AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 127

Organisations as Victims of Fraud, and How They Deal With It

Russell G. Smith

When we think of victims of crime, we often focus on those who suffer from violent, personal crimes such as assault or rape. Businesses and other organisations, however, may also be victims of crime—usually economic crimes, such as those that involve fraud and deception. The effects of those crimes can be devastating, with companies wound up and their employees forced to leave. Those who have invested in the organisation may lose all or part of their capital. Fraud against public sector agencies affects us all through loss of government resources.

This paper relates how organisations respond to commercial crime. It identifies the scope of the problem and details a number of ways in which those who manage organisations are best able to deal with it. Often fraud is "swept under the carpet", with those responsible dismissed without further consequences. There are compelling reasons, however, why fraud should be reported to the authorities. The author considers those reasons and describes ways in which organisations can be encouraged to report economic crimes to the police.

Adam Graycar
Director

Organisations vary greatly in size and scope—from small business partnerships to medium-sized corporations and multinational enterprises. Each may be victimised through crime, with the losses being sustained either by the individual proprietors of an unincorporated association, or by the shareholders of a corporate entity. If the crime is large enough, the business may be forced to close or the company may be wound up, in which case employees may lose their livelihoods and shareholders may lose all or part of their investment. Fraud directed at organisations within the public sector has a direct impact on government revenue. Clearly, crimes that are directed at organisations initially affect particular individuals and, eventually, the whole community.

Organisations may be victimised in a wide variety of ways, and by a range of people. Rarely, they will suffer from crimes of violence such as bombs being used against buildings or staff being victimised through acts of extortion. Most often, their experience of crime will be economic, and acts of fraud and deception will constitute the principal type of economic crime from which they suffer. They may also be victimised through infringement of intellectual property rights or acts of industrial espionage. Offenders may come from outside the organisation or from within, and may be either lower level employees or managers.

This paper examines the nature and extent to which organisations are victimised through fraud and deception, and how the problem may best be dealt with. It focuses on the way in which

September 1999

ISSN 0817-8542
ISBN 0 642 24121 X

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9200
Fax: 02 6260 9201

For 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

fraud is reported within organisations and the barriers organisations face in making effective use of the criminal justice system.

The Nature and Extent of Fraud Against Organisations

In recent years, a number of surveys have been carried out to determine the extent to which organisations have been victimised through fraud; that is, crimes which entail an element of deception in which the offender seeks to derive some financial benefit. Although victimisation surveys have been criticised on a number of grounds to do with the unrepresentative samples they employ and the limited types of activities that they examine, they do provide information other than that recorded in official police statistics. In the area of fraud, police statistics record only the most general information.

Surveys of business victimisation have been carried out regularly by two large firms of accountants, KPMG and Ernst & Young. These surveys have dealt specifically with the fraud experiences of large organisations and have provided an indication of the nature of organisational fraud and the extent of losses suffered. Although the response rate to these large-scale surveys has been rather low, they provide a good starting point for documenting the nature and extent of fraud in recent years.

KPMG survey

KPMG's latest Fraud Survey examined over 1800 of Australia's largest businesses in February 1999. Twenty per cent (367) replied, with information being provided on fraud awareness, the experience and cost of fraud, the perpetrators of the fraud, how it was discovered, and why it occurred. Information was also provided on action taken and fraud prevention steps relied upon. Specific data were also obtained concerning computer-related fraud. In all, some 7280 incidents of fraud were reported in the two years preceding the survey and 57 per cent of respondents reported at least one incident during that period. Sixty-nine per cent of those who had been victimised had suffered more than one incident, with the majority reporting between two and 10 incidents. Total losses amounted to $239 million (KPMG 1999).

The three industry groups that reported the largest numbers of incidents were the insurance, communications, and retail, wholesale and distribution industries, with financial services, insurance and government organisations reporting the greatest losses.

Since KPMG's previous survey was undertaken in March 1997, some improvements have occurred. In 1997, 100 per cent of communications organisations reported being victimised through fraud whereas in 1999, this had reduced to 85 per cent. Similarly, 100 per cent of tourism and hospitality organisations reported fraud in 1997, and this had reduced to 60 per cent in 1999 (KPMG 1997).

As in previous years, most frauds were perpetrated by employees of organisations rather than by outsiders. In 1999, only 22 per cent of fraud was carried out by parties external to the organisation. Interestingly, 21 per cent of fraud was carried out by managers, the largest proportion of which involved making improper claims on expense accounts. The highest proportion of fraud carried out by persons outside the organisation involved stealing property belonging to the organisation, such as stock and machinery; submitting forged cheques; and making improper use of credit cards.

Ernst & Young survey

The firm of Ernst & Young has also undertaken fraud victimisation surveys of its clients since 1989. The latest international survey, conducted in October 1997, surveyed 11,000 senior executives in major organisations in 32 countries, of whom 1205 (11%) replied . Approximately three-quarters of respondents reported being victimised during the preceding five years, with more than half having been defrauded in the preceding 12 months. Over 70 per cent of the 84 Australian respondents and 88 per cent of the 59 respondents in the United States had experienced fraud in the preceding 12 months. The total value of the worst frauds suffered by respondents in the preceding 12 months was US$628 (A$941) million, with one in five Australian respondents experiencing frauds in excess of US$1 ($A1.5) million. One Australian respondent alone lost US$25 ($A37.5) million in the 12-month period (Ernst & Young 1998). More than half of the frauds were committed by long-term employees who had been with the organisation for more than five years—it was these employees who were aware of the organisation's fraud control policies and knew how they could be circumvented.

Deakin University survey

In 1994, Deakin University, in conjunction with the Victoria Police Major Fraud Group, conducted a survey of the fraud victimisation experiences of 477 medium or large businesses in Victoria. Data were collected on 22 fraud categories, the most frequently mentioned of which involved theft of property belonging to the business, such as stock and equipment (251 cases—25%) and theft of cash (162 cases—16%). Losses for these two categories were estimated to be $284.67 million and $165.9 million respectively (Deakin University 1994).

Persons within organisations were involved in 78 per cent of cases reported, whilst persons outside the organisation accounted for 22 per cent of cases. The types of fraud most frequently carried out by persons within the organisation related to

false or inflated claims on travel or expense accounts (91%) and payroll padding—making improper claims in respect of salaries—(91%), whilst passing worthless cheques (84%) and overcharging by suppliers (74%) were most often carried out by persons external to the organisation.

Information Technology Fraud Against Organisations

One area of victimisation which is increasingly concerning organisations is that arising out of the use of computing and communications technologies. Between 1997 and 1999, there was a 71 per cent increase in the percentage of respondents to KPMG's surveys who reported computer-related fraud (from 7% to 12%). Total reported losses due to computer crime were over $16 million in KPMG's 1999 survey, although these figures are likely to be underestimates as many organisations were unaware of the extent to which their organisation was being defrauded through the use of computers, and some did not define other forms of fraud as computer-related (such as fraud involving electronic funds transfers or the creation of false identities through the use of desktop publishing equipment). In 1999, 36 per cent of KPMG's respondents who reported computer crime were either unaware of how much they had lost or were unwilling to disclose it.

Of the 84 Australian organisations surveyed by Ernst & Young (1998), 80 per cent believed that they were vulnerable to computer fraud, which was considerably higher than in other countries.

In November 1998, a survey of 350 large Australian organisations was carried out (Victoria Police and Deloitte Touche Tohmatsu 1999). Thirty-three per cent of respondents reported unauthorised use of their computers within the preceding 12-month period and one-quarter of these attacks were motivated by financial gain. More than one-third of those who responded believed that computer theft would have an impact on their organisation over the next five years.

High-technology fraud against government organisations is an area of particular concern as agencies become increasingly reliant upon computers for the provision of services and the payment of benefits. In the survey of computer crime and security conducted by the Office of Strategic Crime Assessments and the Victoria Police Computer Crime Investigation Squad (1997), 36 per cent of the 11 government agencies surveyed reported misuse of their computer systems, with 45 per cent reporting external forms of attack, that is remote access to computer systems. The most common types of computer abuse reported by the government agencies surveyed related to damage or unauthorised access to, or copying of, data and programs.

In the future, government agencies which make use of electronic commerce may be victimised in a variety of ways (see Smith 1999), and appropriate security procedures will need to be established in order to prevent the abuse of on-line payment and claiming systems.

Dealing With Fraud Against Organisations

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) found, for example, 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 or by dismissing the individual in question. Ernst & Young's (1998) study 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 for not reporting fraud to the police that were given by the respondents to Deakin University's (1994) survey 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.

Reluctance to report fraud is 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 staff involvement in court hearings.

The other disincentive to taking official action lies in the reluctance of organisations to publicise the fact of their victimisation. They fear 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, the organistion may not wish to draw undue attention to illegal activities within it.

As a result, many organisational victims simply take no official action, preferring instead to warn or to dismiss the perpe-

trator and to tighten security procedures to prevent a recurrence of the incident. 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.

Any general deterrent effects on the rest of the staff may be diluted or negated if the illegal conduct of one of their number fails to result in official action. This may lead to a more generalised downgrading of the ethical standards within the organisation as management are 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 are identified and implemented. It may be possible, for example, to make use of computer programs that analyse business transactions in order to identify patterns which have previously been found to be indicative of fraud. 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 not be felt. Effective reporting could 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 & Gover 1999). In the context of organisations, the same is very likely to be the case.

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).

In recent years, more and more organisations seem to be developing fraud control policies. In the survey conducted by Deakin University in 1994, only 27 per cent of those surveyed had fraud prevention policies in place (Deakin University 1994). In November 1995, 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). In Ernst & Young's most recent fraud survey, almost three-quarters of the 84 Australian respondents indicated that their organisation had an explicit policy on fraud reporting (Ernst & Young 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 occasion 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 police and the courts would respond effectively to the matter, and that the personal costs and time associated with the investigation and prosecution of the matter could be minimised. A variety of reforms could be made to the way in which cases are dealt with in the criminal justice system. Streamlining interviewing procedures and reducing the necessity for senior witnesses to be present in court for unnecessarily lengthy periods of time could help to reduce the time which organisations devote to the prosecution of cases. Documentary evidence should also be used wherever possible in preference to oral testimony, 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 & Young's 1998 survey, more than 50 per cent of respondents were opposed to the idea, with most opposition coming from company directors. In KPMG's 1999 survey, only one per cent of 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. The law already requires, in certain circumstances, that individuals who become aware that they have been defrauded must bring the matter to the attention of the police. Subsection 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 for misconduct being taken against the professional in question. 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).

If such mandatory reporting obligations were enacted, appropriate safeguards would also have to be introduced to protect those who report their suspicions of fraud from personal liability, where they act in good faith.

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 that are reported simply cannot be investigated because law enforcement agencies are underresourced, particularly for the investigation of serious, complex and time-consuming allegations involving fraud and deception.

An additional impediment to the reporting of fraud lies in the fear which some individuals have of reporting matters in the public interest, where this may result in their being discriminated against or otherwise being subjected to harassment, intimidation or reprisals. The problem of so-called "whistleblowers" has been documented in a number of studies of individuals who have reported corruption in public sector agencies.

De Maria and Jan (1996), for example, conducted Australia's largest study into whistleblowers, and 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 used in appropriate cases to protect those who report fraud in the public interest. 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.

Changes might also need to be made to the sentencing dispositions and practices used by the criminal courts. Provision should be made in all jurisdictions for the confiscation of assets and priority in paying compensation to organisational victims, in order to maximise the chances of recovery of the losses occasioned by fraud (see, for example, s. 86 *Sentencing Act 1991* (Vic.) and s. 30 *Confiscation Act 1997* (Vic.)).

In addition, more imaginative sanctions could be considered for serious corporate offenders. Braithwaite (1992, p. 170), for example, describes the utility of so-called "equity fines", in which companies are ordered to issue a certain proportion of new shares which are given to victims or to the state. For example, if a court ordered a corporate offender to issue one new share for every 100 already issued, the market value of all shareholdings would be reduced by one per cent. The company would still be able to operate although shareholders would be penalised.

In appropriate cases other, non-custodial sanctions should also be used, such as apologies, adverse publicity, specifically targeted community service and corporate disqualification. Although those who suffer loss as a result of fraud often consider imprisonment to be the only appropriate sanction, other punishments that affect an offender's livelihood, reputation and ability to earn a living may, in fact, give rise to greater deterrent effects.

Conclusions

This paper has examined the nature of fraud victimisation suffered by organisations and considered some ways to increase the likelihood of offences being reported and dealt with through official avenues of redress. On the basis of a number of recent organisational victimisation surveys, fraud is clearly seen as being a considerable problem

for businesses, with its effects felt throughout the community. Computer-related fraud is causing particular concern amongst organisations, although its precise extent cannot as yet be quantified with precision.

Risk management and fraud prevention activities are clearly preferable to the use of criminal prosecution and punishment once illegal conduct has been carried out, and a high proportion of organisations now have extensive fraud control policies in place. These should be widely publicised and regularly updated to deal with new forms of risk as they arise.

Although effective fraud prevention should be the primary objective of all managers (see Smith 1998), the use of the criminal justice system is still necessary in order to achieve general and specific deterrent effects. In the case of white collar offenders, who can be said to carry out their activities on the basis of some rational calculation, deterrence remains an important component of fraud control. The confiscation of assets, in particular, represents one of the most effective means of achieving deterrence in the case of economic crime.

Deterrence can best be achieved, however, if offences are reported to the authorities. This paper has canvassed a number of ways in which organisations can be encouraged to report fraud, and a number of ways in which favourable outcomes can be achieved in criminal proceedings. By dealing with fraud through criminal prosecution and punishment, the community as a whole benefits from the knowledge that wrongdoing has been detected and sanctions imposed, whilst victims may be able to receive some measure of compensation for losses suffered. There are also important benefits to be derived through identifying and publicising ways in which organisations may be able to avoid victimisation through fraud in the future.

References

Braithwaite, J. 1992, "Penalties for white-collar crime", in *Complex Commercial Fraud*, ed. P. N. Grabosky, AIC Conference Proceedings no. 10, Australian Institute of Criminology, Canberra, pp. 167–71.

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

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

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

—— 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.

Office of Strategic Crime Assessments and Victoria Police 1997, *Computer Crime and Security Survey*, Attorney-General's Department, Canberra.

Smith, R. G. 1998, *Best Practice in Fraud Prevention*, Trends and Issues in Crime and Criminal Justice, no. 100, Australian Institute of Criminology, Canberra.

—— 1999, *Defrauding Governments in the Twenty-first Century*, Trends and Issues in Crime and Criminal Justice, no. 111, Australian Institute of Criminology, Canberra.

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

Titus, R. M. & 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.

Victoria Police and Deloitte Touche Tohmatsu 1999, *Computer Crime and Security Survey*, Victoria Police Computer Crime Squad and Deloitte Touche Tohmatsu, Melbourne.

Dr Russell G. Smith is a Senior Research Analyst at 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.