AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 189

Controlling Financial Services Fraud

Aub Chapman and Russell G. Smith

In its broadest terms, fraud means obtaining something of value by deception. If fraud were described as an industry, it would clearly be one of the growth areas in the economy. It is also one of the least understood areas of the economy and, because fraud is often viewed as a victimless crime (when perpetrated against large organisations), it does not draw community reaction like other crimes. Similarly, fraud rarely attracts a coordinated political focus on measures designed to address the very serious losses that may result. One hardened criminal who served several periods of imprisonment for armed robbery offences was recently reported to have expressed an opinion to senior police that he wished he had understood earlier in his criminal career how easy it was to commit fraud. He now considers that fraud involves less trauma, the rewards are far greater, and the penalties substantially fewer than in other forms of crime. This paper addresses those forms of fraud that target the financial services sector and how this industry has responded, with some measure of success, to controlling this ever-increasing problem.

Adam Graycar
Director

The financial services sector is one of the fastest changing areas in the business community. The combination of industry deregulation and the exploitation of new and emerging technologies has resulted in financial institutions having the ability to deliver a vast array of products and services with an increasing number of delivery channels. The benefits and flexibility now being provided to customers have, unfortunately, also been exploited by those seeking to gain an advantage through dishonest behaviour. New opportunities for fraud are emerging almost daily.

In the financial services sector, the competitive demand for "fast to market" product development has introduced a major challenge in creating cost-effective and efficient controls which do not impede the need for flexibility in product features and delivery mechanisms. This challenge will continue to increase with the introduction of new and emerging technologies.

The decision to engage in any business activity is invariably based on a cost–benefit analysis which aligns the relevant enterprise's business objectives with its appetite for risk. The business of controlling fraud risk is no different from other business risks in that the assessment will be based upon various known factors as well as a number of unknown elements. In order to manage fraud risk effectively, however, we must be able to track it and understand it.

February 2001

ISSN 0817-8542
ISBN 0 642 24210 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

Unfortunately, the quantification and analysis of fraud is somewhat elusive. In 1997 it was estimated that the cost of fraud and misappropriation in Australia was between A$3 billion and A$3.5 billion per annum, which represented approximately one-third (29–30%) of the cost of all crime categories (Walker 1997). Different industry sectors and institutions within sectors have, however, traditionally categorised financial losses under a number of headings to suit internal management reporting, and this has hindered the establishment of aggregated figures which would assist in identifying the magnitude and types of fraud losses that have occurred. Changes in business practices have occurred without consideration of loss categorisation. This, too, has also impeded the identification of losses incurred as a result of fraud. For example, within the financial services sector, it is only in the last two to three years that institutions have come to recognise the need to examine loan write-offs more thoroughly in order to identify those which clearly are fraud-based losses as opposed to genuine lending losses.

As a result, institutions are often unable to say with certainty the extent to which they have been victimised through fraud or exactly what losses have been sustained. Nonetheless, fraud victimisation surveys have found that those in the financial services sector continue to experience fraud at rates generally greater than other business sectors. In 1999, 59 per cent of the 37 respondents from the financial services sector to an Australian fraud survey conducted by KPMG reported experiencing fraud in the preceding two-year period (KPMG 1999, p. 8). Of the Australian respondents to an Ernst and Young fraud victimisation survey who had suffered more than 50 fraud incidents in the preceding 12-month period, four were from the banking and financial services sector. Twenty-seven per cent of Australian bankers surveyed suffered more than 50 frauds compared with 14 per cent of bankers from all countries surveyed internationally (Ernst and Young 2000, p. 2). Of the 43 international respondents to Ernst and Young's fraud victimisation survey who suffered more than 50 fraud incidents of any size in the preceding year, almost half were from the banking and financial services sector, with three of these frauds involving more than US$25 million each (Ernst and Young 2000, p. 6).

Even if it is acknowledged that not all incidents of fraud are reported, the information currently available indicates that financial institutions are frequently targeted by fraudsters who often inflict considerable financial harm.

Types of Financial Services Fraud

Transaction Fraud

While it is necessary to try to predict the fraud risks associated with the future direction of business practices, it is also important to recognise that the more traditional financial services products remain a major area of vulnerability to fraud. In the United States, for example, cheque fraud has been reported to be increasing at the rate of 17 per cent per annum (Bank Administration Institute 1999) while in Australia, research undertaken by the first-named author revealed a substantial growth in losses due to paper-based fraud between 1998 and 1999. Negotiation of valueless cheques, stolen cheques, forged cheques, altered cheques and counterfeit cheques remain fertile ground for those seeking to commit fraud. In a number of instances these activities are well organised and involve a number of parties. Theft of cheques from the postal system, and the use of scanners, colour photocopiers and chemicals to alter existing documents or even to create entirely false documents, demonstrate a growing trend away from single opportunists to more deliberate, widespread attacks on the financial services industry.

The introduction of credit and debit cards which can be used in an ever-increasing marketplace has facilitated new forms of fraud. Lost and stolen cards, lost or misused personal identification numbers and the practices of corrupt card merchants have all provided fraudsters with new channels through which to conduct attacks on financial institutions. Turnover in the workforce of financial institutions, coupled with the growing amounts of information available on the Internet, have added greatly to community knowledge of financial systems and the inherent weaknesses in some products and services. For example, individuals have defrauded financial institutions by exploiting automatic teller machines which operate "off-host" (unconnected in real time to financial institutions' computer networks—see, for example, *Kennison v. Daire* (1986) 160 CLR 537; *R v. Evenett* [1987] 2 Qd R 753, and *R v. Baxter* [1988] 1 Qd R 537). Thus, the provision of a service that enabled customers to withdraw cash at any time of the day or night led to a new fraud risk being created. Similarly, technology designed for use within the industry has become available to the public and has resulted in the "skimming" of account and personal information contained in the magnetic strip on the back of the credit card, thus facilitating the creation of duplicate or counterfeit cards.

Facsimile machines and personal computers are also being used dishonestly by clients to transmit fraudulent instructions to financial institutions. High quality and

relatively cheap desktop publishing facilities are widely available through the use of personal computers, scanners and laser printers which enable near-perfect copies of legitimate business documents to be produced. Many of these contain signatures of company officials which have been scanned from annual reports or other official papers. The resulting documents, once transmitted to a financial institution electronically, may result in funds being remitted, usually offshore, via some irrevocable channel such as the SWIFT system of electronic funds transfer, making recovery difficult. In recent years a number of cases involving organised groups using this simple technique have resulted in substantial losses being incurred by financial institutions.

The imperative to compete in a rapidly changing market has, accordingly, placed considerable strains on financial institutions to limit time-consuming validation and verification checks. Electronic commerce, for example, demands that transactions be executed instantaneously and that payment be provided immediately. This pressure has presented new opportunities for those seeking to benefit through fraud at the transactional level.

Identity-Related Fraud

Over recent years the problem of identity-related fraud has grown, again facilitated by the use of computing technologies (see Smith 1999). Mobility within the community means that business no longer relies on local knowledge of an individual's background and circumstances when entering into commercial relations. A customer or business relationship is now usually commenced by the prospective customer presenting documents by which his or her identity can be verified. Through the theft and alteration of documents it is possible for one person to assume the identity of another and, where reasonable similarity is present (for example, same gender, similar age and so on), it is not difficult to undertake business dealings in the other person's name. Alternatively, fraudsters sometimes create completely fictitious identities supported by entirely fabricated false documents. Credit facilities can then be provided or other benefits obtained and the individual unable to be located following default under contractual arrangements.

The use of good quality, cheap technology facilitates the creation of documents which may be used to misrepresent the details of a legitimate person. When these techniques are used to create a new document, or to falsify an original document, it becomes somewhat easy for a person to use that document to procure other documents and thereby create a new, illegitimate identity.

An example of this kind of crime occurred in Victoria between August 1995 and March 1996. In the case of *R v. Zehir* (Court of Appeal, Supreme Court of Victoria, 1 December 1998), the offender used desktop publishing equipment to create 41 birth certificates, 41 student identification cards (some containing photographs, each in separate names) and a counterfeit driver's licence. These were used to open 42 separate bank accounts throughout the Melbourne metropolitan region, to pay cheques into accounts as wages and make immediate withdrawals before they had cleared, to register a business name, to obtain sales tax refunds and to defraud various retailers. The offender was convicted of a variety of offences and sentenced to five years' imprisonment with a non-parole period of three years. He was also ordered to pay compensation of A$41,300 and reparation to the Commonwealth of Australia in the sum of A$458,383.

Under British and Australian law, the use of a false or alternate identity is not necessarily illegal. The use of an alias is common in entertainment and literary circles. Many women choose to use both their maiden and married names. There are, however, various laws that create offences of using documents with intent to defraud. In addition, in an attempt to prevent large-scale money laundering, the *Financial Transaction Reports Act 1988* (Cwlth) introduced a requirement for cash dealers (which includes many of the major financial institutions) to identify all signatories to accounts and made it an offence to open or to operate an account in a false name. To support this regime, a process was established whereby numeric values were assigned to a defined group of documents—although none of them are officially considered to be forms of identification in their own right. The 100-point system, as it is known, provides for cash dealers to accept a combination of these documents as evidence of a person's identity unless there are obvious discrepancies. The use of modern technology to falsify documents, which to the average person appear to be genuine, has exposed a major flaw in the underlying veracity of the documents acceptable under the 100-point scheme. There has been a disturbing increase in identity-related fraud in recent years and financial institutions are now seeking to quantify losses from this particular type of fraud more accurately.

The future poses even greater risks of loss through fraud. The explosion in remote delivery channels, such as telephone banking and online banking, means that face-to-face contact between financial institutions and their customers is becoming less frequent, and in some cases may never occur. The use of intermediaries such as financial brokers, loan introducers, third-party agents and outsourcing initiatives present new challenges in controlling fraud. Similarly, the impact of the Internet on the conduct of commerce involving

financial transactions is not well understood. Questions surrounding sovereign and judicial borders, powers to undertake transborder investigations, and the ability to successfully mount prosecutions for fraud have yet to be answered.

The Response of the Financial Services Sector

Institutions within the financial services sector have taken action in a variety of ways to contain fraud losses. Measures taken to date have occurred both within individual financial institutions as well as within the wider industry itself. In addition, a number of cooperative initiatives have been undertaken between the financial services sector, law enforcement agencies and government.

Controls within the Targeted Financial Institution

Within the individual financial institution there needs to be a framework or policy which defines fraud control functions and risks in a comprehensive way. Such a policy should be aligned with the institution's appetite for risk. Because of the diverse nature of the larger financial services groups, the policy will not necessarily be consistent across all products, services, systems or delivery channels. It should, however, include the following three elements:

- prevention and detection;
- investigation; and
- case management and recovery.

Information derived from these elements and activities should be incorporated into any new products and services.

Preventive functions should include fraud training and awareness programs, fraud risk assessment on all new products and processes, automated fraud detection systems, and a policy which requires fraud prevention controls to be embedded in all products and systems.

Unfortunately, traditional methods have tended to be reactive in that they rely on manual and inefficient controls in order to identify fraud. Within Westpac, for example, it has been recognised that such an approach is no longer viable nor supportive of the group's business drivers. Westpac's fraud prevention and detection tool kit is now heavily weighted in favour of embedded controls supported by an increasing array of automated analysis tools which identify and report fraud attempts in a timely manner. A mix of inhouse-developed programs and vendor-supplied packages are used which interrogate transactions in either an online / real time mode, or by overnight batch processing. This depends upon the risk profile of the product or process in question.

Such measures have been highly successful in identifying fraud and have resulted in a widening of the gap between, on the one hand, fraud identified and fraud prevented and, on the other, actual fraud losses experienced. This gap is being influenced by both an increase in the proportion of fraud detected and prevented and by a reduction in actual fraud losses sustained.

The challenge for the future lies in enabling the industry to respond to customer demand for more sophistication and flexibility in products and services while minimising the opportunities for fraud. Just as credit processes within financial institutions were advanced through the introduction of automated credit scoring, so too will fraud controls benefit from software which identifies transactions with a high probability of fraud.

To manage the investigations workload, many financial institutions are making use of computerised case management tools which enable the progress of investigations to be monitored and for common features and trends to be identified.

Funding for fraud control initiatives, however, continues to compete with other business initiatives and is not always easy to justify on a cost–benefit basis. Within Westpac, for example, fraud control management information reporting has been revised in such a way that actual losses are no longer simply reported but, rather, the level of fraud identified and prevented is also able to be identified. This approach has enabled the benefits of various skilled resources and automated tools to be quantified more precisely.

Industry Interaction

There have been a number of attempts to achieve uniformity in the categorisation of fraud within the financial services sector. Over recent years the Australian Bankers' Association Fraud Working Group has been successful in addressing a number of issues common to all members. However, attempts at sharing actual fraud data have proven very difficult, with various obstacles being raised. Confidentiality of corporate data and privacy of customer information have often been proffered as reasons for declining to submit information which could be aggregated at industry level. These barriers have broken down over the past two to three years and there is now a commonly held view that fraud is not a competitive issue and that industry-wide initiatives are required to support the internal controls and processes employed within individual institutions.

One of the most urgent needs is the creation of a national fraud database into which financial institutions can input existing fraud data and against which new data can be tested to identify fraud attempts. This could be achieved through matching new data with data known to be fraudulent or by analysing transaction elements that suggest a high probability of fraud. Outputs from such a database could place the inquiring

institution on notice that further investigation may be prudent before proceeding with the transaction. The Australian Bankers' Association has established a research project to assess the viability of a national fraud database. This has evaluated a number of commercial packages and also considered the proposed impact of the *Privacy Amendment (Private Sector) Bill 2000* (Cwlth) which seeks to extend the operation of the *Privacy Act 1988* (Cwlth) to the private sector.

Such an industry-wide database could also be used to support public sector law enforcement initiatives. Already, the Australian Bureau of Criminal Intelligence has established an electronic national fraud desk for use by federal, State and Territory police services as well as a number of government law enforcement agencies in Australia and New Zealand. Although the fraud desk is not available to the public generally, there would be substantial community benefits arising from some restricted form of data-sharing between this law enforcement data warehouse and any database created from within the industry.

Another industry-wide initiative has been the establishment of the Australian Credit Card Industry Fraud Forum. This group, created under the auspices of the Olympic Security Command Centre within the New South Wales Police Service, examined the potential fraud risks which might have emerged at the time of the Olympic Games in Sydney in September 2000. The group comprised banks, credit card scheme providers and law enforcement personnel, and developed and delivered fraud training materials to retailers, financial institutions and law enforcement agencies. Agreement was also reached on the monitoring and reporting of fraud during the period just prior to, during and immediately after the Games. An industry-wide fraud alert process was established as a means of mitigating any fraud scams which were identified. The benefits derived from the creation of this discussion forum now extend well beyond the period of the Games.

Other Cooperative Ventures

Fraud in the public sector remains a considerable problem in Australia. In a recent review of fraud control arrangements within Federal Government agencies alone, the Australian National Audit Office (ANAO) found that some 4,050 fraud cases worth approximately A$146 million were reported by 106 agencies in 1998–99 (ANAO 2000). In a separate inquiry into the administration of tax file numbers in Australia, the ANAO found 3.2 million more individual tax file number registrations than people in Australia counted at the last census, with an estimated 185,000 potential duplicate records of individual taxpayers present amongst 17.1 million active tax records (ANAO 1999, p. 21). This clearly creates a situation conducive to fraud against the government.

Benefits fraud remains a major concern to Centrelink, Australia's primary agency for income support, and many of the elements are common with the types of fraud being experienced by financial institutions. In New South Wales a pilot program between the Registry of Births, Deaths and Marriages and Westpac, and a concurrent pilot program between the Registry and the Roads and Traffic Authority, identified a number of false birth certificates that had been presented as part of the identification process. The New South Wales Attorney-General subsequently announced the formalisation of this verification process and it is now under active investigation for extension to other States and Territories. A national scheme linking State and Territory driver's licence databases is also under way.

As one outcome of the 2000 Australian Crime Commissioners' Conference, the Major Fraud Group of the Victoria Police has promoted a new strategy to deal with fraud that makes use of identification documents. The so-called "Challenge Response" project is an Australia-wide approach to identification issues which seeks to utilise a single independent conduit to coordinate data transfers between individual financial institutions and specific government authorities for verifying the authenticity of key documents presented for identification purposes when establishing accounts. Such a scheme would preserve customer privacy, reduce fraud and provide the relevant authorities with an ongoing quality assurance process regarding the level of fraudulent documents in the community. The scheme seeks to cover birth certificates, driver's licences and passports, and would have benefits in reducing both fraud against financial institutions arising out of abuse of the 100-point system, as well as fraud against public sector agencies perpetrated through the use of fraudulent tax file numbers and other official forms.

The need to prevent identity-related fraud against the government has also been identified in the report of the House of Representatives Standing Committee on Economics, Finance and Public Administration (2000). In its review of the ANAO's audit report on the management of tax file numbers, the Committee recommended that the Australian Taxation Office improve its internal processes for establishing identity and preventing identity fraud (p. 68) and that the government instigate a formal process for assessing proof of identity risks across the Commonwealth (p. 71).

Specifically, the Committee recommended that the government work with industry to develop options for reducing and preventing identity fraud, including the investigation and development of a national electronic gateway for document validation (p. 74). This idea would reinforce the Challenge Response initiative already being implemented in some States.

Conclusion

It can be seen that fraud directed at financial institutions continues to be a problem in Australia despite the introduction of a number of innovative policy and technological solutions by the financial services sector. Although financial institutions are seen as having relatively deep pockets with which to absorb fraud losses, these invariably increase the cost of services to consumers. Those who are responsible for creating or enhancing fraud risks, be they corporations or consumers, should bear some responsibility for the resulting losses. This market-driven approach has taken on importance in the United States recently with the introduction of a Uniform Commercial Code which encompasses the concepts of contributory negligence and comparative negligence in allocating commercial risks.

Governments, too, sustain considerable losses through fraud; often the same means are used to perpetrate offences as are used in the private sector. Manipulation and abuse of identification documents represents a continuing problem which affects financial institutions and government agencies alike. It is for this reason that the industry needs to work in partnership with governments to devise effective solutions that minimise risk while respecting individual privacy and confidentiality. Using technology to carry out verification of documents, such as the Challenge Response protocol, is likely to be a simple solution to an enduring problem.

References

Australian National Audit Office (ANAO) 1999, *Management of Tax File Numbers, Audit Report No 37, 1998–99,* Australian National Audit Office, Canberra.

Australian National Audit Office (ANAO) 2000, *Survey of Fraud Control Arrangements in APS Agencies, Audit Report No 47, 1999–2000,* Australian National Audit Office, Canberra.

Bank Administration Institute 1999, *Combating Check Fraud Conference*, 14–17 November, Scottsdale, Arizona.

Ernst and Young 2000, *Fraud: The Unmanaged Risk: An International Survey of the Effect of Fraud on Business*, Ernst and Young, London.

House of Representatives Standing Committee on Economics, Finance and Public Administration 2000, *Numbers on the Run: Review of the ANAO Audit Report No. 37, 1998–99 on the Management of Tax File Numbers*, Parliament of Australia, Canberra.

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

Smith, R.G. 1999, 'Identity-related economic crime: Risks and countermeasures', *Trends and Issues in Crime and Criminal Justice*, no. 129, Australian Institute of Criminology, Canberra.

Walker, J. 1997, *Estimates of the Costs of Crime in Australia: Revised 1997*, John Walker Consulting Services, Queanbeyan.

Mr Aub Chapman is Chief Manager, Operational Control, Westpac Banking Corporation.

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.