Identifying and Responding to Electronic Fraud Risks

30th Australasian Registrars' Conference
Canberra
November 13, 2002

Adam Graycar
and
Russell Smith

Australian Institute of Criminology
GPO Box 2944, Canberra 2601
phone: 02 6260 9205
fax: 02 6260 9203
e-mail: adam.graycar@aic.gov.au

Fraud involves the use of dishonest or deceitful conduct in order to obtain some unjust advantage over someone else. Fraud currently costs the community in excess of $3.5 billion, and last year alone cost the Commonwealth Government over $150 million. It costs big business megabucks, though the dollar value is hard to ascertain. Its not just big business and government - at the Australian Institute of Criminology we are ready to release data from a study of crime against small business, which shows that fraud costs small business more in dollar terms than employee theft, burglary, armed robbery, unarmed robbery, and vandalism.

Defrauding land titles systems impacts upon us all. Those who deal in land include ordinary citizens, big business, small business, governments, not-for-profit organisations, deceased estates, etc etc. Fraud here touches almost everybody.

The prevention and control of fraud are two of the great challenges for Australia now, and in years to come.

It has been around for as long as people have been around - somebody trying to con somebody else, to offer them an unbelievable and unattainable deal, or to work the system unlawfully to their own advantage so that things come incredibly easily. While crimes of deception are well-established in history, technological, social, demographic and economic developments have brought about changes in the form fraud takes and how it is perpetrated.

The circumstances in which fraud can exist are enormously diverse. Some of the types include: commercial fraud, fraud against governments, consumer fraud, migration fraud, securities fraud, superannuation fraud, intellectual property fraud, computer and telecommunications fraud, insurance fraud, plastic card fraud, art fraud, charitable contribution fraud, identity-related fraud, advance fee fraud, health care fraud, the list goes on and on, and new opportunities for deceptive conduct arise all the time.

The basic motivation for fraud is greed, a fairly robust and enduring human characteristic. We are unlikely to eliminate greed in my lifetime or yours, so countermeasures have to be more than psychological or feel good tactics.

Crime follows opportunity, and opportunities for fraud flow from economic growth. The more commerce there is, the more opportunities there are to commit fraud. Nobody wants to pull the plug on electronic commerce, close down the stock market, or the health insurance system, just because they may be vulnerable to fraud.

The area of concern closest to your interests relates to the opportunities for fraud that arise out of electronic service delivery by Land Registries. In the past, sophisticated paper-based systems were present to reduce the opportunities for fraud involving conveyancing transactions. As we move into on-line registration of titles and electronic transactions, new opportunities arise for people within organisations as well as for external customers to misrepresent themselves and to manipulate electronic transactions for financial gain. I'll come back to these risks shortly.

The challenge lies in designing systems which allow commerce to flourish while blocking opportunities for fraud. This challenges us to extend our ingenuity to counter that of villains, and to build smart systems.

Like all crimes, fraud is the product of 3 factors

- Motivation - somebody willing to offend
- The presence of a prospective victim or target
- The absence of a capable guardian

This general rule applies whether we are referring to fraud against a government benefits program, fraud against elderly people, fraud against your organisation, or misappropriation of corporate assets by a company Director.

Three ways to work on the limitation of fraud involve:
- Reducing the supply of motivated offenders
- Protecting and educating the suitable targets
- Limiting opportunities by making the crime more difficult to commit

I am not going, this morning, to be able to go through the whole gamut of fraud, so I'll focus only on 3 types of examples that raise issues relevant to electronic conveyancing: *Electronic Funds Transfer Crime; Identity-Related Crime; On-line Sharemarket Manipulation.* The techniques that have been used to commit fraud in these areas are exactly the same as those that could be used to attack the Offices of Titles around the country.

While fraud has been around forever, the common thread running through most of the current wave of economic crimes is that they are greatly facilitated by recent developments in information technology.

The benefits of computing and communications technologies are clearly apparent.

People are able to communicate more effectively and at lower cost than in the past. It has also meant that geographical boundaries are able to be crossed more easily which has enhanced the process of globalisation of economic and social life enormously.

These same technologies that have provided so many benefits have, however, created enormous opportunities for offenders—

Criminals are able:
- to communicate with each other in secret,
- to disguise their identities in order to avoid detection,
- to counterfeit and alter documents using desk-top publishing equipment; and
- to manipulate electronic payment systems to obtain funds illegally.

They are also able to perpetrate fraud on a much wider scale than in the past, duplicating countless fraudulent invoices, or establishing large numbers of accounts that only exist in cyberspace. Their victims may also be located anywhere in the world.

Electronic Funds Transfer Crime

All companies and organisations move money electronically. In the old days, law clerks would stand in line at the Titles Office and hand a piece of paper over to an officer at the counter who probably knew the person by sight, and if there was an anomaly, it would be picked up by the official who just knew!

Crime today takes place by manipulating the security systems established to protect electronic funds transfers. These systems are designed to ensure that information cannot be manipulated as it passes over computerised networks and that only authorised users have access to computers. Law clerks of the future will spend their time in the office in front of a screen rather than physically walking to the Titles Office to lodge documents and to pay fees.

Most of the large scale electronic funds transfer frauds which have been committed in the past have involved the interception or alteration of electronic data messages transmitted from the computers of financial institutions.

In many cases offenders have worked within financial institutions or corporations themselves and been privy to the operation of the security systems in question.

One recent example of funds transfer fraud involved a financial consultant contracted to the Department of Finance and Administration in Canberra who, on 25 September 2001 was convicted of defrauding the Commonwealth by transferring A$8,735,692 electronically to private companies in which he held an interest. He did this by logging on to the Department's computer network using another person's name and password. He also was able to obscure an audit trial by the use of other employees' logon codes and passwords. He was sentenced in the ACT Supreme Court to 7 ½ years imprisonment.

Could this sort of thing happen in your organisation?

Identity-Related Crime

In the old days bushrangers and outlaws used masks to cover their faces so nobody would know who they are. Today, on the internet, nobody really knows who you are.

One of the most frequently used strategies to perpetrate crime is the creation of false documents used to misrepresent one's identity. Once a convincing identity has been fraudulently established, it is then possible to defraud organisations, steal funds and then to evade detection, investigation, and arrest.

Stealing identities, or creating false identities, pervades every aspect of our life.

At the benefit concert in New York to raise money for families of the emergency services victims killed in the World Trade Centre attacks, the legendary British rock group The Who brought the audience to their feet with a rousing rendition of their classic song "Who are you". At the time however, neither the band nor the audience, were aware of just how significant was the timing of this song. Even as it was played, the FBI were busy with the

added burden of a new and rapidly escalating economic crime directly related to the New York tragedy.

Within days of the appearance of lists of those missing – or presumed missing – in the rubble of Manhattan, hundreds of millions of dollars of goods and services were being illegally obtained by people who had adopted the identities of the victims. Such was the outpouring of public sympathy that people were literally able to walk in off the street into government offices, shops and banks, report that their usual documentation was lost in the rubble, and on the production of the flimsiest of identification, obtain documentation like real driver's licences, which in turn were then used to obtain other genuine documents.

From here, it was only a short step to illegally obtaining goods and services, such as opening up lines of credit large enough to drive away in brand new and expensive cars. False identity was also an issue on September 11 in that nobody knew for a long time who it was who was flying those planes, how they got into the country etc etc.

This example is grotesque under the circumstances but it highlights in graphic detail a problem of identity theft - a crime which is the boom crime of our times.

The risks of identity-related fraud associated with electronic conveyancing are great as the most sophisticated security systems that protect data as they are transmitted electronically across telephone lines or via satellites are of little protection if someone simply adopts a false identity, perpetrates a fraud and then is unable to be located by the police. Obtaining cryptographic key pairs for use in a Public Key system that Titles Offices of the future will use, by presenting false proof of identity documents, would be the easiest way in which to perpetrate conveyancing fraud in the future.

Similarly, if internal staff use other people's passwords to enter networks to which they do not have authorisation, this may create enormous opportunities for fraud to occur.

Finally, there is the possibility that staff within Registries may be subject to bribery or duress by individuals seeking to gain access to secure systems. In this way, security systems can be overcome by resorting to the potential for corruption from within agencies.

On-line Sharemarket Manipulation

An illustration of the risks that on-line service delivery can entail is electronic share trading. The use of computers and E-mail has greatly facilitated the manipulation of share markets during secondary trading of securities. This can occur through the use of rumour, hyperbole, or other forms of misinformation to boost the price of a stock prior to the manipulator's quick and profitable exit ('pump and dump'), or by talks down a stock so that he or she may buy in at a bargain price ('slur and slurp').

In a recent Australian prosecution, a 24 year-old man who lived in a Melbourne suburb, manipulated the share price of an American company by posting information on the Internet and sending E-mail messages around the globe that contained false and misleading information about the company. On 8 and 9 May 1999, he posted messages on Internet Bulletin Boards in the United States and sent more than four million unsolicited E-mail

messages to recipients in the United States, Australia and in other parts of the world. The messages contained a statement that share value of the company would increase from the then current price of US$0.33 to US$3.00 once pending patents were released by the company, and that the price would increase up to 900 per cent within the next few months. The effect of the information was that the company's share price on the NASDAQ doubled, with trading volume increasing by more than ten times the previous month's average trading volume.

The offender had purchased 65,500 shares in the company through a stock broking firm in Canada several days before he transmitted the information. He sold the shares on the first trading day after the transmission of the information and realised a profit of approximately A$17,000. The offender was prosecuted by the Australian Securities and Investments Commission for distributing false and misleading information with the intention of inducing investors to purchase the company's stock. He pleaded guilty and was sentenced to two years' imprisonment on each of three counts, to be served concurrently. The Court ordered that twenty-one months of the sentence be suspended upon his entering into a two-year good behaviour bond with a surety of $500.

These are only some of the types of fraud facing Australian organisations today. Before discussing what to do about it, you have to know that you're being scammed. This is not nearly as obvious as it sounds, and often does not come to light until late in the piece - often too late! There are certainly some risk factors, and some red flags.

Always look for anomalies - in essence, there are three types of anomalies to look out for, behavioural anomalies, statistical anomalies and organisational anomalies.

Behavioural anomalies can be found in people suddenly changing their lifestyles, living beyond their means - they might have come into a lot of money legitimately, but keep an eye out for behavioural anomalies.

Statistical anomalies are when the numbers don't look right, expenses claims out of whack with past patterns, sudden changes in credit card bills, tax deductions out of proportion to income, insurance claims that bear no resemblance to a person's lifestyles etc.

Organisational anomalies are activities which diverge notably from best practice - inadequate systems of communication within the organisation, lack of transparency to outside observers, the absence of financial control systems, the Board of Directors handpicked by the CEO., poor leadership, inflated financial targets, unrealistic incentive structures based on commissions are all risk signals.

The absence of anomalies, however, does not mean the absence of fraud. How, then should corporations respond to these risks?

Let me outline four general preventive strategies:

- Effective Corporate Governance
- Fraud Control Policies
- Personnel Monitoring

- Computer Usage Monitoring

These however are a backdrop to the hard approach - using a range of technologies to prevent corporate fraud, or using the criminal justice system to prosecute and punish offenders.

Effective Corporate Governance

In the first place it is important for those who manage organisations to have a proper understanding of the risks that are present within their organisation. This requires managers to know precisely how their business operates. Often those in charge of companies may not understand how their organisations function in sufficient detail to be fully aware of the risks of fraud that exist. This is particularly the case with respect to information technologies. In Ernst and Young's survey of large organisations, for example, less than one third of the Australian respondents considered that their directors had a good overall understanding of their business for fraud prevention purposes.

Although managers may not be able to understand the technicalities of all the computer software and hardware that their organisation makes use of, they should be in a position to understand the areas where fraud risks arise and instruct appropriately trained personnel to monitor these areas regularly.

Fraud Control Policies

It is also important for organisations to have clear and transparent fraud control policies in place. These are necessary in the digital environment no less so than in the terrestrial world.

Australian Standard No. AS 3806-98 *Compliance Programs* provides guidelines for both private and public sector organisations on the establishment, implementation and management of effective compliance programs. The Standard also provides principles which organisations are able to use to identify and to remedy any deficiencies in their compliance with laws, industry codes and in-house company standards, and to develop processes for continuous improvement in risk management.

Establishing principles on, for example, the ethical use of information technologies and how to respond to instances of fraud are essential in conducting a business of any kind, whether or not it makes use of electronic commerce.

Of particular importance is the need to develop specific policies on computer security along with appropriate guidelines on reporting computer misuse and abuse. Policies need to deal with specific on-line behaviour of employees such as security of user authentication systems (e.g. passwords), access to and use of the computers for private purposes, personal use of electronic mail, downloading software, and the use of copyright material. Principles also need to be established to ensure that those who report illegal conduct are not disadvantaged by their conduct.

Personnel Monitoring

There is also a need for organisations to be confident that the staff they are employing are reliable and trustworthy, as electronic fraud often involves confederates with inside knowledge of a company's security and computer procedures. The administration of

modern technologically-based security systems involves a wide range of personnel—from those engaged in the manufacture of security devices to those who maintain sensitive information concerning passwords and account records. Each has the ability to make use of confidential information or facilities to commit fraud or, what is more likely to occur, to collude with people outside the organisation to perpetrate an offence.
Preventing such activities requires an application of effective risk management procedures which extend from pre-employment screening of staff to regular monitoring of the workplace.

Long-term employees who have acquired considerable knowledge of an organisation's security procedures should be particularly monitored, as it is they who have the greatest knowledge of the opportunities for fraud which exist and the influence to carry them out.

Caution is also needed when internal disputes develop.

A case heard before the New South Wales District Court on 27 March 1998, for example, concerned an unsuccessful applicant for a position with an Internet Service Provider (ISP). When he was refused the job he took revenge by illegally obtaining access to the company's database of credit card holders and publishing details relating to 1,225 cardholders on the Internet as a demonstration of the security weaknesses of the company. As a result, the business lost more than $A2 million and was forced to close its ISP activities.

Risks might also arise with the use of external contractors. As you move toward the implementation of on-line conveyancing, you will need to rely heavily on contractors to develop, install and monitor new systems. Those individuals will have a detailed knowledge of the new systems and how to manipulate them. As such they may be subject to temptations to act illegally, particularly if disputes develop during the period of the contract. Particular care may be needed in ensuring that honest and trustworthy contractors are used in connection with secure systems.

Computer Usage Monitoring
Employees' use of computers and their on-line activities can be monitored through the use of software which logs usage and allows managers to know, for example, whether staff have been using the Internet for non-work-related activities. Ideally, agreed procedures and rules should be established which enable staff to know precisely the extent to which computers are able to be used for private activities, if at all. If staff are permitted to make use of computers for private purposes, then procedures should be in place to protect privacy and confidentiality of communications, subject, of course, to employees obeying the law.

Where certain on-line activities have been prohibited, it is possible to monitor the activities of staff, sometimes covertly such as through video surveillance or checking electronic mail and files transmitted through servers.

Filtering software may also be used to prevent staff from engaging in certain behaviours. 'Surfwatch', for example, can be customised to deny employees access to specified content. When the employee requests a site, the software matches the user's ID with the content allowable for the assigned category, then either loads the requested page, or

advises the user that the request has been denied. The software also logs denied requests for later inspection by management.

The use of computer software to monitor business activities also provides an effective means of detecting fraud and deterring individuals from acting illegally.

The Consequences of Failure to Respond to Fraud within Organisations

Where corporations have experienced electronic fraud, managers are faced with difficult choices as to how they should respond. On the one hand, they may choose to 'exit' the situation — and to dismiss the employee responsible, or cease doing business with the individual who perpetrated the offence.

On the other hand, they may seek legal avenues of redress, either employing civil proceedings to recover compensation or criminal proceedings to punish the offender and to deter others from acting similarly.

Many organisations prefer not to report crime to the authorities. A survey of organisations victimised through fraud conducted by Deakin University found that fraud was not reported officially because the matter was not considered to be serious enough to warrant police attention, a fear of consumer backlash, bad publicity, inadequate proof, and a reluctance to devote time and resources to prosecuting the matter.

The reasons for the reluctance to report fraud are often due to a fear of 'sending good money after bad' as experience may have shown that it will be impossible to recover losses successfully through legal avenues and that the time and resources which are required to report an incident officially and to assist in its prosecution simply do not justify the likely financial returns. Prosecution may entail countless interviews with the police, extensive analysis of financial records, and lengthy involvement in court hearings for staff.

The other disincentive to taking official action lies in the reluctance of organisations to publicise the fact of their victimisation through fear of losing business or damaging their commercial reputation in the marketplace. Government agencies might also believe that adverse publicity may result in a loss of confidence in voters, whilst financial institutions might believe that publicity of security weaknesses might result in acts of repeat victimisation taking place using the same techniques as those being investigated.

Finally, where crime has been committed by those in positions of responsibility within organisations, they may not wish to draw undue attention to their own illegal activities.

Although some of these responses are understandable, failure to take action creates an undesirable atmosphere in the organisation indicating that fraud is tolerated. It may also may result in the offender in question being able to re-offend, either in the same organisation or elsewhere. Failure to report crime also means that new forms of crime do not receive publicity and thus others may be victimised in the same way. Finally, if crime is not reported then it is not possible to gather statistics on the nature and extent of incidents that takes place.

There are no easy fixes!

Conclusions

Fraud is not going to go away. The electronic systems used to conduct commercial transactions are changing rapidly, and considerable effort is being put into ensuring the security of digital transmissions which represent monetary value. The opportunities for fraud are, however, substantial.

The solution to electronic fraud will ultimately involve the adoption of a range of strategies both technological and strategic in which close cooperation will exist between all those involved in providing and using systems. This includes telecommunications carriers and service providers, financial institutions, corporations, and individual users.

Going back to my three opening points, reducing fraud involves

- Reducing the supply of motivated offenders
- Protecting and educating the suitable targets
- Limiting opportunities by making the crime more difficult to commit

⇒ To deal with the first objective, reducing the supply of motivated offenders, is a hard one because there has always been greed, and the traditional crime prevention activities of early intervention are not applicable. People commit fraud without many of the usual risk or predictive factors. We are dealing here with culture and ethics - not something that comes in a five minute pep talk It is here that things like effective corporate governance and ethical standards are central. At the other end of the spectrum, but dealing with the same issue of reducing the supply of motivated offenders, judicial punishments also play a role. Prison, which has few redeeming features, probably works better as a deterrent for fraud offenders than for many others. Similarly, confiscating a fraudster's home or car and requiring ill-gotten gains to be repaid over a lifetime are appropriate sanctions for white collar offenders.

⇒ To deal with the second objective, protecting and educating the targets of fraud is a crucial part of the prevention equation. It involves imparting knowledge and information that will permit the identification of problems immediately they arise as well as a mechanism for keeping new information flowing, at both an individual and organisational level. This goes hand in hand with a fraud control policy.

⇒ Limiting opportunities by making the crime more difficult to commit brings in the other side of the prevention equation, fraud control policies, computer usage monitoring, policing anomalies, corporate governance and professional regulatory procedures. The technologies of crime prevention are also of fundamental importance here.

It all points to careful risk management. Risk management and fraud prevention are clearly preferable to the use of prosecution and punishment.

The prevention and control of fraud are two of the great challenges for Australia in the years to come. Success in dealing with fraud will enhance Australia's business reputation, and reduce the personal hardship that fraud causes to countless victims each year.

Most fraud in the twenty-first century is sophisticated in planning and execution. Fraud prevention also needs to be sophisticated, although, as a recent British Home Office publication notes, it's 'Not Rocket Science'! Some aspects of fraud prevention may involve us in taking basic measures to protect ourselves, such as by using the security measures that modern computing technologies have to offer in a sensible and thoughtful way—and not simply writing one's password on one's deskpad! Other target hardening measures may require elaborate and complex planning in order to thwart the efforts of fraudsters fully trained in the operation and management of electronic business systems.

Managers also need to take personal responsibility for dealing with fraud and for reporting it to the authorities. This will not only help to inculcate an environment of honesty and openness within an organisation, but will enhance deterrent effects for other staff and enable the public generally to understand new areas of risk and security weaknesses. Sweeping fraud under the carpet by dismissing untrustworthy employees, compounds the problem and creates an atmosphere of complacency within organisations. At every available opportunity, a **culture of compliance** needs to be reinforced.

In the end, fraud prevention and control require the concerted efforts of individuals working both within the public and private sectors who make use of the most up-to-date and effective fraud control technologies. When all else fails, an efficient legal system must also exist to detect, investigate, adjudicate, and sanction those who seek to obtain funds dishonestly. There has been considerable progress in each of these aspects already and Australia is at the forefront of many innovative developments in fraud control.

The challenge for the years to come lies in understanding how new forms of fraud are perpetrated and ensuring that those charged with preventing and dealing with fraud have adequate resources to do their work. Although the systems being introduced to facilitate electronic land transactions will entail many efficiencies, they will also, unwittingly, create new opportunities for crime. As in most areas of crime control, it is better to allocate resources in preventing crime than in seeking to deal with the consequences after the problem has arisen.