AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 100

Best Practice in Fraud Prevention

Russell G. Smith

This Trends and Issues paper seeks to distil from a diverse range of sources, the most effective strategies and programs which have been devised throughout the world in recent years to prevent criminal fraud perpetrated against both individuals and organisations. Eight areas are examined: fraud awareness and education; management of fraud control; personnel monitoring; transaction monitoring; improvements in personal identification; counterfeiting prevention; computer systems monitoring; and legally-based deterrence. Each of these strategies and programs relies to varying degrees upon the actions of people as well as technology and, where fully implemented, the benefits in terms of fraud reduction can be dramatic.

Adam Graycar
Director

Fraud is a generic category of crime which involves an individual or group of individuals dishonestly obtaining property or some financial advantage by means of deception. Perpetrators of fraud may seek to gain money, property, time or information and the means used are as varied as are the opportunities which arise. Offenders may be individuals or employees or managers of organisations in both the public and private sectors, while their victims may be their employers as well as individual consumers of any age and gender. Put simply, fraud affects us all and is of particular concern to those who manage large government and business organisations where the potential losses are greatest.

Strategies used to prevent and to control fraud are astoundingly diverse, varying from the most general policy statements designed to ensure the efficient conduct of business organisations, to highly specific information offered to enable people to avoid personal victimisation.

Fraud prevention involves a complex and sensitive process of balancing an organisation's diverse interests and limited resources. Some solutions may be totally effective in terms of reducing fraud but may have the consequence of stifling commerce and making everyday business transactions so unwieldy and costly to manage that no-one would be willing to use them. Fraud prevention should, therefore, aim to maximise crime reduction without imposing unrealistic burdens on legitimate business activity.

This paper identifies eight areas which may be described as "best practice in fraud prevention"; namely, strategies and techniques which have been used successfully in the past to prevent fraud and which have the greatest potential to prevent emerging instances of fraud in the future. The challenge lies not only in identifying and publicising these approaches but also in persuading members of the community to make use of them in both their personal and business lives.

Fraud Awareness and Education

Informing the public of the need to protect PINs and passwords which are used in conjunction with card-based transactions is a

December 1998

ISSN 0817-8542
ISBN 0 642 24089 2

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9200
Fax: 02 6260 9201

For subscription information together with a complete list of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au
or send an email to:
aicpress@aic.gov.au

simple and effective strategy which can have highly beneficial results. In the United Kingdom, one particularly effective plastic card fraud prevention strategy involved a high profile publicity and education campaign by the Association for Payment Clearing Services to raise public awareness of the problem and to encourage card holders to take more care of their cards which was highly successful in reducing plastic card fraud (Webb 1996).

There are also many other practical steps which card users can adopt to detect the possibility of fraud. Some danger signs, for example, include monthly bills not arriving on time, the amount shown on charge slips not corresponding with users' originals, sales assistants being unusually attentive of card details during transactions, renewal cards not arriving on time, double imprinting by cashiers, and sales staff misplacing cards (Grau 1993).

Educating retailers and particularly sales staff about the ways in which fraud may be perpetrated has also been effective, although care is needed to ensure that staff are not alerted to ways in which they may act dishonestly themselves. Conducting close examinations of plastic cards to detect forgeries and looking out for suspicious customers have been recommended by both law enforcement and business organisations (Dyson & McKenzie 1996; Van Leeuwen 1996).

Finally, one of the recent success stories in fraud control has been efforts taken by the insurance industry in Australia which, through the adoption of a range of measures including the use of publicity and education, has reduced estimated losses incurred through fraud and arson from $A1.19 billion in 1994 to $A500 million in 1997 (Insurance Council of Australia 1997).

Management of Fraud Control

Effective Fraud Control Policies

To be effective, fraud prevention policies need to be established and supported by management. Guidelines have been developed by the Commonwealth government in its Fraud Control Competency Standards and by the national body, Standards Australia, in its Standard No. AS 3806-98 *Compliance Programs* (1988) which provide guidelines for both public and private sector organisations on the establishment, implementation and management of effective fraud control and compliance programs.

In recent years, more and more organisations seem to be developing fraud control policies. In the survey of 477 medium and large organisations in Victoria conducted for the Victoria Police by Deakin University in 1994, only 27 per cent had fraud prevention policies in place (Deakin University 1994). In November 1995, the 48 per cent of the 123 Australian respondents to Ernst & Young's fraud survey had a fraud prevention policy in place and 51 per cent had conducted fraud reviews (Ernst & Young 1996). Most recently, in Ernst & Young's 1997 fraud survey, almost three-quarters of the eighty-four Australian respondents indicated that their organisation had an explicit policy on fraud reporting (1998). An example of one of Australia's most thorough and comprehensive fraud control policies in the private sector is BHP's "Guide to business conduct" (1997).

Governments, too, have taken steps to introduce comprehensive fraud control policies. In 1987, the Commonwealth government embarked upon a review of its systems for dealing with fraud and concluded that each agency should have primary responsibility for dealing with fraud, that the emphasis should be on fraud prevention rather than deterrence-based approaches, and that agencies should bear primary responsibility for investigating minor instances of fraud. Procedures were then introduced to implement these reforms which were subsequently evaluated. In 1992, consultants were specifically engaged to examine the Department of Administrative Services (Ernst & Young and Australian Institute of Criminology 1993) and the subsequent report set in train a process of consultation which led to the creation of the current Fraud Control Policy of the Commonwealth.

Monitoring Fraud Control Policies

Following implementation, fraud control policies need to be monitored in order to ensure that they achieve the desired effects. In 1992, for example, the New South Wales Independent Commission Against Corruption examined the cash-handling systems which operated in New South Wales public hospitals and made recommendations aimed at improving cash-handling procedures and controls. Although this review was directed at the prevention of corruption, it also entailed fraud control. A monitoring project was then undertaken to establish the effectiveness of the reforms introduced (*see* New South Wales, Independent Commission Against Corruption 1994).

In another initiative, believed to be a world first, the Australian Payments System Council, which has only recently been dissolved, conducted a review of the security standards evident in retail electronic funds transfer systems in 1990-91. Where shortcomings were revealed, these were followed up at both institution and industry level and more general guidelines published to improve EFT security. The Council also conducted an annual review of the level of compliance with various financial system codes of conduct (Australian Payments System Council 1998).

Personnel Monitoring

Perhaps the greatest risk of fraud to an organisation lies within its personnel. Recent surveys by KPMG (1997) and Ernst & Young (1998) both found that fraud is

most often carried out by employees, particularly at senior management level. 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 collude with people outside the organisation to perpetrate an offence. Preventing such activities requires an application of effective risk management within an organisation in which the comprehensiveness of the strategies adopted are matched with the extent of the risks involved.

Pre-Employment Integrity Screening

In addition to having detailed job application forms and checking references with named as well as independent referees, managers should be trained in interviewing skills in order to ensure that dishonest conduct in a potential employee's past may be identified and an assessment made as to whether or not dishonest behaviour is likely to occur in the future (Sims & Sims 1995).

On-going Monitoring of Integrity

It is essential that personnel be regularly monitored in terms of their risk of behaving fraudulently. There are now extensive lists of "red flags" which are available to assist managers in isolating individuals most likely to be at risk of committing fraud which often include behavioural or social characteristics such as problems with addiction to alcohol or gambling or unusual working patterns. Long-term employees who have acquired considerable knowledge of an organisation's security procedures should also be monitored, particularly where work-related disputes develop or where redundancy may be a possibility.

Finally, employment practices such as regular training, supervision and job rotation assist in fraud minimisation. Having separate control systems in place, such as for purchasing and payment, has also been found to be effective.

Transaction Monitoring

Because computers play such an instrumental role in the operation of modern commercial transactions, they provide an effective means of monitoring what takes place. This is helpful not only in detecting fraud immediately when it occurs, but also in maintaining profiles of normal behaviour as a preventive strategy.

Software to Analyse Normal Transaction Patterns

A number of organisations are now, for example, using so-called neural networks in the prevention of electronic funds transfer fraud. Software has been devised to analyse plastic cardholder spending patterns in order to alert individuals to the presence of unauthorised transactions, and also merchant deposit monitoring techniques to detect claiming patterns of corrupt merchants. Software has also been created which will maintain records of lost cards, stolen cards, counterfeit cards, fraudulent applications, cards never received, mail order, phone order and catalogue sales as well as merchant fraud (Nestor Inc. 1996).

Payment Authorisation

One of the main strategies used to prevent debit and credit card fraud has been to lower floor limits (the transaction value at which authorisation is required from financial institutions before the card can be accepted). In Britain, the percentage of plastic card transactions which required authorisation increased from approximately 10 per cent in 1992 to close to 50 per cent in 1998. This strategy, along with the introduction of a national "Hot Card File", or database of stolen cards, led to a 49 per cent reduction in point of sale fraud between 1991 and 1994 (Webb 1996, p. 24).

A related authorisation strategy which has been highly successful in preventing cheque fraud is the Positive Pay system provided by various banks. Businesses are able to provide their bank with electronic lists of cheques issued each day, which are immediately reconciled with cheques actually presented. Any forged or altered cheques will then be detected and payment stopped (Bank of America 1996).

Centralised Reporting

Centralised fraud reporting has also been important in reducing plastic card fraud. Cardlink Services Limited, for example, maintains extensive records of fraudulent credit card transactions which are used for prosecution purposes (Van Rhoda 1991). The Australian Bankers Association is also establishing a system to share information relating to card-based fraud between various financial institutions in an attempt to identify suspect transactions and individuals.

Personal Identification

The most successful countermeasure to creation of a false identity based upon altered or counterfeit documentation involves improving the reliability of evidence used for personal identification.

Biometric Identification

Biometric identifiers which make use of an individual's unique physical characteristics are the best way to establish identity. Common examples include fingerprints, voice patterns, typing patterns, retinal images, facial or hand geometry, subcutaneous vein structures and body odours (Johnson 1996). One company, "Fingerscan", has supplied fingerprint identification systems to Woolworths in

Australia and to a major Indonesian Bank, which have been used to replace password identification (Anonymous 1996). Because these physical properties are generally impossible to counterfeit, they create a very high level of security.

The costs and volume of data required to be stored online to enable comparison for any potential user may, however, be prohibitive and there is always the possibility that computer security systems could be compromised by reproducing data streams which correspond with the biometric characteristics in question. An additional problem is that users must be required to provide samples of their characteristics and that the security of these samples could be compromised. Some people also find the process of providing personal information in public distasteful, which was one reason given for the reluctance of retailers to make use of a cheque fraud prevention initiative which required customers to leave their fingerprint on cheques before they would be accepted by retailers (*see* Pidco 1996).

Databases

Maintaining extensive databases of individuals is another way of being able to validate identities. However, this raises problems relating to privacy and security of the information which is held. In the United Kingdom, for example, a long and bitter struggle took place before a voluntary national system of identity cards could be introduced in conjunction with photo drivers' licences (Gill 1997).

In Australia in the early 1990s, a complex database was created by the federal government in an attempt to prevent taxation and social security fraud, by identifying individuals who have made claims for benefits from government funds to which they are not entitled. The Parallel Data-matching Program makes use of tax file numbers and permits income records to be compared with payment records held by various benefit providing departments. The Program permits anomalies in payments to be identified and targeted for further investigation, and also permits the identification of individuals who are entitled to receive benefits which they have not claimed. In the year 1996-97, the Program resulted in direct savings of $A157 million for two departments, Social Security and Employment, Education, Training and Youth Affairs. The cost of conducting the Program for the same year was $A25 million resulting in a net saving of $A132 million.

The 100 Point System

In the world of banking, verification of one's identity is a critical element of fraud control. It is for this reason that multiple and independent primary sources of identification are required pursuant to the *Financial Transaction Reports Act 1988* (Cwlth) when one wishes to open an account with a financial institution. Primary documentation (passport, driver's licence, certificate of citizenship, birth certificate worth 70 points) along with matching secondary documentation (for example, a utility account etc.) are required in order to satisfy the 100 points of documentary evidence of identity required. Unfortunately, it is possible to submit documents which have been forged or altered through the use of computerised desktop publishing equipment.

Many primary documents are now protected through the use of various security devices, such as holograms, micro-printing and void pantographs (which reveal the word "void" when photocopied). Unless staff who inspect such documents are fully trained in recognising false or altered documents, it is possible to open various accounts in a variety of false names and make use of all of the banking facilities available, including loan facilities, until such time as the fraud is discovered or the false identity made known.

Another simple solution to the problem of counterfeit identification documentation is to validate identification documents with the issuing source. Staff presented with a birth certificate should, for example, check if the details correspond with those held in the central office of Births, Deaths and Marriages. An electricity account tendered as an identification document should be validated by checking with the electricity company concerned.

An example of an effective computerised personal identification system is that used by a retail chain in New York, Tops Appliance City Inc. This strategy, which was introduced in 1993, involves a computer network which checks credit card applications by photographing the applicant digitally, and recording the applicant's signature and other identifying information such as driver's licence, telephone and social security numbers. This information is then used to validate future purchases and also when the customer collects merchandise. The strategy resulted in a 90 per cent reduction in credit card fraud losses over a 17-month period following its introduction, with a 57 per cent reduction in losses per incident (Masuda 1996).

Counterfeiting Prevention

Counterfeiting prevention has developed greatly in recent years and a wide range of security features are now commonplace for plastic cards, cheques, and banknotes. Standard cheque security features include laid lines, colour prismatic printing, void pantographs, warning bands, high-resolution borders, holograms, micro-printing, secure number fonts, artificial watermarks and chemical voids.

Plastic cards are now protected by security printing, micro-printing, holograms, embossed characters, tamper-evident signature panels, magnetic stripes with improved

card validation technologies and indent printing. Smart cards, of course, are much more difficult to copy than ordinary magnetic stripe cards by reason of the need to re-engineer the silicon chip used to record data on the card.

The main problem with having so many security features in cards is that those who are required to validate them might not be familiar with all of the features present in the legitimate card and not trained to recognise counterfeit copies. There is also the possibility of sales staff being subjected to intimidation or violence if they refuse to process transactions, or delay unduly.

Another means of reducing the risk of counterfeiting is to imposing controls on the availability of the raw materials used in the manufacture of counterfeit cards, documents and currency. In Canada, recently, the RCMP introduced a campaign of issuing warning posters to companies which design and distribute white plastic and embossing machines used in the production of credit cards. The companies used the notices to educate staff about security and to monitor unusual requests for materials which could be used for counterfeiting (Duncan 1996).

Australia has been a world leader in the prevention of currency counterfeiting. Following the release of Australia's decimal currency in 1966, more secure banknotes were designed. The result was the development of polymer substrate banknotes which make use of two layers of polypropylene which are laminated under heat and pressure. The process also enables a clear window to be incorporated into the note with a space for hologram-like devices visible from either side of the note (James 1995).

Modern banknotes may also be protected by Optical Variable Devices (OVDs) which are images formed by grooves placed in ultra-fine aluminium which act like multiple miniature prisms to scatter white light into colours. This image is far more difficult to counterfeit than a hologram, but is a more expensive security measure (Michaelis 1993).

Computer Systems Monitoring

Fraud in recent time has been greatly facilitated through the use of computers, and fraud prevention initiatives, particularly in the areas of electronic commerce, have sought to protect computers and computer networks from interference and manipulation. As we approach the year 2000, with the ever-developing sophistication of computer systems, continued efforts directed at preventing fraud through effective management and monitoring of information technology systems will be essential.

Already, however, there have been great improvements in this area. ATM and EFTPOS terminals are now being located in secure places where users are protected both physically, as well as against shoulder surfing to obtain PINs. Terminals are now being placed in lobbies with card access and some have even been placed under armed guard. Systems which monitor vital points of an ATM for signs of physical attack have also been installed. Standardised requirements for ATM placement and design have been created, such as Australian Standard AS 3769 which governs the positioning of ATM and EFTPOS devices where PIN entry is required.

Various commercial products are available to prevent computer eavesdropping, or the interception of the electromagnetic emanations from computer equipment. These include the use of computers which limit the amount of EMR which is emitted and shields which prevent emissions from extending beyond certain areas or the external walls of buildings. Insulated covers and containers, for example, may be used on each micro-computer. It is also possible to produce electronic interference (noise) which will prevent EMR from being scanned, although some scanning devices are able to filter out such noise. By using micro-computers which do not use CRTs for video display the amount of emanation is reduced although it may still be intercepted (Wolfe 1995). Emission screening tends, however, to be expensive making its use beyond the budget of all but those organisations which deal in high-level security information.

Finally, continuing developments in cryptography help protect digital transmission streams. New algorithms now make the decryption of protected data extremely difficult, although concerns remain regarding the physical security of cryptographic keys which may be held on computer hard drives or disks.

Legal Deterrence

The deterrent effects of criminal prosecution and punishment represent the final means of deterring fraud, although quantifying the extent to which they are successful is problematic, to say the least. In addition to conventional judicial punishments such as fines, restitution and compensation orders, forfeiture and disqualification, unsupervised release, supervised release (probation, community service, intensive corrections) and custodial orders, there are a variety of other consequences which may follow the detection of fraudulent conduct including adverse publicity, professional disciplinary sanctions, civil action, injunctive orders and, most recently, various forms of reconciliation or community conferencing.

Whilst many small-scale property offenders behave more or less impulsively, and are unlikely to be deterred by the possibility of a criminal sanction being imposed, white-collar offenders are much more likely to engage in rational calculation, making some assessment of the prospective benefits and costs of a given course of action. In these circumstances, the greater the perceived likelihood of convic-

tion and the more severe the expected punishment, the less the inclination to offend. Individuals who are aware, for example, that their assets may be confiscated following a criminal conviction, may consider that the benefits to be derived from offending are not worthwhile. Arguably, the continued use of assets forfeiture legislation is beneficial and deserves increased publicity.

The conclusions which may be reached from the extensive research into the deterrent effects of criminal sanctions, are that while the availability of incarceration acts as a general deterrent to an unsubstantiated extent for some members of the community, increasing the use of incarceration will not result in greater deterrent effects nor in an overall reduction in crime. On the other hand, well publicised prison sentences help send the important message to the community, and particularly members of the business community, that dishonesty is not tolerated.

On rare occasions fraudsters are reformed following a period of imprisonment. Probably the best known example is of Frank Abagnale, who served four years in the United States for forging numerous cheques worth the equivalent of $A3.16 million. He was released from prison on condition that he assist law enforcement agencies in designing fraud prevention strategies and now runs a successful financial crime prevention consultancy (Boreham 1996).

Prison, however is not a panacea. Prospective offenders would more effectively be deterred through increased efforts at fraud prevention and enhancing rates of detection and reporting of offences.

Conclusions

This paper has identified eight areas in which efforts have been made to prevent fraud. Some have been used with considerable success while others have only partially been used due to a variety of financial and logistical problems.

Unfortunately, some of the strategies which have been mentioned are unlikely to be taken up fully because of the costs involved or the perceived potential impact on commerce. Others, however, such as the provision of information, are relatively inexpensive and it is these which are likely to yield the greatest immediate benefits in terms of fraud prevention.

In preventing this highly technical form of crime, it is essential for all those involved to work cooperatively, making use of the latest developments devised to deal with the sometimes highly specific and deviously imaginative ways in which fraud is now being carried out.

References

Anonymous 1996, "Fingerscan's $2.5m deal", *Security Australia*, vol. 16, no. 10, p. 2.

Australian Federal Police 1993-97, *Annual Reports* 1993-97, AGPS, Canberra.

Australian Payments System Council 1998, *Annual Report 1997-98*, Reserve Bank of Australia, Sydney.

Bank of America 1996, "Using technology to fight check fraud", http://www.bofa.com/corporate/cash_management/fraud.htm

Boreham, T. 1996, "Master fraudster turns gamekeeper', *Australian*, 3 July, p. 23.

BHP 1997, "Guide to business conduct", http://bhpweb.bhp.com.au/publications/b_conduct/index.htm

Deakin University 1994, *Fraud Against Organisations in Victoria*, Deakin University, Geelong.

Duncan, M.D.G. 1996, "Counterfeiting in a technological society", *International Criminal Police Review*, no. 456, pp. 18-21.

Dyson, C. & McKenzie, D. 1996, *Guidelines to Fraud Prevention*, New South Wales Police Service, Fraud Enforcement Agency, Sydney.

Ernst & Young 1996, *Fraud: The Unmanaged Risk*, Ernst & Young, London.

Ernst & Young 1998, *Fraud: The Unmanaged Risk*, Ernst & Young, London.

Ernst & Young and Australian Institute of Criminology 1993, *Consultants Report on Fraud Control in the Department of Administrative Services*, Department of Administrative Services, Canberra.

Gill, M. 1997, "Ethnic minorities and policing: The impact of national ID cards", *Security Gazette*, vol. 39, no. 8, p. 33.

Grau, J.J. (ed.) 1993, *Criminal and Civil Investigation Handbook*, 2nd edn, McGraw-Hill Inc., New York.

Insurance Council of Australia 1997, *Research into Insurance Fraud: Member Survey 1996-97*, Insurance Council of Australia, Sydney.

James, M. 1995, "Preventing the counterfeiting of Australian currency", in *The Promise of Crime Prevention: Leading Crime Prevention Programs*, eds P. Grabosky & M. James, Australian Institute of Criminology, Canberra, pp. 12-13.

Johnson, E. 1996, "Body of evidence: How biometric technology could help in the fight against crime", *Crime Prevention News*, December, pp. 17-19.

KPMG 1997, *1997 Fraud Survey*, KPMG, Sydney.

Masuda, B. 1996, "An alternative approach to the credit card fraud problem", *Security Journal*, vol. 7, pp. 15-21.

Michaelis, A.R. 1993, "OVD: The bank notes of the future", *International Bank Note Society Journal*, vol. 32, n..3, pp.5-14.

Nestor Inc. 1996, "Proactive fraud risk management: Neural network based credit card fraud detection from Nestor Inc." http://www.nestor.com/rmd.htm

New South Wales, Independent Commission Against Corruption 1994, *Monitoring Cash Handling in Public Hospitals: A Corruption Prevention Project*, ICAC, Sydney.

Pidco, G.W. 1996, "Check print: A discussion of a crime prevention initiative that failed", *Security Journal*, vol. 7, pp. 37-40.

Sims, S.J. & Sims, R.R. 1995, "Countering corporate misconduct: The role of human resource management", in *Corporate Misconduct: The Legal, Societal and Management Issues*, eds M. P. Spencer, & R. R. Sims, Quorum Books, Westport, pp. 183-208.

Standards Australia 1998, *Compliance Programs*, AS 3806-1998, Standards Association of Australia, Sydney.

Van Leeuwen, H. 1996, "A surge in credit card fraud", *Financial Review*, 24 September, p. 49.

Van Rhoda, T. 1991, "Credit card fraud", *Journal of the Australasian Society of Victimology*, Special Edition, April, pp. 127-9.

Webb, B. 1996, "Preventing plastic card fraud in the UK", *Security Journal*, vol. 7, pp. 23-5.

Wolfe, H.B. 1995, "An important reminder (anti-surveillance measures)", *Computer Fraud and Security Bulletin*, April, pp. 16-18.

Dr Russell G. Smith is a Research Analyst with the Australian Institute of Criminology

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia
Note: Trends and Issues in Crime and Criminal Justice are refereed papers.