business Practices Cont.

- A related risk concerns the theft of personal information from databases which can then be used to commit **fraud**.
- Organizations that engage in electronic transactions maintain extensive databases of personal information including names, addresses, bank account and credit card details, as well as detailed personal information relating to patterns of purchasing which can be used for marketing purposes.
- Where such information is not held securely, considerable opportunities arise for fraudsters, not only in misusing identities but also in being able to target victims more easily and extensively.

RISKS Inherent in Fraudulent Online Business Practices Cont.

- Electronic commerce may also involve parties located in different countries.
- While this simply replicates the traditional risks associated with international trade, in the case of online transactions it may be more difficult to identify and to locate the offending party, and even more difficult to mobilize law enforcement agencies to take action.

RISKS Inherent in Fraudulent Online Business Practices Cont.

- A further problem associated with conducting business transactions online relates to the use of encryption.
- Although useful in order to protect confidentiality of legitimate information, the use of encryption makes it difficult or, on occasions, impossible for law enforcement and other official agencies to read the communications in question.
- This has already occurred in the international investigation conducted into the 'W0nderland' group in which those involved in distributing child pornography used heavy encryption to prevent law enforcement officers from obtaining evidence (the number '0' in its name also prevented inadvertent users of the **Internet** from stumbling across the group when searching the **Internet**). In business contexts, there is a risk that individuals could encrypt important communications and then refuse to decrypt them unless a fee were paid.

Impact on Business Reputation and Consumer Confidence

- Cases of **Internet fraud** directed at consumers occasionally result in prosecution and punishment by the courts, although the sentences given are sometimes relatively low.

Impact on Business Reputation and Consumer Confidence Cont.

- Some potential consumers or business clients are hesitant to engage in e-commerce due to eFraud in Online Commerce
- May present serious concerns and significant deterrents to the public's use of e-commerce.

Impact on Business Reputation and Consumer Confidence Cont.

- Major impact on business reputation is negative perception of those businesses that have been associated with fraud.
- Consequences include:
 - Loss of business
 - Loss of trust
 - Potential litigations
 - Government imposed sanctions including fines
 - Closure of business

Impact on Business Reputation and Consumer Confidence Cont.

- Major impact on consumer confidence is disastrous
- Consumer loss of confidence on any business has lots of consequences including boycotts which ultimately leads to business loss.

Challenge

- The challenge is for Web services product developers to implement security measures in the products that enable or drive online transactions; and
- For vendors to verify the security of Web services in a manner that is very reassuring to consumers

Conclusion

- The conclusion is that the growth of e-Commerce is directly related to secured Web services and as result;
- Web services security holds the key to the prosperity of online transactions; and
- More and more people will enlist online transaction activities when appropriate safeguards are place.