Speech delivered by Adam Graycar:

"Fraud prevention and control in Australia"

at the Australian Institute of Criminology Fraud Prevention Conference, Gold Coast, 24 August 2000

© Australian Government
This speech is made available under the CC-BY-NC-ND 4.0 license:
http://creativecommons.org/licenses/by-nc-nd/4.0/
Fraud Prevention and Control in Australia

Australian Institute of Criminology
Fraud Prevention Conference
Gold Coast

24 August 2000

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

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

Fraud involves the use of dishonest or deceitful conduct in order to obtain some unjust advantage over someone else.

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

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

Fraud is not specifically defined by legislation in Australia, but everybody seem to know what it is (except some who commit it, and purport to have no idea that what they had done was wrong!). It is, like an elephant, easier to recognise than it is to define!

Both individuals and organisations may be the victims of fraud.

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 over time. In Victoria, for example, police statistics record over 100 separate offences included in the category ‘deception’. These include various forms of obtaining property by deception, forgery, conspiracy, impersonation, secret commissions, and making false statements.

Whichever way we look at it, fraud is a crime, and despite protestations of all sorts, nothing mitigates that.

Every crime requires three ingredients: a motivated offender, a suitable target and an opportunity. We have our work cut out for us in developing policies and practices to

- Try to reduce the supply of motivated offenders
- Protect and educate the suitable targets
- Limit opportunities by making the crime more difficult to commit
In exploring these ideas we confront policy agendas of considerable complexity. We also find ourselves confronted by boundaries, which on the surface can be easily mapped, but which, in reality sometimes appear convoluted and unconquerable. When we add a dose of technology to the boundaries then we are confronted with complex jurisdictional and technical issues, especially if the victim and offender are in different places, and the money has moved at the speed of light through cyberspace.

The key to attacking fraud is to work in partnerships to attain the objectives just listed.

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

⇒ To deal with the second objective, protecting and educating the targets of fraud is a crucial part of the prevention equation. It involves a knowledgeable and informed public able to identify an offer which appears “too good to be true” as well as a mechanism for keeping new information flowing, at both an individual and organisational level. This goes hand in hand with a fraud control policy.

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

These are some of the things I will deal with in this talk today.

The Extent of Fraud in Australia

It is confidently assumed that fraud costs the nation more than any other type of crime. The Australian Institute of Criminology estimated that fraud comprised about 16% of the total annual cost of crime, and in 1996 that was estimated to be between $3 and $3.5 billion (based on a submission from the Australian Federal Police, to AUSTRAC). However, any dollar figure can only be a guess, although in individual cases losses are often calculated to the exact cent.

There are a number of ways in which to estimate how much fraud takes place in Australia. Official statistics give an insight into crimes that come to the attention of the police, while business victimisation surveys provide information concerning those who have suffered at the hands of fraudsters. Anecdotal historical accounts of high-profile crimes also document how fraud takes place and how much it costs the community. Using each of these sources, fraud stands out as enormously costly, and a crime that has affected all sectors of society throughout history, even though dollar estimates are often no more than guesses.
The financial journalist, Trevor Sykes, for example, has a lot of stories to tell. In his book, *Two Centuries of Panic* (1988), he documents corporate collapses in Australian history since the turn of the nineteenth century until some of the building society and financial institution collapses of the 1970s. In another book, *The Bold Riders* (1994), Sykes examines the corporate collapses of the 1980s concluding that these collapses and the associated fraudulent activities of some of the financial entrepreneurs were facilitated through unsound lending policies of the banks and the rise of fringe financial institutions.

Official statistical information shows that small scale fraud convictions increased substantially during the 1930s depression years but decreased during and after the Second World War when many young men were away. Throughout the 1950s and 1960s there was a large increase, and in general, fraud boomed between the late 1980s and 1991 around and following the time of the economic boom and subsequent collapse of the share market on 20 October 1987. (Institute of Chartered Accountants 1998).

During the early 1990s, there was a decline, which may be due to the effects various fraud control initiatives taken by some public and private sector agencies such as the insurance industry. Over the last few years, however, the rate has again begun to increase which may indicate a greater willingness to report fraud to the police, as already mentioned. These trends may also, of course, reflect changes in the underlying incidence of fraud in the community.

In order to estimate the actual incidence of fraud committed, surveys of business victimisation are regularly conducted by some of the large international firms of accountants and consultants.

KPMG’s latest Fraud Survey (1999) examined over 1,800 of Australia’s largest businesses in February 1999. 367 replies were received (20%) with information being provided on fraud awareness, the experience and cost of fraud, who perpetrated the fraud, how it was discovered, and why it occurred. Twelve per cent of respondents were unwilling to disclose the extent of their losses or were unable to quantify them. Although two per cent of respondents reported having lost over $5 million in the two year period surveyed, most organisations reported losses of between $10,000 and $500,000 each. In the absence of more consistent and widespread policies on fraud reporting, we are unlikely to know exactly how much fraud is costing Australia.

**Responses**

It is obvious that different types of fraud require different responses. This paper will not describe the many types of fraud listed in the opening, and will confine responses to functional response - those that can be described as systemic or legal.

**SYSTEMIC RESPONSES TO FRAUD**

The key to fraud prevention on the part of organisations, whether of the public or the private sector, is the development and refinement, of an effective 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 complex corporate fraud is to ensure the greatest possible transparency of corporate transactions.

Surveys have found that most frauds were perpetrated by employees of organisations rather than by outsiders. In the 1999 KPMG survey it was found that only twenty-two per cent of fraud was carried out by parties external to the organisation. The highest proportion of fraud carried out by outsiders related to theft of inventory and plant, forgery of cheques, and credit card fraud.

This poses us with challenges for both reducing the supply of motivated offenders and making the frauds harder to commit. Both can be achieved by looking at corporate governance, and various private sector initiatives.

Corporate Governance

It is now widely accepted that effective fraud prevention strategies must, in the first instance be generated from upper-level management. If chief executive officers and managers at all levels have a commitment to fraud prevention and understand how it may be achieved, this will provide a foundation for other employees to support the notion of fraud control.

Achieving this aim presents difficulties, however, in view of recent research which has demonstrated that most fraud is perpetrated by managers themselves who make purchases for personal use, misuse expense accounts or misappropriate funds (KPMG 1999). Some of Australia’s largest corporate frauds have also been characterised by chief executive officers who exercise unfettered power, and boards of directors who are unwilling to challenge that power. This makes the establishment of effective codes of practice and the creation of an ethical environment in the workplace difficult to achieve as such initiatives may challenge directly those in charge of the company who may, themselves, be the primary offenders.

Another impediment to management taking a stance on fraud control is simple lack of understanding of how their organisations function in sufficient detail to be fully aware of the risks of fraud which exist. In Ernst and Young’s survey of large organisations, for example, less than one third of the Australian respondents considered that their directors had a good overall understanding of their business for fraud prevention purposes (1998).

Where it has been proved that company directors have acted dishonestly or in breach of the Corporations Law, it is essential that they not be permitted to repeat their illegal conduct at the same or at some other corporation. Sub-section (3) of section 229 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 from acting in the management of a company. This information is readily accessible to the public through information brokers as well as the Internet (http://www.asic.gov.au/).
As we live in a global economy, international markets increasingly require conformity with global standards. Today, best practice in corporate governance will require a degree of independence on a board of directors, and the existence of an audit committee comprised of board members. Among the functions of such a committee are the selection of independent auditors for the company, and the review, in collaboration with the external auditors, planning and results of the audit engagement. The committee also reviews the results of the audit, and recommendations made by the auditors, as well as the planning and results of the internal audits. On top of this is the necessity of corporate disclosure, so that markets are kept fully informed of a company’s activities.

Given the difficulties in prosecuting fraud, there has been increasing reliance in recent years placed on civil remedies as a complement or as an alternative to criminal prosecution. In contrast to the criminal law, which requires proof beyond reasonable doubt of intent to defraud, civil remedies only require proof on the balance of probabilities. Civil actions have prevailed not only against the perpetrators of fraud, but also against auditors who have been found negligent in the performance of the audit function. The quantum of damages which might follow a successful civil action could be formidable, and act as a significant deterrent, at least where it is possible to gain access to seizable assets. Civil remedies also provide for a degree of compensation to the victim which might not otherwise flow from the criminal process.

**Private Sector Initiatives**

Increasing recognition that the best line of defence against fraud is self-help has moved many private sector organisations to introduce and to improve fraud control systems. To this end, they are aided significantly by the burgeoning industry of loss prevention services. Failure to have effective fraud prevention and compliance systems in place may, in the future, result in corporations being subjected to civil and criminal penalties, not to mention bad publicity, poor profitability, and disruption to their operations.

The need for businesses to develop and to implement effective fraud control policies has been affirmed with the publication of Australian Standard No. AS 3806-98 *Compliance Programs*, which provides guidelines for both private and public sector organisations on the establishment, implementation and management of effective compliance programs.

One of the most comprehensive private sector fraud control policy documents is BHP's *Guide to Business Conduct* (1997). This 54 page, clearly indexed booklet, which is available in various Asian languages, provides guidance for employees and managers in dealing with business conduct and in helping them to understand and to take responsibility for business conduct issues. Issues canvassed include general principles for conducting business, ensuring compliance with legal requirements, how to identify and to avoid dishonest and unethical business practices and how to respond to conduct which appears to be in breach of the guidelines, such as through the use of the BHP Business Conduct Helpline.

Many large accounting firms have established departments or subsidiaries specialising in fraud prevention. Their products range from a total review of risk management practices to more narrowly focused issues such as security of information technology systems.
Private fraud control services are by no means limited to prevention. Private organisations which find themselves the victims of fraud may retain their own in-house investigators, or may engage specialised fraud investigators residing in the private sector. These private investigators may conduct an entire investigation, handing the matter over to the police for prosecution. This is common in the Australian insurance industry in response to insurance fraud.

Public Sector Initiatives

Public sector fraud takes many forms. The vulnerabilities to fraud exist along three main dimensions:

- individuals claiming benefits to which they are not entitled;
- individuals evading payments due to government; and
- individuals who contract with government to provide goods or services, failing to act as they have contracted to do.

Because government agencies such as the Australian Tax Office or Centrelink deal in such large sums of money, the potential losses due to fraud are considerable. The Australian National Audit Office’s (2000) recent survey of fraud control arrangements in public service agencies, for example, found that $145,862,000 was reported to be lost to fraud by 106 agencies in 1998-99. There is no doubt that Australian Governments have become increasingly sensitive to fraud risks.

The design of systems can be an important means of fraud prevention. The introduction of a requirement that the recipients of public funds have an account with a financial institution in which the funds can be deposited automatically, has dramatically reduced the risk of lost or stolen cheques, or fraudulent claims. Automated payment also reduces clerical costs.

An important strategy introduced in the early 1990s to control revenue fraud involved the establishment of an extensive database by the federal government which sought to reduce taxation and social security fraud, by identifying individuals who have made claims for benefits from government funds to which they are not entitled. The Parallel Data-Matching Program (PDMP) which was introduced in 1991 by the Data-Matching Program (Assistance and Tax) Act 1990 (Cth), makes use of tax file numbers and permits income records to be compared with payment records held by various benefit providing departments.

The Fraud Control Policy of the Commonwealth outlines the principles of fraud control and develops national standards. Although the policy relates only to Commonwealth government departments, and does not encompass any enforcement function, it provides a consistent set of policies and directions to assist departments in carrying out their responsibilities to combat fraud against their programs. These include agency responsibilities for fraud prevention, reporting of fraud information, fraud investigation case handling and training of agency fraud investigators.

Significant advances have also been made by various State and Territory government departments in developing fraud control policies. The Australian Capital Territory Government Service Fraud Prevention Unit, for example, has established a fraud control
policy in accordance with the *Public Sector Management Standards* on Fraud Prevention. The policy sets out the responsibilities of managers and employees in relation to fraud control, describes the investigatory functions of the Fraud Prevention Unit and details the procedures for reporting fraud and corruption. Section 9(t) of the *Public Sector Management Act 1994* (ACT) requires public employees to report suspected fraud while the *Public Interest Disclosure Act 1994* (ACT) provides protection against reprisals for those who report fraud and corruption in good faith (ACT Government 1994). There are other examples in other jurisdictions.

**LEGAL RESPONSES TO FRAUD**

Dishonest and fraudulent behaviour is able to be dealt with using a variety of legal responses in addition to informal sanctions such as dismissing an employee who has defrauded a business, or what is known in the dispute resolution literature as ‘exiting’ a problematic situation (Hirschman 1970). Often an organisation which has suffered loss through fraud may be unwilling to incur further time and expense in pursuing legal remedies, be they in the civil or criminal courts.

Some may also view the benefits which may follow from reporting fraud to other regulatory agencies as plainly inadequate, and take no action at all. By refraining from taking legal action, the potential benefits to an organisation, as well as to the wider community, in terms of individual and general deterrence will be lost, leaving the offender potentially free to repeat the dishonest conduct at the same or another place of employment, and providing no external sign to the rest of the community that fraudulent behaviour is unacceptable.

Criminal fraud has traditionally been dealt with through the legal processes of investigation employing publicly-funded police services, prosecution by state-administered prosecution agencies, trial in the criminal courts often employing juries, and punishment in the state-administered correctional system.

In recent times, however, many of these functions have been taken over by privately-funded agencies usually working in conjunction with their publicly-funded counterparts. Financial considerations have meant that only the most serious cases involving substantial monetary losses are likely to be fully investigated and tried, with the attendant possibility of convicted offenders receiving the most severe sanction of a term of imprisonment. The legal response to fraud control has, therefore, been severely restricted, although the possibility of criminal prosecution and sanction has always remained open.

**Fraud Reporting**

The first barrier to the criminal prosecution of an allegation of fraud lies in encouraging those who have suffered loss at the hands of offenders to report their complaint to the authorities. Some, however, such as those who fall prey to bogus charitable solicitations, may never realise that they have been defrauded. Where individuals are, in fact, aware that they have been defrauded, the law requires, in certain circumstances, that they bring this fact to the attention of the police.
Despite this requirement, there are powerful reasons why individuals may not wish to report offences of dishonesty to the authorities. KPMG (1999), for example, found in its survey of businesses, that one third 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. Other surveys have found that 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.

Various inducements may be needed to enhance the reporting of fraud. These may include guarantees of anonymity where this is necessary to protect a business reputation, assistance in reducing the personal costs and time associated with the investigation and prosecution of a matter, perhaps by streamlining interviewing procedures and reducing the necessity for senior witnesses to be present in court for unnecessarily lengthy periods of time, and for documentary evidence to be used in preference to oral testimony wherever possible.

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 (1998, p. 11).

Investigation and Policing

In addition to the reluctance of individuals to report fraud, are many problems associated with the effective investigation of cases. Offenders often go to considerable lengths to disguise their identity and to make documentary financial trails of evidence difficult to follow.

Those who seek to mask their identity through the use of computer networks are often able to do so, by means of ‘looping’, or ‘weaving’ through multiple sites in a variety of nations. Electronic impersonation, colloquially termed ‘spoofing’, can be used in furtherance of a variety of criminal activities, including fraud. Anonymous re-mailers and encryption devices can shield one from the scrutiny of all but the most determined and technologically sophisticated regulatory and enforcement agencies. As a result, some crimes may not result in detection or loss until some time after the event, thus making the process of investigation even more challenging.

Other issues which may complicate the investigation of computer-based frauds, entail the logistics of search and seizure during real time, the sheer volume of material within which incriminating evidence may be contained, and the encryption of information, which may render it entirely inaccessible, or accessible only after a massive application of decryption technology.
Public/Private Sector Partnerships

Partnerships are required among both public sector and private sector agencies to assist in the process of fraud investigation. In the future, the initial procedures associated with the collection and analysis of financial and business information in relation to cases of serious fraud will most likely be undertaken not by state-funded law enforcement bodies, but by individuals in the private sector and corporate entities themselves.

Private sector professionals, such as solicitors and accountants who act for corporations, have a primary responsibility to their client and the information they collect and the advice they give is directed toward the needs of the client who is paying for their services. Public sector law enforcement agencies, however, have primary responsibility to the community at large in detecting, investigating and prosecuting illegality. A tension thus exists between investigations which may assist the corporation in its future business affairs and investigations undertaken primarily for use in legal proceedings. A good example of this tension concerns the responsibilities of auditors in the examination of corporate financial statements.

To be effective, public and private sector bodies which engage in the investigation of fraud will be required to liaise closely with law enforcement personnel and prosecutors in order to ensure that evidence is obtained in such a way as not to prejudice its use in criminal trials or otherwise to result in critical evidence being lost or damaged. Such cooperation already occurs in many agencies, such as ASIC which works closely with private insolvency practitioners.

Recently, initiatives have been taken to establish comprehensive training programs for those involved in the investigation of fraud. Both the Victoria Police Major Fraud Group and the New South Wales Police Service’s Commercial Crime Agency have fraud investigators courses conducted by tertiary educational institutions which are now becoming open to non-police investigators. This will help to ensure that all those involved in the investigation of fraud and forensic accounting, both from the public and private sectors, understand the role and duties of each other and conduct investigations in a coordinated way.

Prosecution Policies

Having investigated a case of serious fraud, it then remains for the evidence to be presented to the relevant prosecution agency. It is at this point that serious fraud cases often founder, as prosecutors may believe that the evidence presented to them is inadequate or that the chances of success are insufficient to justify the time and expense involved in a lengthy trial.

The Commonwealth Director of Public Prosecutions maintains a dedicated group responsible for corporate prosecutions, and he will be speaking later today.

In 1992 the High Court of Australia in the case of *Dietrich v The Queen* ((1993) 67 ALJR 1) ruled that, unless exceptional circumstances exist, where a genuinely indigent accused person is unrepresented by counsel at a trial for a serious offence, the trial will be considered to be unfair and should be adjourned until legal representation is made available.
Few individuals are able to afford the costs associated with a long and complex criminal trial. Defendants charged with serious fraud are often able to arrange their financial circumstances in such a way as to make them appear indigent and thus able to take advantage of the *Dietrich* ruling. The effect may well be that a long and complex investigation will be stayed indefinitely.

**Trans-Jurisdictional Problems**

Because many fraud offences do not involve face-to-face interactions in their commission, it is possible for offenders and victims to be located in more than one jurisdiction. More sophisticated conspiracies may involve individuals in three or more jurisdictions within Australia or overseas. Few remedies are available to the unfortunate individual who might fall victim to such activities. Even if one is able to mobilise the law, the chances of locating the fraudsters, obtaining extradition, mounting a prosecution, or recovering compensation may be impossible.

Even where a perpetrator has been identified, two problems arise in relation to the prosecution of offences which have an international aspect: first, the determination of where the offence occurred in order to decide which law to apply; and, secondly, obtaining evidence and ensuring that the offender can be located and tried before a court. Both these questions raise complex legal problems of jurisdiction and extradition (*see*, generally, Lanham 1997).

In Australia, a package of measures was adopted in the later 1980s to facilitate the prosecution of organised crime and serious fraud. These included the *Mutual Assistance in Criminal Matters Act* 1987 (Cth) which established mechanisms to facilitate international cooperation between investigators with respect to obtaining evidence, the location of witnesses and suspects, the execution of search and seizure warrants, the service of documents, the forfeiture of property and recovery of fines and various other matters; the *Proceeds of Crime Act* 1987 (Cth) which enables investigators to follow the trail of the illegal proceeds of crime internationally and to confiscate assets; the *Cash Transactions Reports Act* 1988 (Cth) which established a government agency to monitor the movement of large-scale cash transactions; the *Extradition Act* 1988 (Cth) which extended Australia’s ability to enter into extradition arrangements internationally; and the *Telecommunications (Interception) Amendment Act* 1987 (Cth) which extended the ability of agencies to undertake electronic surveillance for law enforcement purposes. The International Branch of the Commonwealth Attorney-General’s Department administers these pieces of legislation.

**Court Processes**

The challenge for law reform in relation to complex fraud trials lies in striking a balance between the efficiency of the judicial system and the rights of individual offenders and victims involved in the prosecution.

The principal difficulties relate to the presentation of voluminous business and accounting records to a court, the difficulty of presenting complex financial transactions to a jury in such a way as to permit lay people, perhaps unfamiliar with business transactions, to understand the factual issues involved, and the length of time which such trials take, which
is often exacerbated in cases of criminal conspiracy by having multiple defendants and multiple charges (see, generally, Rozenes 1992).

Various reforms to court procedures have been introduced throughout Australia in recent years to reduce the length, complexity and cost of prosecutions, particularly those which involve substantial sums of money or complex factual circumstances. Computer technology, for example, has greatly facilitated the presentation and analysis of complex business dealings (see Livermore 1992). In addition, legal practitioners are now closely regulated with respect to the length, manner and nature of material which they present to the courts.

Legal Problems

At present in Australia each jurisdiction has its own laws and rules which regulate business activity, and this is not the time to do a lecture on federalism.

The problem of harmonising laws relating to fraud and the implementation of the Model Criminal Code in this area has been comprehensively addressed in the response of the Commonwealth Attorney-General’s Department to the proposed uniform legislation. The benefits of reforming the law in this area were graphically described in the Report as including the elimination of over 250 unnecessary and convoluted Commonwealth offences and the repeal and replacement of 150 offences in New South Wales alone (Commonwealth Attorney-General’s Department 1996, p. ii).

Sentencing

In Australia, the following judicial punishments are currently available in most jurisdictions:

- fines;
- restitution and compensation orders;
- forfeiture and disqualification (confiscation);
- unsupervised release (suspended, deferred, conditional sentences);
- supervised release (probation, community service, intensive corrections) and
- custodial orders (either full time or periodic).

In addition there are other consequences of wrongdoing which may be invoked: adverse publicity; professional disciplinary sanctions; civil recovery action; injunctive orders and, most recently, various forms of reconciliation or community conferencing which are being evaluated at present.

Little research has been carried out in Australia on the manner in which offenders convicted of serious fraud offences are dealt with following a criminal trial. A few prominent individuals have received wide publicity following their conviction when they have been sentenced to terms of imprisonment, but there is little that is systematic.

Proportionally few offenders are in Australian prisons serving sentences for offences involving fraud. Of Australia's 20,000 prisoners 3.5% of males and 10.5% of females have fraud/ misappropriation as their most serious offence.
There is a long debate about whether prison is more of a deterrent for white collar criminals than it is for those involved in street crime and violence. We would like to think that prospective offenders would more effectively be deterred through increased efforts at fraud prevention and enhanced rates of detection and reporting of offences. Increased spending on law enforcement activities might first be directed at detecting crime quickly and with certainty, and publicising this fact. In addition, increased spending on education, training in business ethics, and fraud prevention initiatives would produce benefits in terms of reducing fraud to complement expenditure on the incarceration of individuals.

Conclusion

As I observed earlier, fraud, like all crime, can be explained by the presence of three factors:

- motivation
- opportunity, and
- the absence of capable guardianship

The basic motivation for fraud is greed, an fairly robust and enduring human characteristic. We are unlikely to eliminate greed in my lifetime. This is not to disparage the ethicists among us. Theirs is a noble calling, and their efforts to improve humankind have met with some success. But the real payoffs in fraud prevention and control lie elsewhere.

Crime follows opportunity, and opportunities for fraud flow from economic growth. The more commerce there is, the more opportunities there are to commit fraud. We do not want to close down the stock market, or the health insurance system, or pull the plug on electronic commerce, just because they may be vulnerable to fraud.

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

And of course, capable guardianship implies surveillance of transactions to enhance the risk that fraud will be detected. This is the basis for auditing, which thanks to technology, can now occur in real time. It also implies the simple raising of awareness to enable ordinary Australians to identify offers that are too good to be true. This involves a partnership process in which we all can be capable guardians in the prevention of fraud.

The challenge for the years to come lies in understanding how new forms of fraud are perpetrated, and in ensuring that those charged with preventing and dealing with fraud have the intellectual and operational resources with which to do their work.

Reducing the risk of fraud without detracting from prosperity is the challenge which we face in the years ahead, and I hope that this conference will contribute to these goals.

Most fraud in the twenty-first century is sophisticated in planning and execution. It utilises computing and communications technologies and crosses jurisdictional boundaries.
with ease. The solutions, therefore, must acknowledge these characteristics. Fraud control needs to be sophisticated and needs to be carried out nationally and globally. Already we have seen considerable achievements in both these aspects. Policing already makes use of the most recent forensic computing techniques and cooperative partnerships are widely established within Australia and overseas.

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

Because it is usually those within organisations who perpetrate fraud internally, efficient measures need to be adopted to scrutinise staff when they are first appointed and to monitor their trustworthiness throughout the length of their employment. There are now sophisticated electronic technologies available that may be used to monitor the activities of staff and to ensure that they do not succumb to the temptations and opportunities for fraud which middle and upper management have to offer. Maintaining surveillance of staff must, of course, respect individual privacy and comply with laws that regulate surveillance, electronic monitoring, and the maintenance of databases containing personal information.

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

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

The challenge for the years to come lies in understanding how new forms of fraud are perpetrated and ensuring that those charged with preventing and dealing with fraud have adequate resources to do their work. As in most areas of crime control, it is better to allocate resources in preventing crime than in seeking to deal with the consequences after the problem has arisen.