AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 270

Identifying and Responding to Risks of Serious Fraud in Australia and New Zealand

Yuka Sakurai and Russell G. Smith

In their Trends and Issues *paper, "Red Flags of Fraud", Grabosky and Duffield (2001) identified a number of warning signals for fraud, or anomalies. While the existence of anomalies is not always indicative of criminality, they do signify heightened risks that should be investigated further. Drawing upon data collected for the Australian Institute of Criminology and PricewaterhouseCooper's study,* Serious Fraud in Australia and New Zealand *(2003), this paper identifies those circumstances or anomalies that were present in the cases of serious fraud examined. Understanding these factors will help those at risk of fraud victimisation to take action to prevent financial crimes from being perpetrated or to detect instances that have already begun at the earliest available opportunity.*

Acting Director
Toni Makkai

The Australian Institute of Criminology and Pricewaterhouse Coopers (AIC/PwC) recently examined a sample of Australian and New Zealand 'serious fraud'[1] cases within the calendar years 1998 and 1999. For the two years in question, the total amount in respect of which offenders were sentenced was $260.5 million, while the total actual loss suffered by victims was $143.9 million. Details on sample and methodology are provided in the Serious Fraud study (Australian Institute of Criminology and Pricewaterhouse Coopers 2003).

Identifying Anomalies

Recent studies have identified a number of circumstances that arise regularly in cases of serious financial crime (e.g. Ernst and Young 2002, KPMG 2001 and 2002, Krambia-Kapardis 2001). Part of the AIC/PwC study (2003) involved the examination of how cases were detected. Internal audit was the most frequently identified manner of discovery (19%), followed by cases in which offenders simply failed to make payments to creditors or investors (13%)—thus leading to complaints being made. A number of cases were also discovered during police investigations (11%) or inquiries by law enforcement agencies (10%). Despite research to the contrary (Association of Certified Fraud Examiners *Report to the Nation* (2002)) relatively few cases involved whistleblowers.

Internal auditing generally led to the discovery of accounting anomalies resulting from fraudulent transactions, such as those carried out by a bank employee or a company's financial manager. Behavioural anomalies associated with professional misconduct, such as professionals failing to make payments due to their clients, were detected often when the clients reported this to the police or other regulatory bodies.

While a large number of offenders failed to take effective measures to conceal their misconduct, it was apparent that many instances were difficult to detect. The mean period between the first offence and the last offence committed by a single offender was

December 2003

ISSN 0817-8542
ISBN 0 642 53822 0

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text 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

approximately two years, and the mean period between the last offence to the date of detection was an additional 10 months. In one instance, offences were committed over a period of almost 13 years without the illegal conduct being discovered.

Understanding Anomalies

What, then, are the anomalous circumstances that give rise to the commission of serious fraud and to its discovery?

Prudential Failures

- **Poor investment controls**

Where funds are invested either by corporations or individuals, it is critical for adequate steps to be taken to investigate the legitimacy of the entity to whom funds are provided and the adequacy of securities. Sometimes investment funds will be lost in so-called advance fee schemes in which capital is not at risk but supporting advance payments are stolen. This is the gist of the many West African-based schemes that currently operate globally.

On other occasions, the target is the investment fund itself which can be misappropriated by dishonest finance providers or lost if funds are placed in unacceptably risky ventures. In both cases, risks are created through investors failing to assess the legitimacy and security of individuals or organisations with whom investment funds are placed.

- **Poor cheque control procedures**

The absence of, or weak, financial control systems are often indicative of fraud risks (Grabosky & Duffield 2001). Poor cheque control procedures regularly lead to client or employee fraud. Procedures that permit signatories to sign blank cheques, the absence of formal cheque requisition forms, or the lack of verification procedures concerning information written on cheque butts, enable insiders to commit fraud. In one case an associate director of finance and administration of a company had access to company cheque books and authority to write cheques. There was, however, no requirement for cheque requisition forms to be prepared, thus enabling the offender to obtain money from the accounts without verification. Although two signatures were required, the offender was able to choose a person to counter-sign the cheques who was unaware of the nature of the transactions and willing to allow the cheques to proceed without further investigation.

Negotiation of valueless, stolen, forged, altered or counterfeit cheques is one of the high risk areas for financial institutions (Chapman & Smith 2001). With regard to valueless cheques, the clearance time between banking houses may permit a person to make substantial withdrawals from accounts without being financed sufficiently. In order to keep business ventures afloat, an offender passed valueless cheques for the amounts of $186,000, $204,000 and $80,000 respectively drawn on eight accounts held with two financial institutions. He was regarded as a 'particularly valued customer' of the banks, and was thus allowed to draw against cheques deposited immediately although none of the accounts had an overdraft facility. He was convicted and sentenced to a fixed term of 12 months' imprisonment to be served by way of periodic detention (R v *Bernard*, NSWCCA 156, 11 June 1999).

- **Failure to verify identification evidence**

Documentary evidence is generally used to establish one's identity when dealing with government agencies and in conducting business transactions (Smith 1999a). In one instance, 116 false identities were used by an individual to open credit card accounts and subsequently to obtain various goods and services on credit.

Recent advances in the technologies of desk-top publishing have made the preparation of counterfeit documents relatively easy (Smith, 1999b). In one recent case, the offender used computer scanning and printing equipment to create 41 birth certificates and 41 student cards in separate names. These documents were used to open 42 bank accounts in the Melbourne metropolitan region that were used for various illegal purposes (R v *Zehir*, Court of Appeal, Supreme Court of Victoria, 1 December 1998).

On occasions, offenders will make use of their physical similarity to the person whose identity is misused. In one instance an offender obtained a passport using his brother's expired driver's licence, his brother's Medicare card, an airline ticket, but containing a photograph, birth-date and signature of himself. These were used to support an application for finance to purchase various goods.

- **Failure to verify ownership of property**

Verification of the legitimacy of ownership of property in order to avoid purchasing goods from illegitimate sources, is important. In one case purchasers of second-hand motor vehicles accepted the explanations given to them by the dealers to justify why locks were damaged and number plates were removed from the vehicles in question. In another case, an offender pretended to own a motor vehicle which he then sold to a third party. In fact, the vehicle remained under the ownership of a finance company, pursuant to an unfinished hire-purchase agreement. In both cases the victimised purchaser acquired no title to the vehicle and lost the purchase price.

- **Failure to verify credit worthiness**

There were a number of incidents in which financial institutions lent money to applicants on the basis of inflated property prices, bogus employment status or non-existing assets without verifying the information described in loan applications. False claims were supported by forged documents such as payslips, letters of employment and ATO group certificates. Viability and credit worthiness of companies were commonly used to induce finance companies to advance funding beyond the finance companies' usual prudential controls.

Fictitious or altered documents in relation to purchase orders, invoicing, management

accounting records, minutes of a Board meeting and a sale and purchase agreement were provided to support the claims. These types of offences were commonly detected when the offender was unable to make payments to creditors.
On one occasion, a director of the company in question, adjusted original bills of lading, and created bogus invoices and correspondence by cutting, pasting, and photocopying, as well as using templates for invoices and purchase orders on a personal computer.

- **Failure to verify insurance claims**

Fraudulent insurance claims may be entirely fictitious in cases in which losses have never occurred or in which the extent of loss has been exaggerated. On occasions, insiders may collaborate with offenders to defraud insurance companies. In one instance, an employee of an insurance company created fictitious policies using false names and addresses. Immediately after the policies had been created, fictitious claims were logged involving a fictitious third party. The false claims were supported with a range of forged documents. Inadequate background checks of the applicant for insurance, failure to verify the authenticity of documents, and lack of supervision enabled the offences to take place. Internal company audit procedures eventually revealed anomalies, which led to the discovery of the false transactions.

Personnel Failures

- **Inadequate staff employment screening**

Stringent checking of references and the background of applicants for employment is a key means of minimising internal fraud risk. However, it is not always easy to identify dishonest events in a potential employee's past. When employees, in particular in positions of responsibility, commit dishonest acts within an organisation, the victimised organisation may be reluctant to report the matter to the police. This may be because the victimised organisation wishes to avoid adverse publicity that could affect its commercial reputation in the market place (Smith 1999a). Consequently, the organisation may allow perpetrators to resign without formal action being taken. Failure to take official action and fear of adverse publicity make it difficult for other organisations to discover the perpetrator's prior misconduct. The AIC/PwC study found that 17% of accused persons had committed prior fraud offences (2003 p. 41).

- **Inadequate supervision of staff**

While senior managers are identified as having major responsibility for preventing and detecting internal fraud and setting up ethical standards in organisations (KPMG 2002), they pose a greater fraud risk to an organisation than non-managerial employees (KPMG 2002; Ernst & Young 2002; the Association of Certified Fraud Examiners 2002). Long-serving senior employees tend to be under-monitored. In the case of *Power* v R, a bank employee in a middle-management position had been an employee of the bank for 26 years. As a trusted employee, her activities were not under regular scrutiny. This enabled her to defraud her employer of $3.88 million over a period of four years by entering false information into her computer (*Heather Kathleen Power* v *Regina*, NSWCCA 244, 19 June 2002). Inadequate supervision of non-managerial staff members can be caused by reduced staffing levels, supervisors being on leave or excessive workloads held by supervisors. Supervision is important both during regular working hours, as well as after-hours. There were a few instances in which perpetrators committed fraud while working outside normal working hours. In addition, good human resource management and a high level of job satisfaction is essential to reduce fraud perpetrated by employees (Grabosky & Duffield 2001).

- **Failure to segregate staff duties**

Having separate control systems in place such as for purchasing and payment has been found to be effective for fraud prevention, in particular, against organisational insiders (Smith 1998). However there were cases in which internal perpetrators were responsible for multiple duties. In one case a systems manager was responsible for creating financial systems and had access to computers used to process cheques and to receive payments. In another case, a sales manager had duties of receiving orders from customers, placing the orders into the computer system, and issuing credit notes. This enabled payments to be made without authorisation from others. In the second case, a new person in the firm noticed discrepancies relating to orders and payments leading to an audit being carried out and the fraud discovered.
Lack of segregation of duties in another case led an offender to fraudulently withdraw $25,000 a year on average from a company account without being detected for eight years. This employee was responsible for maintaining the business accounts journal, paying outstanding creditors as well as being a signatory on the business's cheque books.

Accounting/Auditing Failures

- **Internal auditing failures**

Inadequate internal audit procedures can enable employees, especially those with accounting duties, to manipulate accounting records so as to embezzle money within organisations. Lack of accountability in a company's bookkeeping records or failure to ensure a proper and regular reconciliation of accounts, can provide opportunities for motivated individuals to create false transactions.
In one case a potential buyer of a business requested detailed financial records, leading to the discovery of accounting anomalies which, following an internal investigation, resulted in fraud being uncovered. In one case the same employee who had been defrauding the company was responsible for preparing financial reports to the parent company. This made it possible to disguise the reason behind the company's loss of profit.

- **External auditing failures**

Inadequacy and ineffectiveness of external auditing procedures cause significant delays in detection of professional misconduct. Professionals are well-placed to conceal trust and investment account deficiencies resulting from fraudulent activities, and in the absence of effective auditing can continue to perpetrate fraud for lengthy periods of time.

In some cases, the misappropriation of trust and investment funds by solicitors and financial advisors will only be detected when clients seek repayment of capital, as interest payments can sometimes be made illegally from other clients' accounts. Without effective external auditing of trust accounts by professional regulatory bodies, such Ponzi schemes[3], as they are known, can continue for many years. There was only one instance in which offending was discovered during routine audits of trust accounts by a Law Society. Earlier detection of offending would have been possible, if more rigorous and regular auditing had taken place.

Security Failures

- **Inadequate computer access controls**

Organisations are susceptible to employee fraud when effective computer access controls are not in place. Logon name and password combinations are the usual means by which logical access to electronic accounting and finance systems is obtained. However, a number of incidents demonstrated that password protection controls were not adequate to prevent unauthorised access to systems. In one case a bank employee logged onto a fellow staff member's computer work station and entered false income and asset figures in order to facilitate the approval of bogus loan applications he had created. In another case, an accounting clerk obtained the chief accounting officer's password which provided access to an electronic payment system that was used for processing and approving false allowance payments. Adequate computer access controls and segregation of duties are closely related (KPMG 2001).

Between October 1998 and February 2000, a customer service officer stole $186,812 from a bank in New South Wales that employed her. She manipulated a number of term deposit account records electronically. Her individual employee number was used to gain access to the details of the customers' accounts and deposits. Firstly, she used her access to the bank's computer system to create withdrawals on term deposit accounts of several customers and applied the moneys withdrawn to her own use. Secondly, she entered false information or altered data stored in the computer to make it appear as if all moneys were still present in these accounts. Thirdly, she issued a new, false term deposit certificate to disguise her wrongdoing from the customers. She then either withdrew false deposits or reversed them to make the account balance at the end of the day. She was sentenced to four years imprisonment with a non-parole period of two years (*R* v *English-Russell*, NSWCCA 179, 10 May 2002).

Organisations are also vulnerable to attack from internal sources, particularly when new accounting or banking software systems are being installed. At this point, security control measures tend to be weak. In one case, deficiencies in accounting records were overlooked as it was thought that the problems were caused by errors arising out of some malfunction of the new system.

- **Inadequate card security controls**

The introduction of plastic cards has created many new risks of fraud. Lost and stolen cards and lost and misused PINs are commonly used to deceive financial institutions or merchants (Chapman & Smith 2001). In one case an offender fabricated merchant credit card vouchers using details from a stolen credit card and then banked the vouchers and eventually drew and cashed cheques.

Personal and account information contained in the magnetic strip on the back of the credit card is also not free from attack by fraudsters. The information can be skimmed and used for the creation of counterfeit cards. A range of security features such as security printing, micro-printing and holograms are adopted by financial institutions to prevent counterfeiting, although organised crime groups are adept at overcoming these security features.

- **Failure to secure personal identification documents**

Misuse of documents used to establish identity lay behind numerous cases examined in the AIC/PwC study (2003). In some cases over 100 false identities were created through the use of information derived from stolen documents or computerised databases.

Regulatory Failures

- **Professional regulatory failures**

It is often difficult to prevent and to discover dishonest acts of a professional, in particular, a sole practitioner, due to the absence of peer supervision (Williams 2002). In one instance a solicitor was under investigation by the Law Society in one state in relation to misappropriation of his clients' investment funds and had surrendered his practising certificate in that state. However, he moved to another state and recommenced practice as a solicitor without his activities in the first state being disclosed or investigated. He then committed further offences in the second state.

- **Corporate regulatory failures**

Lack of background checks on company directors can allow individuals to continue their fraudulent activities. In one case, a director of a superannuation company which had failed owing a large sum of money, was declared bankrupt and disqualified from holding further company directorships. His sons, who had no real business experience, became directors of two newly-established superannuation companies. The father (the banned director) resumed his work as a superannuation consultant for these two companies and, although not technically a

Table 1: Risk Factors and Fraud Prevention Measures

Risk Factors	Fraud Prevention Measures
Prudential Failures	
• Poor investment controls	• Investigate the credibility of scheme providers and investment schemes
	• Obtain adequate security for monies advanced
	• Improve consumer awareness
• Poor cheque control procedures	• Ensure compliance with clearance times
	• Have payment authorisation systems in place between businesses and banks
	• Use of formal cheque requisition forms
	• Strict verification of information written on cheques
	• Careful selection of signatories
• Failure to verify identification evidence	• Education and training of employees
	• Validate ID documents with issuing sources
• Failure to verify ownership of property	• Validate legitimacy of ownership of the property before purchasing
	• Check financing databases
• Failure to verify credit-worthiness of applicants for credit	• Validate information concerning applicants financial capabilities
• Failure to verify insurance claims	• Validate personal information provided by policy applicants (e.g. name, address)
	• Validate authenticity of documents with issuing sources (e.g. a quote from car repairer)
Personnel Failures	
• Inadequate staff employment screening	• Have detailed job application forms
	• Stringent checking of references and backgrounds of applicants
	• Train managers to improve interview skills to identify potential fraudsters
	• Regular fraud awareness staff training
• Inadequate supervision of staff	• On-going monitoring of integrity of employees
	• Awareness of behavioural and social anomalies (e.g. gambling problems, unusual work patterns, living beyond one's means)
	• Awareness of staff not taking leave or working after-hours
	• Mandatory staff recreational leave
	• In-house fraud hotlines
	• Implement corporate code of conduct/ ethics
• Failure to segregate staff duties	• Job rotation
	• Clear segregation of duties, in particular, purchasing, payments and authorisation of payments
	• On-going monitoring of long-serving employees and managerial staff
Accounting/Auditing Failures	
• Internal auditing failures	• Increase the role of audit committees
	• Increase budget allocation for internal audit
	• Provide fraud detection training for audit committees
	• Conduct random audits
• External auditing failures	• Conduct random audits
	• Employ active reporting
Security Failures	
• Inadequate computer access controls	• Enhance access security controls through systems(e.g. regular change of passwords, single use passwords)
	• Appropriate education of users of passwords
• Inadequate card security controls	• Improve security features of cards
• Failure to secure personal identification	• Carefully deposit and destroy expired ID documents
	• Store current ID documents in a secure place
Regulatory Failures	
• Professional regulatory failures	• Update and continuously review professional codes of ethics
	• Increase communication between regulatory bodies
	• Set objective standards and regular monitoring of non-statutory professionals
	• List the names of disqualified professionals and share data between agencies

director, was clearly in control of the business. As a result, cheques paid by clients of the two companies were deposited into a general bank account, instead of being paid into a special account on their behalf, and were disbursed in various unauthorised ways. Given that the father was no longer a director, he denied his involvement in the administrative affairs of the company, and hence in any of the dishonest acts. However, the Court convicted him as the principal offender with one of his sons as an accomplice (*R* v *Child*, NSWCCA 407, 8 December 1999).

- **Non-compliance with legislative requirements**

Failure to comply with the Corporations Law can also create opportunities for dishonesty. The case of Alan Bond illustrates how non-compliance with regulatory legislation can result in substantial financial loss, in this case over one billion dollars.

Minimising Risk of Serious Fraud

In June 2003, Standards Australia International Limited published a new standard, AS 8001 *Fraud and Corruption Control*, which provides useful guidance to both private and public sector organisations on the implemention of fraud and corruption control programs. The new standard focuses on three elements:

1. Structural elements;
2. Operational elements; and
3. Maintenance elements.

These standards specifically deal with some of the key risk areas identified in the AIC/PwC study (2003) that concern action, or lack of it, by management within organisations that creates an environment in which fraud can take place.

Conclusions

Given that the average length of offending identified in the AIC/PwC study (2003) was two years, fraud control policies are of critical importance in order to ensure speedy detection. This study demonstrates that organisations need to employ effective means of detecting anomalies, especially in dealing with identity-related fraud and computer fraud. Adequate on-going personnel monitoring and supervision and ensuring that a high ethical culture exists within an organisation are also key ways in which fraud risk may be reduced. Internal controls need to be coupled with effective education of staff to improve fraud awareness and to understand that dishonesty within the workplace is unacceptable. Finally, ongoing re-assessment of risks is necessary in order to design appropriate countermeasures suitable for our fast-changing society.

Acknowledgments

The AIC/PwC study of Serious Fraud in Australia and New Zealand was a jointly-funded project undertaken with the cooperation of police and prosecution agencies throughout Australia and the Serious Fraud Office in New Zealand.

References

Association of Certified Fraud Examiners 2002 *Report to the Nation: Occupational Fraud and Abuse*, Association of Certified Fraud Examiners, Austin. <http://www.cfenet.com/pdfs/2002RttN.pdf>.

Auditor-General 2003 *Management of Fraud and Corruption Prevention in the ACT Public Sector*, Auditor-General, Australian Capital Territory, Canberra.

Australian Institute of Criminology and PricewaterhouseCoopers 2003 *Serious Fraud in Australia and New Zealand*, Research and Public Policy Series, No. 48, Australian Institute of Criminology, Canberra.

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

Drugs and Crime Prevention Committee 2002 *Inquiry into Fraud and Electronic Commerce: Emerging Trends and Best Practice Responses—Discussion paper*, DCPC, Parliament of Victoria, Melbourne.

Ernst & Young 2002 *Fraud: The Unmanaged Risk: 8th Global Survey*, Ernst & Young Global Investigations & Dispute Advisory Services, <http://newsweaver.ie/ernst/global_fraud_survey.pdf>.

Grabosky, P. and Duffield, G. 2001, "Red Flags of Fraud", *Trends and Issues in Crime and Criminal Justice*, No. 200, Australian Institute of Criminology, Canberra.

KPMG 2001, *Global efraud Survey*, KPMG Forensic and Litigation Services.

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

Krambia-Kapardis, M. 2001 *Enhancing the Auditor's Fraud Detection Ability: An Interdisciplinary Approach*, Peter Lang, Frankfurt am Main.

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

Smith, R. G. 1999a "Identity-related Economic Crime: Risks and Countermeasures", *Trends and Issues in Crime and Criminal Justice*, No. 129 Australian Institute of Criminology, Canberra.

Smith, R. G. 1999b "Organisations as Victims of Fraud, and How they Deal with It", *Trends and Issues in Crime and Criminal Justice*, No. 127 Australian Institute of Criminology, Canberra.

Smith, R. G. 2002 *Crime in the Professions*, Ashgate, Aldershot.

Standards Australia International Ltd (2003) AS 8001-2003: *Corporate Governance-Fraud and Corruption Control*, 23 June 2003.

Standards Australia International Ltd. Website, 'New Standard seeks to put an end to corporate corruption' <http://www.standards.com.au/NEWSROOM/NEWS%20RELEASE/2003-07-03A/2003-07-03A.HTM>.

Williams, A. 2002 "Crime and Misconduct in the Accounting Profession" in *Crime in the Professions* (ed.) Smith, R. G, Ashgate, Aldershot, pp. 55-66.

Notes

1 Seriousness was defined on the basis of financial loss (generally over $100,000 per file), sophistication in the planning and/or execution of the offence; the degree of organisation of the offenders, or whether offences were committed by professionals (see AIC/PwC (2003) for further information).

2 A file was defined as the documents relating to legal proceedings that involved charges against one or more accused persons that were heard by one judge in a single sentencing hearing.

3 A Ponzi scheme refers to a certain type of fraudulent investment practice in which early investors are paid dividends out of the investments of subsequent investors.

Dr Russell G. Smith is Deputy Director of Research and Dr Yuka Sakurai is a Research Analyst with the Australian Institute of Criminology.

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Toni Makkai, Acting Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.

Project No 0037 Ethics No P020