Fraud & Electronic Commerce

Academic paper by Peter John Lynch (PJL) of Lynch Investigations & Countermeasures Pty Ltd.

Grad. Cert. Fraud Investigations (CSU)
Adv. Dip. Gov Fraud Control Management
Adv. Dip. Security Risk Management
www.pjlinvestigations.com.au

Electronic Commerce has certainly automated the way in which every public sector, commercial entity and individuals do business with each other. The need for efficient and effective pathways of financial transactions allows for exploitation of the new and emerging technologies that deliver products and services.

Opportunities for fraudulent behavior are emerging daily for those seeking to behave dishonestly.

There are needs to establish awareness of identity theft and to introduce the correct controls within this rapidly developing deceptive environment.

The main players being, financial institutions, public sector, commercial business and individuals all use the technological environment to fulfill their business relationships with each other.

The weaknesses within the business environment can be seen, especially the areas of greatest fraud risk, where the risk is originating as well as how it can be prevented and controlled.

But in order to manage risk we must be able to track it and understand it, so let's look at the source of weaknesses and the need for policy, procedural necessity and technological development controlling financial services fraud.

Walker 1997 cited in Chapman & Smith 2001, p.2, '1997 it was estimated the cost of fraud and misappropriation in Australia was between $3 billion and $3.5 billion per annum.'

KPMG 1999, P.8 cited in Chapman & Smith 2001, p.2, 'in 1997, 59% of the 37 respondents from the financial sector to an Australian fraud survey conducted by KPMG, reported experiencing fraud in the past two year period.'

Ernst & Young 2000 cited in Chapman & Smith 2001, p.2. 'In 2000 more than 50 fraud incidents in the last twelve months had occurred on Australian bankers in comparison to 14% of bankers from all companies surveyed internationally (Ernst and Young 2000). Three of these frauds involving more than 25 million dollars each' (Ernst and Young 2000).

The introduction of credit cards and debit cards has been used in an increasing market place and has assisted in new forms of fraudulent transactions occurring.

Lost and stolen cards have facilitated in the extraction of personal banking information and have assisted in production of fake cards being produced.

Turnover of staff in financial institutions has allowed intelligence leakage; the availability of information on the Internet about financial systems weaknesses in products and services has facilitated fraudulent activities.

Technology becoming available to the public such as skimming devices placed over magnetic card readers on ATM's allowed for personal banking information to be extracted to gain access to these accounts by fake credit card production.

Covertly sealed cameras are hidden on the ATM's above the PIN keyboard allowing wireless transmissions of video images of the keyboard and PIN sequence to be transmitted to a receiver/recorder.

The skimming device is placed over the original card swipe reader on the ATM's that is later removed for viewing of the customer bank card account details from computer, details are held in the credit card skimmers memory, (The Daily Telegraph 2003).

Business documents that are required to be produced for financial transactions are being forged by the use of personal computers, scanners and laser printers to copy signatures of company officials. These have been scanned from annual reports. The documents are then transmitted to the financial institution electronically, resulting in funds being transferred usually offshore making recovery difficult.

A case of *R v Zehir* (1998) Court of Appeal, Supreme Court of Victoria, 'offender used desktop publishing equipment to create 41 birth certificates, 41 student identification cards and counterfeit driver licences containing photographs all in separate names. These were used to open bank accounts throughout Melbourne. Cheques were paid into accounts as wages; withdrawals were made from these accounts before cheques were cleared. The false identification was also used to register a business name, to obtain sales tax refunds and to defraud retailers.'

ANAO 1999 cited in Chapman & Smith 2001, p.5. 'Australia counted at the last census an estimated 185,000 potential duplicate records of individual taxpayers present among 17.1 million. This situation allowing fraud against government, especially benefits fraud by offenders of Centrelink office of income support. The authorities have identified false birth certificates used in gaining government funds by deception.'

Computer technologies will greatly enhance the ability of people to defraud governments, private business, individuals and entities enabling transfer of funds illegally. This would increase if this issue is left unresolved. It will cause much greater injury to the members of the community, government and corporations, much more than it has in the past with criminals becoming much wiser to the weak areas of electronic commerce. An increase in their ability to penetrate viable areas of the system will occur.

More intrusions to computers by remote access would increase with the advances in wireless technology. As a result I can see greater opportunities for unauthorised access to copy data and programs aiding in further false identities being produced to assist in fraudulent activity, such as setting up false bank accounts, production of driver licences, birth certificates and businesses certificates.

This aids in defrauding HIC, ATO, banks, government agencies and the private sector enterprise.

With the use of electronic processing of claims also increasing, by the use of computer technologies, it would also be recognised that electronic claim forms would be electronically counterfeited increasing fraud by signature. This can allow electronic funds transfer being altered or diverted from legitimate recipients.

With the ability of government employees to access sensitive information through the course of their employment, I think greater risks to national defence would have to be considered in looking at the September 11 outcome.

Employees of government can gain great financial benefit through espionage and selling of information. With this concern and ongoing terrorism increasing around our country with increased immigration, insecurities of national defence would increase.

Internet crime involving banking fraud through non-delivery of goods or payment with fake or false credit details, I think will increase due to low levels of regulation on transactions.

False information provided by the Internet would increase aiding interested parties to manipulate share markets. Copyright pirate is expected to increase without prosecutions increasing.

The ability of companies in illegal production of music, films and products for markets is growing. This area will flood the country with poor quality products with damage to competitive producers of the patented copyright protected products.

If electronic commerce is allowed to stay as insecure as its introduction and past development, it may be seen by organisations better to revert back to paper based transactions as opposed to electronic forms. I see this to be a consideration for everyone involved without some forward strategic risk management and planning in the fraud control management process in electronic commerce.

References

Commonwealth of Australia 2002, *Style manual for authors, editors & printers,* 6th edn, rev. Snooks & Co, John Wiley, Australia.

Confederation of Asian and Pacific Accountants 2001, *The nature and extent of Internet fraud, Controlling fraud on the Internet,* pp.41-63, viewed 20 March, 2004, www.capa.com.my/article.cfm?id=1

Parliament of Victoria, Drugs and Crime Prevention Committee 2002, *Inquiry into Fraud and Electronic Commerce: Emerging Trends and Best Practice Responses, Discussion Paper,* Parliament of Victoria, Melbourne.

Grabosky, PN Smith, RG & Dempsey, G 2001, *Defrauding governments electronically, in Electronic Theft: Unlawful acquisition in cyberspace,* Cambridge University Press, Cambridge UK, pp. 51-69.

Grabosky, PN Smith, RG 1996, Fraud: *An Overview of Current and Emerging Risks,* Trends & Issues in Crime and Criminal Justice*,* no. 62, Australian Institute of Criminology, Canberra.

Bibliography

Australian Institute of Criminology & PricewaterhouseCoopers 2003, *Serious Fraud in Australia and New Zealand, Research & Public Policy Series,* no. 48, Australian Institute of Criminology, Canberra.

Australian Federal Police 2001, *Model Criminal Code Computer Offences,* no. 21 posted April 2001.

Australian Federal Police 2001, *Timely Relevant & Cooperative Resources for e-Crime Investigators,* no. 22 posted July 2001.

Fraud International (2003-2004) Publisher Phil Peart, Raleigh NC USA.

Larmour, P & Wolanin, N (eds) 2001, *Corruption & Anti Corruption,* Asia Pacific Press & Australian Institute of Criminology, Canberra.

Roberts, P 2003, *Fraud Prevention,* Faculty of Arts study guide JST412, Charles Sturt University, Albury-Bathurst-Wagga Wagga NSW Australia.

Smith, RG 1999, *Electronic Medicare Fraud: Current & Future Risks,* Trends & Issues in Crime & Criminal Justice, no.114, Australian Institute Of Criminology, Canberra.

Smith, RG 1999, *Identity Related Economic Crime: Risks & Countermeasures,* Trends & Issues in Crime & Criminal Justice, no.129, Australian Institute of Criminology, Canberra.

Smith, RG 1999, *Organisations as Victims of Fraud and How They Deal With It,* Trends & Issues in Crime & Criminal Justice, no. 127, Australian Institute of Criminology, Canberra.

Smith, RG 1997, *Plastic Card Fraud,* Trends & Issues in Crime & Criminal Justice, no. 71, Australian Institute of Criminology, Canberra.

Tandukar, A 2004, *Embezzlers Quick off The Mark,* Fraud International, issue 20, pp 34-36.

Yuka, S & Smith, RG 2003, *Identifying & Responding to Risks of Serious Fraud in Australia & New Zealand,* Trends & Issues in Crime & Criminal Justice, no.270, Australian Institute of Criminology & PricewaterhouseCoopers, Canberra.

Law Reports & Case

R v Zehir (1998) CA, SC, VIC.