

**NATIONAL FRAUD SUMMIT 2005  
23 March 2005, Grace Hotel, Sydney**

**“Understanding Fraud Reporting  
as an Effective Risk-Management Tool”**

**Dr Russell G. Smith  
Principal Criminologist  
Australian Institute of Criminology**

**Introduction**

This paper argues that effective reporting of fraud can offer a wide range of benefits for both organisations and the community as a whole. These include raising awareness of fraud victimisation which can help to create a fraud-averse culture amongst management and employees; enabling effective quantification of fraud victimisation for risk-management and resource allocation purposes; helping to evaluate existing fraud minimisation procedures by seeing if they have been effective in preventing fraud from taking place; compiling intelligence which can be used for policing and fraud prevention activities; providing feedback to those who have detected fraud to reward their vigilance; enabling information on new crime methodologies to be shared with others at risk of similar types of victimisation; and assisting in the compilation of statistical data for trend identification and analysis.

Only by understanding the true extent of fraud victimisation can business and government begin the process of designing and implementing targeted risk-management activities that will be effective in addressing the new and emerging problems as they arise.

At the outset, however, we need to assess the scope of the problem of under-reporting of fraud and to determine why under-reporting takes place. We can then look to some of the solutions that have recently been proposed to encourage fraud reporting including the use of hotlines, whistleblower protections, mandatory reporting legislation, and suggestions which have recently been made for the establishment of central fraud reporting agencies.

The aim is to enhance the reporting of fraud, so that repeat victimisation can be avoided and the deterrent effects of prosecution and punishment maximised. There is now clear evidence that it is neither effective nor ethical simply to dismiss a person suspected of dishonesty from their employment, without taking further action. Unfortunately, this practice remains all too prevalent.

**Quantifying the Current Extent of Fraud Reporting in Australia**

In order to assess the extent to which fraud is reported, we have to rely on the evidence that comes from surveys of organisations and individuals about their victimisation

experiences. Unfortunately, these have consistently found that fraud tends to be a category of crime that often goes unreported to police and other regulatory agencies.

Some of this evidence is as follows.

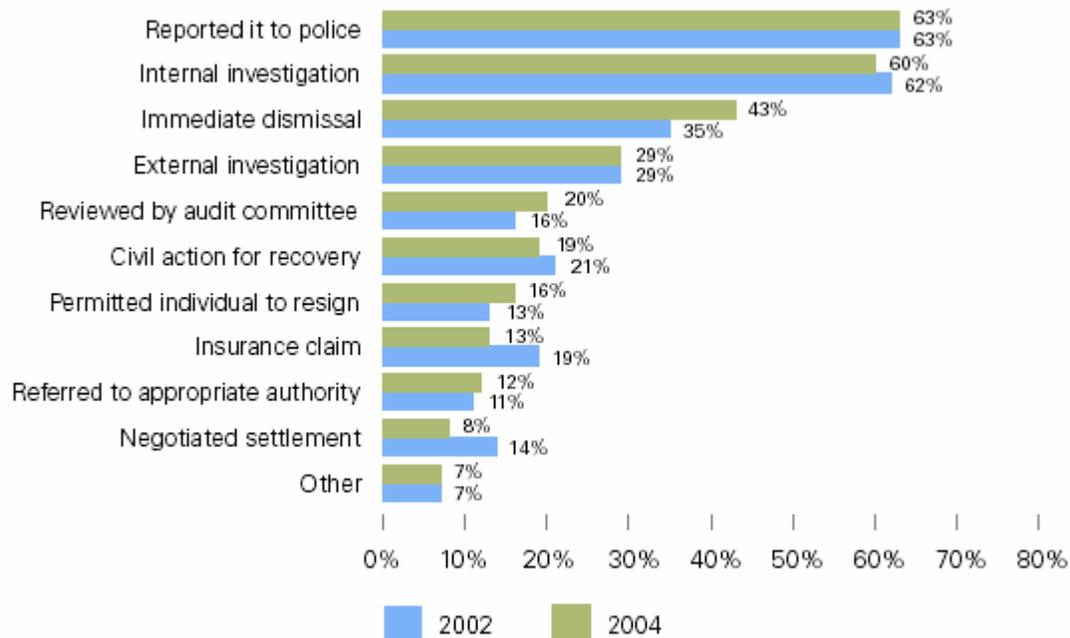
The Australian Institute of Criminology's Small Business Crime Survey, found that crime reporting behaviour of small retail businesses varied, depending on the type of crime and whether the crime was attempted or completed. While nine in 10 completed burglaries and robberies were reported to police, only one in 17 incidents of employee theft, one in five incidents of shoplifting, and one in four incidents of cheque/credit card fraud were reported (25%) (Taylor 2002).

More recently, the Australian Institute of Criminology undertook a survey of 1,703 small businesses in five business types across Australia in April 2003. These were florists, booksellers, toy and game traders, computer hardware retailers, and recorded music retailers. Some 13 per cent of respondents traded online and in 2001, 35 per cent of incidents of fraud were reported to police while in 2002, only 21 per cent were reported (Charlton and Taylor 2004).

In the latest in a series of Ernst and Young fraud victimisation surveys, conducted in about fifteen countries, a reporting rate of between twenty per cent and twenty-five per cent was found (Ernst and Young 2003).

In its most recent survey of business fraud, KPMG (2004) found that 63 per cent of major fraud incidents reported in the survey were referred to the police. This leaves nearly 37 per cent of fraud matters handled without police involvement. A range of other responses was reported, including internal and external investigations, or simply immediate dismissal of the individual in question (KPMG 2004, p. 23). These results are shown in Figure 1.

**Figure 1 – Action Taken Concerning Largest Fraud Incident in KPMG’s 2004 Fraud Survey**



Source: KPMG (2004, p. 23)

### Identifying the Barriers to Effective Fraud Reporting

The reasons for non-reporting of fraud are well-known. Some victims, such as those who have given money to fraudulent and non-existent charities, may never realise that they have been victimised. Some organisations, may be unaware that employees have stolen stock.

In the case of fraud relating to electronic commerce, victims may be unable to locate the offender who may be resident overseas or who may have used an anonymous re-mailing system in carrying out the fraud. Often the victims of economic crime may be unwilling to incur further time and expense in pursuing legal remedies - in the case of electronic fraud, the key factor is the need to re-instate systems quickly so as to prevent loss of business.

There may be a belief that there is inadequate proof or that the matter is not serious enough to warrant police attention or there may be fear of reprisals if matters are reported or that publicity of security weaknesses could result in victims being targeted again, or of losing business or damaging commercial reputations

Finally, many public sector agencies often don't like to admit that they have a problem.

In KPMG's Fraud Survey (2004, p. 23), the organisations surveyed indicated a 'lack of evidence', 'concern about adverse publicity' and 'concern about the resources required to

prepare the complaint' as their main reasons for not reporting matters to the police (see Table 1).

**Table 1 – Reasons for Failing to Report Largest Fraud Incident to Police in KPMG's 2004 Fraud Survey**

Reason for not reporting to the police	%
Lack of evidence	25
Concern about adverse publicity	12
Concern about the resources required to prepare the organisation's complaint	9
Immaterial amount involved	7
Concern about costs associated with making the report	5
Concern about the effectiveness of the criminal justice process in deterring the further incidence of fraud within the organisation	5
Concern about the effectiveness of the criminal justice process in deterring the further incidence of fraud within the community generally	5
Concern about the impact on a civil claim against the person for recovery of the stolen property	3
The organisation has a policy that such matters are not reported to the police	3
Other	26
Total	100

Source: KPMG (2004, p. 23).

In the Australian Institute of Criminology's Small Business Crime Survey, it was found that reasons for non-reporting generally reflected a pessimistic belief that reporting crime was pointless and achieved nothing (see Taylor 2002).

Similar reasons for non-reporting of electronic commerce incidents were given by the respondents to KPMG's *Global eFraud Survey* (2001), in addition to the key factor of the need to re-instate systems quickly so as to prevent loss of business. Reporting the matter to the authorities simply prevented the organisation in question from minimising its financial losses, and risked incurring further losses in prosecuting the matter.

Businesses are often reluctant to report fraud simply due to a fear of 'sending good money after bad'. Their experiences may have led them to believe that it is impossible to recover losses through legal avenues and that the time and resources required to report an incident officially and to assist in its prosecution simply do not justify the likely return on investment. 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 their victimisation because of a fear of losing business or damaging their commercial reputation. A government agency that is the victim may believe that adverse publicity could result in a loss of confidence by voters, while financial institutions that have suffered from fraud might believe that publicity of security weaknesses could result in being targeted again.

In the financial services sector, it is often the case that reporting fraud is not seen to be in the commercial interests of corporations. In the Report of the Victorian Parliamentary Drugs and Crime Prevention Committee's (2004, p. 54) *Inquiry into Fraud and Electronic Commerce*, the Victorian Director of Public Prosecutions referred to a recent case in which a bank had provided 60 to 70 loans based on false information. Only four of these, however, resulted in default by the borrower and it was only these cases that the banks pursued. From a prevention and intelligence perspective, however, each of the 60 or so cases would have been relevant.

American Express, also gave evidence to the Committee (p. 54) that less than five per cent of their total fraud incidents were reported, which was felt to be a similar proportion for most financial institutions. Similarly, Acting Detective Superintendent Peter Lavender of the Commercial Crime Division of Western Australia Police told the Committee (p. 54) that:

I believe that there is a dark figure of fraud that exists that we don't know about. Because corporate bodies decide that there is a threshold, a nominated threshold, under which they won't report and over which they will bring it to our attention. That deprives us of a lot of intelligence as to exactly how much fraud there is. With electronic fraud at the moment, ID fraud, it is usually high volume, low cost fraud, which would mean that a vast area of fraud won't get reported to us and we would be left without knowing exactly what was going on.

### **The Consequences of Not Reporting Fraud**

Failure to take official action, however, causes a number of problems. First, 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).

### **Encouraging Reporting**

There are a various ways in which reporting of fraud can be enhanced. These include educating the public and corporate world about the need to report offences to the police; extending *Whistleblowers Protection* legislation to individuals who report suspected fraud and offences involving dishonesty committed in the private sector; establishing a central agency which can receive reports from all sources and which could coordinate investigatory action by sending reports to appropriate agencies; creating electronic systems to make reporting simple and efficient including the establishment of a hotline for reporting public or private sector fraud; providing regular feedback to complainants about what is being done with their cases; enacting legislation to make it obligatory to report fraud to the central agency, and creating a criminal offence for failure to report a serious offence involving dishonesty.

Three issues deserve some further discussion, namely the use of hotlines, whistleblower protection legislation, and mandatory reporting requirements.

### **Using Hotlines to Encourage Fraud Reporting**

The use of fraud reporting 'hot lines' is a 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. More recently, in KPMG's (2004, p. 28) survey, 48 per cent of respondents reported having instituted a system for anonymous reporting of fraud and corruption (either operated by the organisation itself, or by an external agency on the organisation's behalf). The use of anonymous reporting systems had increased by 15 per cent since KPMG's 2002 survey was conducted.

Anonymous hotlines are telephone numbers dedicated to the reporting of relevant matters. Most commonly, the person receiving the calls will be part of the organisation, such as a manager although some people may not feel comfortable reporting to someone within their own organisation. It is possible, for example, that the person nominated to receive calls will actually be the perpetrator of the wrongdoing, creating additional difficulties. To overcome such concerns, some hotlines are externally maintained. Companies may engage a separate organisation to provide a whistleblowing facility. Employees can call the hotline and somebody neutral to the company will take the call. Information can be provided anonymously if desired. Relevant information will then be passed on to the company for investigation.

Externally maintained hotlines are particularly useful in encouraging reporting because they can make people feel comfortable in speaking out against others whom they know and work with in the organisation. Often potential whistleblowers may feel frightened of that person, or of their possible reaction to their claims. Alternatively, they may not believe that the contact person will properly pursue their allegations. In addition, internal reporting mechanisms will rarely provide for the possibility of truly anonymous reporting, even in larger organisations, as there is always a risk that an individual's voice will be recognised. Many individuals may feel more willing to be open and honest if their anonymity is protected.

### **Understanding Whistle-blower Protection Strategies in the Public and Private Sectors**

Relying on individuals within organisations to report fraud is of critical importance as it is often the case that colleagues will be the first to detect suspicious transactions or activities. In Ernst & Young's 8<sup>th</sup> *Global Survey* (2003), for example, whistleblowing was seen to be the second most effective method of fraud detection, while in KPMG's *Fraud Survey* (2004, p. 19) 19 per cent of fraud was detected by employee notification, with a further 6 per cent being notified to the organisation by anonymous letters or calls.

If employee notification is to be encouraged, however, appropriate safeguards need to be in place to protect those who report their suspicions from personal liability or reprisals. The problems faced by whistleblowers have been documented in a number of studies which have looked at individuals who have reported corruption in public sector agencies. The difficulties relate 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. This will be a particular problem if the wrongdoing is being committed by those in management. In such circumstances, individuals may reasonably fear that if they speak up, their employment with the organisation may be placed in jeopardy.

In Australia, whistleblower protection statutes have been introduced in various jurisdictions, some with greater consequence than others. In Victoria, for example, the *Whistleblowers Protection Act 2001* (Vic) attempts to provide protection for those who disclose improper conduct or detrimental actions by public officers and public bodies. The Act sets out procedures for both disclosure and investigation, and under section 109 exempts documents connected to protected disclosures from the ambit of the *Freedom of Information Act 1982* (Vic). Offences are created in relation to taking reprisals against a whistleblower (s.18), revealing confidential information related to a protected disclosure (s. 22), obstructing an investigation (s. 60) and making a false disclosure (s.106).

While this legislation offers protection to those in the public sector, the same level of protection is not offered to those in the private sector. Protection for those outside the public sector already exists in some other jurisdictions. For example, under the South Australian *Whistleblowers Protection Act 1993*, anyone who discloses 'public interest information' is protected. While the definition of 'public interest information' covers

such public sector wrongs as the maladministration of public officers, the irregular use of public money and the substantial mismanagement of public resources, it also includes wrongs that could equally be perpetrated by the private sector. For example, it covers illegal activity or conduct that causes a substantial risk to health and safety, or to the environment.

The Queensland *Whistleblowers Protection Act 1994* also protects public interest disclosures, which include those that relate to a substantial and specific danger either to the health and safety of a person with a disability or to the environment, or if the disclosure is of a reprisal taken against a person who themselves made a public interest disclosure.

Limited protection is also provided in the case of those who provide information or documents to the ACCC or to the Australian Competition Tribunal. Section 162A of the *Trade Practices Act 1974* (Cth) provides for penalties of up to 12 months' imprisonment for individuals and fines of up to \$10,000 for corporations who intimidate individuals who report matters.

The desirability of offering such protection to those outside the public sector is supported by Standards Australia in its Standard AS 8004-2003 *Whistleblower Protection Programs for Entities* as part of its Corporate Governance package. In the Foreword to that Standard, it stated that:

A whistleblower protection program is an important element in detecting corrupt, illegal or other undesirable conduct... within an entity, and as such, is a necessary ingredient in achieving good corporate governance.

An effective whistleblower program can result in–

- (a) more effective compliance with relevant laws;
- (b) more efficient fiscal management of the entity through, for example, the reporting of waste and improper tendering practices;
- (c) a healthier and safer work environment through the reporting of unsafe practices;
- (d) more effective management;
- (e) improved morale within the entity; and
- (f) an enhanced perception and the reality that the entity is taking its governance obligations seriously (Standards Australia 2003, p.4).

Standard AS 8004-2003 sets out a number of elements of a desirable whistleblower protection program. For example, a whistleblower protection policy should be established that articulates 'the benefits and importance to the entity of having such a program as well as the sanctions and disciplinary procedures for non-compliance with the entity's whistleblower protection policy' (Standards Australia 2003, p.8). There should also be procedures in place for handling any reports received.

### **Evaluating Mandatory Reporting Legislation**

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.

There are also some statutory obligations in some jurisdictions for public sector agencies, other than local government, to report cases of suspected fraud to State Auditors-General and Ministers for Finance. In Victoria, for example, Procedure (c) under Direction 4.3 of the Standing Directions of the Minister for Finance states that the Auditor-General and the Minister for Finance must be notified of 'all cases of suspected or actual theft, arson, irregularity or fraud in connection with the receipt or disposal of money, stores or other property of any kind whatsoever under the control of a Public Sector Agency' (Department of Treasury and Finance 2003).

In the private sector there are certain circumstances in which an obligation arises to report fraud. For example, there is an obligation on financial dealers to report fraud committed by licensees to the Australian Securities and Investments Commission, and there are now obligations on company auditors to report certain matters following the passage of the *Corporate Law Economic Reform Program (Audit Reform and Corporate Disclosure) Act 2004*.

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.

Recently, the Victorian Parliamentary Drugs and Crime Prevention Committee (2004) suggested the enactment of legislation to make it obligatory to report fraud to a central reporting agency, and to create a criminal offence of failure to report a serious offence involving dishonesty where the victim believes that any financial loss suffered amounts to at least \$100,000. If such a proposal were introduced, it would be essential for 'fraud' to be defined precisely so that it would be clear exactly what kinds of dishonesty need to

be reported. There would also be significant resourcing implications for law enforcement if fraud reporting increased substantially.

### Coordinating Avenues of Reporting for Complainants

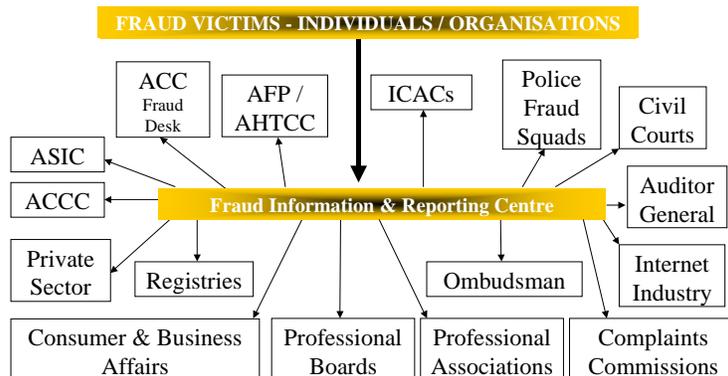
At present there is a wide variety of organisations to whom incidents of suspected fraud or corruption can be referred (see Figure 2).

**Figure 2 – Current Avenues of Complaint for Fraud Victims**



Establishing a single central agency which could receive reports from all sources and which could coordinate investigatory action by sending reports to appropriate agencies would help to ensure that victims know exactly to whom suspected incidents should be reported (see Figure 3).

**Figure 3 – Proposed Avenues of Complaint for Fraud Victims**



Creating simple and efficient electronic reporting systems, including the establishment of a hotline for reporting public or private sector fraud, would also make reporting easier than at present. Providing regular feedback to complainants about what is being done

with their cases would also help to raise confidence in the system and would avoid duplication of investigatory activities involving witnesses, such as the conduct of multiple interviews.

In Victoria, the Victorian Parliamentary Drugs and Crime Prevention Committee (2004) recommended the establishment of a central fraud reporting agency within police to act as a clearinghouse for complaints. That agency would receive reports, compile statistical information, and then transmit reports to relevant agencies for investigation. For example, a complaint involving misleading and deceptive practices concerning the sharemarket on the Internet could be referred to the Police, the Australian High Tech Crime Centre, the Department of Business and Consumer Affairs, the Australian Securities and Investments Commission and other agencies at federal and state level. Victims of fraud would, thus, only need to approach one agency to make their report.

The Committee further recommended that the central agency produce a best practice guide to reporting fraud, including a description of what information should be provided. The Committee suggested that the guide should contain specific information on preparing reports where the matter is likely to require further police action to be taken.

## **Conclusion**

In order to encourage organisations and individuals 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.

Hopefully, if these initiatives are implemented not only would fraud reporting increase, but as a consequence, the actual incidence of fraud may be reduced once it becomes apparent that crimes of dishonesty will result in official action being taken. Encouraging individuals to report their suspicions of fraud, if handled in a sensitive manner, will have benefits for organisations and the community as a whole.

## References

Charlton, K and Taylor, N. 2004, *Online Credit Card Fraud Against Small Businesses*, Research and Public Policy Series No 60, Australian Institute of Criminology, Canberra.

Department of Treasury and Finance, Victoria 2003, *Standing Directions*, State Government of Victoria, Melbourne.

Ernst & Young 2003, *Fraud: The Unmanaged Risk*, Ernst & Young, Johannesburg.

KPMG 2001, *Global efr@ud Survey*, KPMG Forensic and Litigation Services.

KPMG 2002, *Fraud Survey 2002*, KPMG, Sydney.

KPMG 2004, *KPMG Fraud Survey 2004*, KPMG, Sydney.

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

Standards Australia 2003, AS 8004-2003 *Whistleblower Protection Programs for Entities*, Standards Association of Australia, Sydney.

Taylor, N. 2002, 'Reporting of Crime by Small Retail Businesses', in *Trends and Issues in Crime and Criminal Justice*, No. 242, Australian Institute of Criminology, Canberra.

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.

Victorian Parliamentary Drugs and Crime Prevention Committee 2004, *Inquiry into Fraud and Electronic Commerce: Final Report of the Drugs and Crime Prevention Committee*, Parliament of Victoria, Melbourne.