I.I.R. CONFERENCES
Applying Risk Management to Implement a
Proactive Fraud Prevention Strategy in Financial Services
Parkroyal Darling Harbour, 19-20 July 2001

"Defining, Measuring, and Reporting Fraud Risk Within Your Organisation"

Dr Russell G. Smith
Senior Research Analyst
Australian Institute of Criminology

Introduction

Fraud can be described as deceit or trickery deliberately practised in order to gain an advantage over someone dishonestly. If fraud were described as an industry, it would clearly be one of the growth areas in the economy. It is also one of the least understood areas of the economy and, because fraud is often viewed as a victimless crime (particularly when perpetrated against large organisations), it does not draw community and political reaction like other crimes (Chapman and Smith 2001).

Because fraud occurs in so many different ways and settings, there is no standard recipe for fraud prevention. In the area of financial services, for example, the prevention of transaction fraud (such as fraud perpetrated through the use of counterfeit cheques or plastic cards) relies on different solutions to the prevention of identity-related fraud (such as establishing a line of credit using false identification or credit-worthiness documents)—although both make extensive use of technological, target-hardening approaches which seek to make paper documents and plastic cards difficult to manipulate or counterfeit.

The key to fraud prevention, however, lies in the development, and refinement, of a fraud control system. The foundation for such a system is a management philosophy which is sensitive to fraud risk. The basic elements of such a system are careful recruitment of staff, a culture of integrity and loss prevention within the organisation, and regular auditing of transactions by internal controllers, backed up by independent and accountable external auditors. The first line of defence against fraud in the financial services sector is to ensure the greatest possible transparency of transactions.

In this paper, I would like to examine four issues that arise in relation to the control of fraud and in dealing with it effectively. They are: defining fraud so as to facilitate measurement of the risks; quantifying losses for internal control and prosecution purposes; encouraging reporting of fraud minimising any counterproductive consequences; and utilising the outcomes of previous fraud experiences in a constructive manner.

Defining Fraud so as to Facilitate Measurement of the Risks

In legal terms, fraud is a generic category of criminal conduct that involves the use of dishonest or deceitful means in order to obtain some unjust advantage or gain over another. It is not specifically defined in legislation or at common law in Australia, although there are many criminal offences that contain an element of deception or dishonesty.

In business terms, fraud is sometimes difficult to define as it extends, for example, from conduct as trivial as an employee having an extended lunch break without permission, to large scale misappropriation of funds by a company accountant involving many millions of dollars. Having an understanding of how fraud is defined, is thus able to help organisations decide how best to respond to individual cases when they arise as sometimes an incident could more appropriately be dealt with as a personnel management issue rather than an issue that require a direct legal response.

There is also a need to distinguish between operational fraud risk (that arises from human, technical, or fraud-related considerations) and market or credit risk. Often, there may be a failure to characterise a loss as involving fraud, instead classifying it as a bad debt created through insolvency (Olive 2000). Occasionally, however, the difference between operational and market risk is unclear. For example, fraud perpetrated by a client of a financial institution who applies for and is granted a personal loan after having supplied deceptive information as to credit-worthiness, may be dealt with as a case involving market risk where default occurs, whereas in fact the client may have sought to defraud the lender from the outset. Mis-defining a fraud risk as a market risk may thus result in key fraud prevention measures being overlooked.

In the federal criminal law system which operates in Australia, there are nine separate jurisdictions, each of which has its own common law and legislative offences involving fraud and deception. These offences cover a wide range of conduct involving an element of deception and the definitions used have changed considerably over time. In Victoria, for example, police statistics record over 100 separate offences included in the category 'deception', including various forms of obtaining property by deception, forgery, conspiracy, impersonation, secret commissions, and making false statements.

One of the most important national policy goals in recent years has been to clarify the legal rules that govern criminal offences, and particularly those relating to theft and fraud. This, it is argued, would help not only to maximise the possibility of offenders being prosecuted successfully, but would also facilitate the collection of uniform crime statistics throughout the nation. In addition, in an age in which most fraud offences are carried out through the use of computers in some way or other, the definition of fraud, and particularly its geographical scope, need to be defined in technology-neutral terms that will enable the most sophisticated fraudsters to be dealt with effectively by the courts.

This goal is being gradually achieved with the development of the *Model Criminal Code*, a standardised criminal statute that will eventually be adopted uniformly in each State and Territory. Already Federal legislation has been passed which establishes uniform rules governing offences of theft, fraud, bribery and related offences (*Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act* 2000 (No. 137 of 2000, Cth). It remains to be seen when the various States and Territories will take up the provisions of this Model Act for their own purposes.

Deception is defined in section 133.1 of the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act* 2000 as meaning:

> an intentional or reckless deception, whether by words or other conduct, and whether as to fact or as to law, and includes:
> (a) a deception as to the intentions of the person using the deception or any other person; and

(b) conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorised to cause it to do.

Various offences are specified including the offence of obtaining property or a financial advantage by deception (Division 134) and certain other offences involving fraudulent conduct (Division 135). These offences include doing anything with the intention of dishonestly obtaining a gain from the Commonwealth (which carried a maximum penalty of 5 years' imprisonment), or conspiring with another person with the intention of dishonestly obtaining a gain from the Commonwealth (which carried a maximum penalty of 10 years' imprisonment).

Other offences are created that relate to making false or misleading statements in applications (s. 136.1), giving false or misleading information (s. 137.1), and using various false or misleading documents (s. 137.2)(each of which carry a maximum penalty of 12 months' imprisonment).

The new legislation replaces existing offences under the *Crimes Act 1914* (Cth) and repeals over 250 offences in Commonwealth legislation.

The new laws also make provision for offences that involve new technologies. This, for example, clarifies the law that applies where offenders obtain money from ATMs by making use of flaws in systems that have enabled funds to be withdrawn in excess of account credit balances (e.g. *Kennison* v *Daire* (1986) 160 CLR 537; R. v *Evenett* [1987] 2 Qd R 753 and R. v *Baxter* [1988] 1 Qd R 537). Similarly, where it is only a computer that has been deceived rather than a human actor, the legislation now provides that this amounts to an act of deception.

It should be emphasised, however, that the new legislation at present applies only to the Commonwealth.

Deceitful conduct may not only result in criminal consequences, but also civil ones. Traditionally, fraud was regulated principally through civil action with the use of the criminal law as a regulatory strategy being a relatively new invention, at least in the history of the common law (see Page 1997 for a history of the legal regulation of fraud). Today, the civil consequences of fraud continue to have widespread importance as, clearly, it is beyond the capacities of police and other regulatory agencies to investigate every allegation of fraud which comes to their attention.

To conclude, therefore, it is important for organisations, such as financial institutions, to have policies in place that define fraud in such a way as to facilitate operational risk management. Organisations need to know which types of conduct they are seeking to prevent and, where they occur, which matters should lead to civil consequences and which should be prosecuted in the criminal courts. The procedures that are needed to deal with market risk are often different from those that are needed to prevent the kind of conduct that would result in a criminal prosecution for dishonesty. There is also the need to distinguish personnel management issues from matters that leave an organisation exposed to the risk of large-scale misappropriation of funds.

Quantifying Fraud Losses for Internal Control and Prosecution Purposes

The second issue for discussion concerns the question of measuring how much has been lost in cases involving fraud. This has important implications for deciding whether or not to embark on a prosecution, and also for justifying to management the expenditure associated with taking legal

action. Knowing exactly how much has been lost to an organisation following fraud is also important for the costing of future fraud prevention initiatives.

At the outset, close attention needs to be paid even to seemingly small discrepancies in accounts, as sometimes these may be indicative of a larger problem. A classic illustration of this has been provided by Stoll (1991) whose pursuit of a US$0.75 error in a computer account led to the discovery of an international espionage ring.

Sometimes organisations will be unaware of how much they have lost in individual cases and it will only be after the case has been investigated by forensic accountants and the police that the full extent of losses will become apparent. Once a case has been prepared for prosecution, it may also not be possible to prosecute every allegation of fraud as this would overload charges against an offender and be rejected by the courts on grounds of unfairness as well as the consequential time needed to prove every allegation. As a result, the final amount prosecuted may only be a fraction of the total losses sustained.

Organisations also incur substantial additional costs in investigating and prosecuting matters. Forensic accountants may need to be engaged to conduct an audit of a whole department's accounts. Managers and other key personnel may then be required to attend court to give evidence – although in most cases of serious fraud the offender usually pleads guilty once a preliminary investigation has been concluded, and sometimes immediately the incident comes to light. These indirect costs incurred by victims of fraud can be substantial, sometimes amounting to many thousands of dollars. Although some may be recovered from solvent offenders through court compensation orders, invariably the victim company will suffer at least some additional costs associated with prosecuting a case that will not be able to be recovered, especially where the offender is without assets or has disbursed the sum stolen.

As a result, it is extremely difficult to quantify exactly how much has been lost through fraud cases that are prosecuted in the courts. It is, however, important for management to be made aware of the losses sustained in individual cases so that the associated costs of fraud prevention initiatives are seen to be both reasonable and justifiable.

Bearing these considerations in mind, in Australia, some of the estimates which have been given of the cost of fraud are as follows.

Although now somewhat out of date, the Australian Federal Police (AFP), in a submission to AUSTRAC, estimated in 1996 that between A$3 and A$3.5 billion was lost through fraud in Australia annually (Walker 1997). AFP Annual Reports indicate much smaller sums involved in fraud cases actually dealt with which have ranged from between A$125,970,000 in 1997-98 and A$207,269,000 in 1999-2000 (Australian Federal Police 1998-2000). The ever-increasing trend in the dollar value involved in these cases over the last few years is of particular concern.

The National Survey of Crimes Against Businesses found in excess of A$235 million lost by fraud against businesses in the retail, manufacturing, primary industry and tourism/recreation sectors in the year 1992-93 (Walker 1994), while KPMG's 1999 survey found losses of more than A$239 million due to all forms of fraud including thefts by staff, customers and suppliers, with the average cost per incident of A$1.1 million (KPMG 1999).

Walker (1997) concluded his study of the cost of fraud by calling for increased funding to enable fraud victimisation surveys to be carried out on a wide scale. Official police estimates provide

only a limited indication of the cost of fraud owing to their exclusion of unreported offences. Relying upon cases which proceed to trial is also problematic as only a selection of offences is included for prosecution and it is these which form the basis of the estimated loss. Other offences taken into consideration for sentencing purposes tend not to be included in official estimates of the cost of crime.

Encouraging Reporting of Fraud and Minimising Counterproductive Consequences

Often when organisations have been victimised through fraud, managers are reluctant to report the matter to the police or otherwise to seek official redress. KPMG (1999), for example, found in its survey of businesses, that 33.3 per cent of organisations surveyed failed to report frauds to the police, many instead preferring to deal with the matter internally and or by dismissing the individual in question. Ernst and Young's study (1998) found that although nearly half of the organisations surveyed had a fraud reporting policy in place, fewer than half of those said that their staff were aware of the policy. Some of the reasons given by the respondents to Deakin University's (1994) survey for not reporting fraud to the police included a belief that the matter was not 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 fraud has been committed by those in positions of responsibility within organisations, they may not wish to draw undue attention to their own illegal activities.

As a result, many organisational victims simply take no official action preferring instead to warn or to dismiss the perpetrator and to take steps to prevent a recurrence of the incident by tightening security procedures. On some occasions a desire to 'save face' may result in the perpetrator being allowed to resign with no further action being taken.

Failure to take official action, however, has a number of adverse consequences.

Those who have acted illegally may believe that because they have not suffered any adverse consequences from their conduct, they are free to act illegally again in the future, either in exactly the same way in respect of the same organisation or in a new workplace where their prior misconduct is not known of.

Failure to take action may also result in any general deterrent effects on the rest of the staff being diluted or avoided if the illegality of one of their number fails to result in official action. This

may lead to a more generalised down-grading of the ethical standards within the organisation owing to management being seen to be unwilling to take action.

Increasing the level of reporting of fraud by organisations would help to ensure that similar patterns of offending by the same or other offenders are uncovered by police and that appropriate fraud prevention strategies may be identified and implemented. If the true nature of fraud remains undisclosed and uninvestigated, then it is difficult to devise appropriate measures to guard against it.

The community may also suffer where crime has not been dealt with as incidents will not find their way into official crime statistics and the educative and deterrent effects of publicity in preventing crime will be avoided. Effective reporting may, instead, enhance the feeling in the community that fraud is, in fact, unlawful and likely to result in prosecution where it is detected.

Finally, if offenders are not dealt with, organisations might be subject to repeat victimisation, sometimes at the hands of the same individual or someone else replicating the same form of criminal activity. In the context of personal fraud victimisation, studies have consistently found that one of the most reliable indicators of fraud victimisation is past victimisation (Titus and Gover 1999).

Enhancing Fraud Reporting by Organisations

In order to encourage organisations to take official action where they have been victimised through fraud, a variety of constructive steps may be taken.

In the first place it is important for organisations to have clear and transparent fraud control policies in place. 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 (Standards Australia 1998).

One of the greatest impediments to reporting concerns the fear of bad publicity where criminal proceedings are taken. Although criminal courts are reluctant to conduct proceedings *in camera*, on occasions this could be desirable in order to protect a business reputation from adverse publicity or to ensure that a novel type of fraud does not receive undue public attention which might encourage illegal conduct.

Organisations might also be more willing to report fraud to the police if they were confident that the personal costs and time associated with the investigation and prosecution of the matter could be minimised. This could, perhaps, be achieved by streamlining interviewing procedures and by reducing the necessity for senior witnesses to be present in court for unnecessarily lengthy periods of time. Documentary evidence should also be used in preference to oral testimony wherever possible and the barriers to the use of computer-generated evidence overcome. The appropriate use of awards of costs to assist witnesses should also be considered and scales of witness expenses increased to realistic levels.

The use of fraud reporting 'hot lines' may be another way of persuading employees to report fraud to management, although in Ernst and Young's (1998) survey, more than fifty per cent of

respondents were opposed to the idea with most opposition coming from company directors. In KPMGs (1999) survey, only one per cent of the Australian respondents reported having a formal confidential telephone line as a means of receiving allegations of incidents of fraud.

A more radical way in which fraud reporting could be improved entails the enactment of mandatory reporting legislation to ensure that organisations take official action. Already, however, the law in some states requires, in certain circumstances, that individuals who become aware that they have been defrauded, bring the matter to the attention of the police. Sub-section 1 of section 316 *Crimes Act* 1900 (NSW), for example, creates an offence of failing to report a 'serious offence' (being an offence punishable by at least five years' imprisonment) to the police where the person knows or believes that the offence has been committed and that he or she has information which might be of material assistance to the police. This offence carries a maximum penalty of two years' imprisonment, although a prosecution of professionals such as accountants who fail to report serious offences cannot take place without the approval of the Attorney General.

An alternative to legislation which requires organisations to report fraud to the police, would be a requirement for professionals, such as solicitors, accountants and auditors, who become aware of fraud, to report the matter to the organisation's Chief Executive Officer. Failure to report could then result in disciplinary proceedings being taken against the professional in question for misconduct. Requiring auditors to take on the role of fraud investigators is, however, highly contentious although the idea is continuing to gain support in recent times in a number of countries (see Nel 1999; Azzopardi 1999).

If such mandatory reporting obligations were enacted, appropriate safeguards would need to be introduced to protect those who report their suspicions of fraud from personal liability where they act in good faith. The problem of so-called 'whistleblowers' has been documented in a number of studies which have looked at individuals who have reported corruption in public sector agencies. The difficulty relates to whistleblowers being discriminated against or otherwise being subjected to harassment, intimidation or reprisals as a consequence of reporting what they believe to be illegal conduct.

De Maria and Jan's (1996) study of whistleblowers found that many whistleblowers did not get the treatment or action they expected and were, in fact, seriously disadvantaged by the action they took. The study showed a crisis of competence in the official capacity of government structures to respond effectively to disclosures made in the public interest.

In Australia and New Zealand, whistleblower protection statutes have been introduced in various jurisdictions, some with greater consequence than others (*see* De Maria 1995). Where such legislation exists, its provisions should be widely publicised and its protections used in appropriate cases to protect those who report fraud in the public interest. Additional efforts could also be made to assist those who have reported fraud in the public interest by establishing a fund to provide compensation for financial loss suffered as a result of their reporting. This could be achieved by setting aside part of the funds obtained through criminal confiscation legislation, if the Commonwealth were agreeable to taking such funds out of consolidated revenue.

On a more general level, increasing resources to law enforcement agencies would help to ensure that individuals in the community have confidence in the ability of agencies to investigate and prosecute allegations of fraud. At present, many cases which are reported are simply unable to

be investigated through law enforcement agencies being under-resourced, particularly for the investigation of serious, complex and time-consuming allegations involving fraud and deception.

Minimising Counterproductive Consequences of Fraud Prevention

In implementing countermeasures against fraud care should be taken to ensure that they do not entail any unintended negative consequences. Effort is needed to 'engineer out' any risks that a fraud control policy has which may result in the program 'back-firing' when introduced.

In the first place, any fraud prevention information that is given should serve prospective victims, not prospective offenders. It should seek to reduce and not to inspire criminal activity.

Care should also be taken to ensure that fraud control initiatives do not inspire more inventive or devious activity in the process of seeking to foreclose easy criminal options. With a view towards remaining one step ahead of the law, entrepreneurial criminals may engage in increasingly refined avoidance behaviour.

Fraud prevention measures which are adopted should also not be so demanding on an organisation in terms of administration and cost that business will be retarded and innovation stifled. Fraud control, therefore, should avoid overkill—it should not be so intense as to have a chilling effect on legitimate commerce and responsible risk-taking.

Systems for reporting fraud should also not invite frivolous and vexatious complaints. It will be especially important to ensure that any rewards and incentives which may be offered for the detection and reporting of fraud do not contribute to the creation of a society of bounty hunters and spies.

Another risk inherent in fraud control is that of insufficient coordination. This may take the general form of turf battles between rival organisations, or neglect of matters 'falling between the cracks'.

These risks are real, because the vast array of offences referred to collectively as 'fraud' require a range of different institutions for their prevention and control. No single fraud control agency could be designed to handle this. But those individuals, institutions and agencies who are in the business of fraud control should avoid demarcation disputes, rivalry, and competition.

What this implies, however, is a degree of coordination and cooperation which is still some time away from becoming a fact of organisational life in Australia.

Utilising the Outcomes of Previous Fraud Experiences in a Constructive Manner

Where it has been proved that individuals have acted dishonestly it is essential that they not be permitted to repeat their illegal conduct at the same location or elsewhere. Corporations need to learn from their fraud experiences, difficult though they may have been, and ensure that they will not subjected to repeat victimisation. Sometimes this may mean that entire systems may need to be re-designed or senior management removed. On other occasions, the use of simple tools of staff rotation or increased supervision or auditing may be sufficient.

Consideration also needs to be given to creating and using formal controls that prevent offenders from repeating their conduct again. In some cases, the law itself may assist in this regard.

Section 206B of the *Corporations Law* provides that persons convicted of certain offences are prohibited from managing a corporation, without the permission of a court, for a period of five years from the date of their conviction or, if imprisoned, from the date of their release. One practical strategy to enhance compliance with these rules is the initiative taken by the Australian Securities and Investments Commission (ASIC) which now maintains a public register of persons who have been disqualified by ASIC from acting in the management of a company or as financial advisers. This information is readily accessible to the public through information brokers as well as the Internet (http://www.search.asic.gov.au/ban.html). By including the names of disqualified persons on a public register, ASIC provides a valuable source of information to those in the business world about the standing of individuals with whom they conduct business and who may be seeking positions in management.

By no means should knowledge about fraud and fraud risks remain a monopoly of law enforcement agencies. Because the first line of defence against fraud can and should be self-help, appropriate knowledge should be shared with private citizens, businesses, and public sector agencies alike. All prospective victims of fraud, and this includes just about everyone in Australia, should be aware of the types of fraudulent activity to which they are most vulnerable, the 'red flags' or indicia of fraud, the most appropriate means of prevention, and best avenues of response when they detect an offence.

Again, because of the wide diversity of fraud-related activities, there can be no single message or information medium to communicate the above. Rather, information should be 'sector specific', relevant to the type of fraud and/or category of victim in question. Thus, information for share investors will differ from that appropriate to small businesses, which will in turn differ from that appropriate to public sector agencies which contract with private sector suppliers of goods and services. Each of these sectors will have existing information networks or sources which are best suited to serve as a conduit for information related to fraud prevention and control. These will include professional organisations, industry associations, consumer groups, organisations representing senior citizens, or regulatory agencies such as ASIC and the Australian Competition and Consumer Commission.

The development of comprehensive *Codes of Conduct*, such as that implemented in the field of electronic banking, provides not only a statement of benchmarked standards for those using such systems, but is also useful in resolving disputes between individuals. Potential offenders may also be deterred from acting illegally if they are made aware of the regulatory controls which are in place.

New developments in communications permit not only the dissemination of basic fraud control information, but also the reporting of suspicious activity to appropriate authorities. The Internet abounds with materials on fraud control; some industry-specific, others focusing on certain vulnerable groups such as senior citizens. Other sources of information are medium-specific; sites are dedicated to warning of fraud on the Internet. Moreover, many law enforcement and regulatory agencies have established hotlines which are available to fraud victims or civic minded third parties to report illegal or questionable conduct.

Similarly, the Internet and similar new technologies now permit speedier communication between agencies. Authorities on the other side of the globe may be alerted instantaneously to a new scam, and will thus be prepared to warn of its possible migration, and to interdict it when it first appears on their soil.

Conclusions

What I have attempted to do in this paper is to provide some information on the ways in which fraud may be prevented and controlled, principally through the actions of victims and potential victims of deceptive conduct.

Because fraud exists in some many different guises, it is necessary to define carefully what it is that one is seeking to prevent and to tailor policies and initiatives accordingly. It is trite to say that prevention is better than cure. Given the extraordinary costs of investigating and prosecuting complex commercial fraud, and the uncertainty of outcome, there seems little doubt that it is wiser to close the barn door before the horse bolts. Already a substantial industry is being developed globally in providing fraud prevention advice and products. What is needed is for individuals throughout the community to be made aware of the risks of victimisation through fraud and willing to take appropriate preventive action.

If an organisation has been unfortunate enough to have been victimised through fraud, decisions then need to be made about how to respond. I have suggested that policies should be in place to enable losses to be quantified and for the matter to be brought to the attention of the authorities in appropriate cases. Not every case will require involvement of the police or regulatory agencies, but many cases will, particularly where questions of insurance or compensation arise.

Care should also be taken to avoid any negative consequences of introducing preventive measures or reporting cases officially. Having carefully devised policies may help in this regard.

Finally, any experience of fraud victimisation should be seen as an opportunity to review systems and procedures in order to prevent further victimisation by the same offender, or by others employing the same strategy. Businesses, therefore, need to learn from prior fraud victimisation experiences and not simply dismiss the offender and hope that the same problem will not recur in the future.

It is also important to foster a culture of intolerance to fraud throughout the Australian community. Deceptive practices, in whatever walk of life should not be condoned. Recent lengthy sentences imposed upon convicted perpetrators of commercial fraud might help to convey this message. In addition, constructive education campaigns, such as those that have successfully changed attitudes with respect to discriminatory practices in the community, could be employed throughout Australia in order to help explain why dishonest and corrupt practices are unacceptable. Specific, and perhaps substantial, resources will need to be allocated to achieving generalised changes of attitudes and these should be provided from both the public and private sector. Compelling evidence already exists to indicate that expenditure on such initiatives would be more than cost-effective in reducing losses sustained through fraud.

References

Azzopardi, T. 1999, 'Auditors as Guardians Against Fraud', paper presented to the International Society for the Reform of Criminal Law, 13th International Conference *Commercial and Financial Fraud: A Comparative Perspective*, St Julians, Malta, 9 July.

Australian Federal Police 1998-2000, *Annual Reports 1997-98, 1998-99, 1999-2000*, Australian Federal Police, Canberra.

Chapman, A. and Smith, R. G. 2001, 'Controlling Financial Services Fraud', in *Trends and Issues in Crime and Criminal Justice*, No. 189, Australian Institute of Criminology, Canberra.

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

De Maria, W. 1995, 'Whistleblowing', *Alternative Law Journal*, vol. 20, no. 6, pp. 270-81.

De Maria, W. & Jan, C. 1996, 'Behold the Shut-Eyed Sentry! Whistleblower Perspectives on Government Failure to Correct Wrongdoing', *Crime, Law and Social Change*, vol. 24, pp. 151-66.

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

KPMG 1999, *1999 Fraud Survey*, KPMG, Sydney.

Nel, H. C. 1999, 'The Plight of Victims of Economic Crime: Investors as Victims', *Journal of Financial Crime*, vol. 6, no. 4, pp. 311-22.

Olive, C. 2000, 'Operational Risk in Banking Institutions', in Norton, J. J. and Walker, G. A. (eds.), *Banks: Fraud and Crime*, LLP Professional Publishing, London, pp. 135-71.

Page, F. 1997, 'Defining Fraud: An Argument in Favour of a General Offence of Fraud', *Journal of Financial Crime*, vol. 4, no. 4, pp. 287-308.

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

Stoll, C. 1991, *The Cuckoo's Egg*, Pan Books, London.

Titus, R. M. and Gover, A. R. 1999, 'Personal Fraud: The Victims and the Scams', paper presented to the International Society for the Reform of Criminal Law, 13th International Conference *Commercial and Financial Fraud: A Comparative Perspective*, St Julians, Malta, 9 July.

Walker, J. 1994, *The First Australian National Survey of Crimes Against Businesses*, Australian Institute of Criminology, Canberra.

Walker, J. 1997, *Estimates of the Costs of Crime in Australia in 1996*, Trends and Issues in Crime and Criminal Justice, No. 72, Australian Institute of Criminology, Canberra.