

FRAUD AND THE AUSTRALIAN BANKING INDUSTRY

Ian Woods
Australian Bankers' Association

*Paper presented at the conference Crime Against Business, convened by the
Australian Institute of Criminology, Melbourne, 18-19 June 1998*

FRAUD AND THE AUSTRALIAN BANKING INDUSTRY

In this paper reviews fraudulent activity from the perspective of the banking industry. looks at the types of fraud and the response measures taken by the banking industry to reduce fraudulent activity.

Fraudulent activities, especially the common garden variety, do not have the same aura as violent criminality. They have that air of invisibility and do not appear to provide the attention grabbing headlines needed to sell newspapers. Recent media attention to several expatriate fraudsters is the exception to the rule. On the other hand, violent criminals such as armed bank robber Brendan James Abbott, receive disproportionate media attention whilst fraudsters go about their 'activities' with little, if any, publicity. The community generally and the banking industry in particular suffer financial losses from fraud that far outstrip those resulting from armed attacks. Therefore, it is perhaps surprising that fraud and the damage that it causes does not receive greater media coverage. Let us now look at the size of the problem and ascertain what fraud is costing the community.

Fraud - the Size of the Problem

It is an understatement to say that it is difficult to estimate the cost of fraudulent activity to the community. Adam Graycar in introducing a paper by Russell G Smith titled *Measuring the Extent of Fraud in Australia*, has stated: "Analysts believe that fraud costs the nation considerably more than any other type of crime. It has serious consequences for all Australians, whether they be victims of fraud whose trust has been betrayed, or consumers who are required to shoulder the burden of business losses through increased costs and services. It is surprising, therefore, that so little is known about the nature and extent of fraud." Similar comments have been made elsewhere, refer *Australian Federal Police - Comfraud Bulletin October 1997* where the fraud estimation problem was described as ".....something akin to playing the children's birthday party game of pinning the tail on the donkey." Russell Smith confirms that the latest estimates place fraud and misappropriation offences in Australia in the range of AUD3 billion to AUD3.5 billion. This is approximately 30% of all crime recorded in Australia. He suggests and intuitively we must agree, that increased resourcing of policing services by governments will result in significant benefits for the whole community.

Large scale organisations, especially those specifically dealing in financial assets, are prone to be attacked by fraudsters. In Australia there are no reliable statistics on the size of fraudulent activity taken against financial institutions. By comparison, in the United Kingdom, the British Bankers' Association (BBA), collects data on certain types of fraud, specifically cheque and documentation related fraud. The BBA Fraud Prevention and Intelligence Unit's quarterly publication, *Crimewatcher* summarises this type of activity. In *Crimewatcher* issue No 18, it was revealed, for the nine months ended 30 September 1997, fraudulent activity against banks, resulted in potential losses of GBP252.8 million. These figures do not include credit card and non-cheque/documentary fraud. In the 25 April 1998 British supplement to *The Economist* it was stated that in 1997 plastic card fraud exceeded GBP 120 million. Similarly, in the United States, the American Bankers' Association in its *ABA Banking Journal* (August 1997) quoted a risk management employee of Wells Fargo Bank who had stated that US losses from cheque fraud alone were in the range of USD 10 billion to USD 50 billion. Steven Marlin suggests that credit card fraud in 1997 was in excess of USD 1 billion. The figures quoted above range from the relatively small to the astronomical. Whether or not we have confidence

in these figures is a matter for each person to evaluate. What we can be certain of is that the problem is significant. It requires the urgent attention of all members of the community. As you would be aware, the cost of fraud is not limited to the direct losses. In addition, there is the cost of preventing, investigating and prosecuting fraud cases and these costs are significant. There is also the trauma and stress suffered by the victims of these criminal acts.

In relation to the banking industry, there is a need for it to estimate and track the cost of fraud. There is also a need for greater sharing of information between financial institutions on fraud trends and practices. Many believe that the only way to reduce the intensity and frequency of the fraud problem is to substantially increase the exchange of information between parties on fraudsters and fraud typologies. This does not mean that we overlook the question of protecting customer confidentiality and the rights of the individual. What we should ensure is that criminals are not protected or assisted in carrying out their destructive actions. Later in this paper I will briefly look at what the banking industry is doing in response to these issues. Firstly we will look at the major types of fraudulent activity, taken against financial institutions and their customers.

Plastic Card and ATM Fraud

The age of high technology has partly done away with the risks of carrying cash and the need for cash. Nevertheless, this has resulted in new fraud risks being incurred. The majority of the cards that are used in fraudulent activities have been either lost or stolen. They have been thieved from homes, cars, offices, mail centres and so on. It is surprising how many people leave credit cards in motor vehicle gloveboxes or in the pockets of their unattended coats when dining in restaurants and at entertainment venues. Frequent customer carelessness is making it far too easy for criminals to steal cards. It is essential that customers protect their cards and Personal Identification Numbers (PIN) for what they are and that is valuable. Treat your card and PIN like cash. Another reason for card fraud is that many customers fail to comply with the card issuer's requirement that PIN details are kept in a safe place and are not to be carried with the credit card. If the PIN can be committed to memory then so much the better because the original PIN advice can then be destroyed. I reiterate, the card and PIN in combination are the customer's electronic signature. They must be protected.

It should also be mentioned that many merchants, whilst checking the customer's credit card details, fail to verify the signature of the customer. Many do not even verify that the person presenting the card is of the same sex as the person detailed on the card.

There has also been a growth in counterfeit cards and fraud intensity is likely to expand substantially during the Year 2000 Olympics. This is the fraud prevention personnel's Year 2000 problem! Counterfeit cards are frequently based on details sourced from a genuine card. The latter, as mentioned above, having frequently been either lost or stolen. The genuine card details may be encoded onto another card or several cards. An alternative method, where the genuine card does not permanently change hands is the use of the 'skimming' technique. Skimming is where criminals gain access to merchant locations or technology, and then copy the magnetic information contained on a customer's card which is later transferred onto a counterfeit card or cards. Another source of credit card details is via the Internet where hackers using software programs are able to obtain card information and through trial or error can identify card issuers who do not put in place validation protection on their magnetic strips.

Banks have taken various kinds of action to reduce the levels of card fraud. At the 'low tech' end of the spectrum they have provided customer education on how to protect themselves against fraudulent activity. Brochures have been issued, frequently distributed with the account statements and these outline steps that card users can take to safeguard their cards.

Some banks and card issuers also utilise computer software to control the possible damage when a card, without the knowledge of a customer, is lost or stolen. The system tracks card usage and if it detects an abrupt change in usage then it 'flags' this usage pattern change to bank staff. The card issuer or bank staff are then aware that there could be a potential fraud problem requiring investigation.

With the introduction of the Bankcard in 1974, there was a mass mail-out of cards. This resulted in many cards getting into the wrong hands. Consequently, today banks require the customer to produce identification at a bank branch prior to picking up a card.

Another approach that assists the reduction of fraud levels results from the lowering of floor limits of retailers and also random checks of transactions falling below the floor limits. Card security can be further enhanced by the use of holograms, tamper proof signature panels, improved validation encryption on the magnetic strip and micro printing.

The banking industry is preparing itself for an onslaught of local and international fraudsters during the Year 2000 Olympics in Sydney. At that time there will be a multitude of different credit cards, currencies, and other documents circulating. Thus everyone, particularly financial institutions and retailers, will need to plan now so that they are on their guard to fight fraudulent activity being carried out by criminals.

Card customers should action the following so that they can protect themselves:

- sign your cards as soon as they arrive.
- carry your cards separately from your wallet.
- keep a record of your account numbers, their expiration dates, and the phone number and address of each company in a secure place.
- keep an eye on your card during the transaction, and get it back as quickly as possible.
- void incorrect receipts.
- save receipts to compare with billing statements.
- open bills promptly and reconcile accounts monthly, just as you would your cheque account.
- report any questionable charges promptly and in writing to the card issuer.
- notify card companies in advance of a change in address.

Don't:

- lend your card(s) to anyone.
- leave cards or receipts lying around.
- sign a blank receipt. When you sign a receipt, draw a line through any blank spaces above the total.
- write your account number on a postcard or on the outside of an envelope.

- give out your account number over the phone unless you're making the call to a company you know is reputable. If you have questions about a company, check it out with your local consumer protection office.

By following this advice, cardholders will assist in the reduction in fraud and protect themselves.

Application Fraud

A significant number of losses suffered by the banking industry are the result of fraudulent applications for banking facilities including loan accounts. The customer identification requirements of the Cash Transaction Reports Act and its successor legislation being the Financial Transaction Reports Act, have in all probability significantly reduced the number of accounts in false names. Concurrently, they may have also reduced the number of frauds perpetrated against financial institutions. This legislation requires that cash dealers, such as banks, when opening accounts for new customers or in changing the signatories of existing accounts, to identify those customers. Each customer must be identified under a 100 point scoring process. This involves providing different weightings to various forms of identification. A driver's licence, for example, does not have the same value (viz number of points) as a passport. Notwithstanding these requirements, the process is not foolproof and is far from perfect. We are all aware that driver's licences and a whole range of identifying documents, including Australian and other passports, can be forged or counterfeited.

The ease with which fraudsters can register company and business names with ASC and business affairs offices is of concern. Financial institutions have experienced non-lending losses due to the fraudulent registration of company and business names.

The banking industry considers that the regulators should urgently revisit the issue of the registration of names and companies with names similar to existing corporates.

It is challenging for banks to face skilled counterfeiters of identification documents who may have substantial resources and who are intent on establishing an account using false identification. These criminals will attempt to circumvent any difficulties placed in their way. The banking industry considers that the increased sharing of information between parties on fraudsters at the time account applications are made, would have a significant impact on the level of fraud.

Cheque Fraud

Since they were first introduced, cheques have been the subject of fraudulent activity. In the 1980s and 1990s the problem has been further exacerbated by the swift development of relatively inexpensive computer and related technology. The age of desktop publishing, scanners, laser printers has assisted fraudsters who have used these technologies to carry out their criminal activities. It has been stated that more money today is stolen from banks with a laser printer than a gun. The American Bankers' Association (Lunt 1995) has also advised that the following aspects have contributed to the increase in cheque fraud:

- sophisticated, computer literate counterfeiters;
- laser printers that anyone can buy that are increasingly used to produce cheques legitimately and illegitimately, so it's hard to tell good from bad ;
- colour copiers the quality of which is so good that criminals in some cases simply copy cheques;

- businesses that willingly accept cheque fraud as a cost of business rather than trying to reduce the problem; and
- customers who do not report the loss or theft of their cheque/s straight away.

From the banks' viewpoint there are two main types of cheque fraud. The first is the situation where the customer is the victim. A criminal either steals or falsifies the customers' cheques. The second situation is where the customer and the criminal are one and the same. In this situation the criminal opens an account with the intention of crediting and then drawing against worthless cheques.

Banks are in a bit of a bind, they face the increasingly difficult task of separating good cheques from fraudulent cheques. On the one hand their role is to protect the assets of the customer and the bank. Conversely they need to provide fast high quality service to customers. The challenge is to find the correct balance between good customer service and risk assessment.

In many cases customers have no legal liability for cheque fraud actioned against them. Nevertheless, being a fraud victim can create many problems including inconvenience until the matter is sorted out for both the customer and bank.

What can cheque account customers do to protect themselves? Following are some suggestions:

- never give out your cheque account number to people who you do not know;
- report lost or stolen cheques immediately;
- protect your cheque book as if it was cash; and
- check your bank statement upon receipt and advise the bank of any irregularities.
- be as specific as possible when completing the payee details.

A cheque fraud trend that has rapidly grown in recent years is the counterfeiting of cheques. In the past, to produce a counterfeit document criminals would need to own or gain access to professional printing technology. In addition they would have to be either trained as printers or have printing industry contacts to carry out the document counterfeiting activities. Today, the personal computer, coupled with a good printer and software is a powerful publishing tool. It has the ability to create and store logos, design and print various typefaces. Linked with a scanner, documents can be copied, modified and reprinted. The production of professional looking documents is now in the hands of the amateur. When the amateur is also a criminal, then this creates problems for everyone.

The 27 November 1989 issue of Forbes ran a cover story showing how it was possible for a Forbes reporter to create a counterfeit cheque with technology. The article by David Churback, recounted how he obtained the appropriate equipment and detailed the process of counterfeiting a Forbes Inc cheque. It even documented how he sourced special paper for the cheque and the other techniques that enhanced the credibility of the document. Since the Forbes article was published the world has moved on. But one thing is certain, and that is, with changing techniques and procedures the fraudsters are never too far behind. What the rest of the community has to do is to ensure that they keep in front!

Fraud scams can be quite audacious, as they always have been. An example of this type of audacity is demonstrated in an article in the February 1995 issue of ABA Banking Journal titled What Truly Deters Check Fraud? Part of the article states: "In one type of scam, a group might pull up in a van in front of a bank or check-cashing place where people are cashing payroll checks. One team member will approach someone on line and offer \$50 for a two-minute look at their check. Inside the van, the criminals will scan the check and later duplicate it, altering the payee name and serial number." The scam is now only one step from completion.

What action banks can take to prevent cheque fraud:

- ensure that staff, particularly tellers, are trained to carefully vet cheques and identification documents for anything suspicious;
- open accounts with greater care - the introduction of the Austrac 100 points check may have assisted in the reduction of fraud but it has not eliminated it;
- educate customers, both business and personal, about how they can avoid cheque fraud being perpetrated on their accounts;
- encourage customers to utilise cheques with safety features such as watermarks, micro printing, holograms, void pentagrams and so on;
- banks to internally communicate fraud attacks to ensure that other internal business units are not subjected to attacks by the same fraudster; and
- encourage businesses to prevent cheque (and card) fraud so that more fraudsters are caught.

Other Types of Fraud

Another type of fraud that receives media comment now and then is the Nigerian letter and similar scams. These are often targeted against banks and others. Frequently the 'target' is asked to provide funds to cover 'legal fees' or other 'establishment fees' in order that the cache of account funds can be liberated and exported from the country. This scam involves bogus businessmen seeking assistance in transferring substantial sums out of specific countries. This is a clear example of local vulnerability to global fraudulent scams. Fraud can be 'marketed' globally! Those who want to read more on the current crop of financial scams are referred to Manfred Glinig's text 'International Financial Fraud' that was published in 1997 by the Austrian Bankers' Association.

Internal Fraud, this is a very sensitive subject for any organisation as there is frequently an aversion to bad publicity. Employee fraud in banks as in any organisation may follow various approaches. With lower level employees it will generally involve smaller amounts, eg manipulation or theft of petty cash. At the higher employee level it may involve much larger amounts. Types of defalcation fraud include diversion of funds or account manipulation, bogus loans, tellers' cash shortages, theft of travellers cheques and other valuables, theft of utility payments, and kickbacks. Understandably, banks have a policy of zero tolerance with respect to employee fraud and will ensure that offenders are sacked, prosecuted and funds restituted.

Industry Responses to Fraud

I have already mentioned industry responses to card and cheque fraud. Possible responses to the problem of fraud generally against financial institutions may include:

- biometrics - the use of unique physiological or behavioral identifiers. These approaches may include facial recognition, fingerprints, finger minutae expressed as algorithms, hand geometry, retina scans, iris scans, quasi behavioral approaches such as how one speaks or writes and dynamic signature recognition. Biometric units cannot be lost or stolen. This makes them an obvious antidote to identity theft. However, in its early days application is not widespread, nor always sufficiently reliable.
- fraud detection software (including 'cheque kiting detection' programs) to recognise activity patterns on customer accounts and to highlight significant variances;

It is generally agreed that the increased sharing of information on fraudsters and fraud typologies will assist in the reduction of fraud.

Adequacy of the Criminal Law

Anecdotal information from the security and fraud specialist sections of banks suggests that the offence provisions are generally appropriate. However, the level of sentencing is frequently inadequate, this is particularly so in relation to the so called 'white collar' crimes and also armed attacks against banks. There is a need for government to ensure that law enforcement bodies are adequately and appropriately funded so that they can effectively fight crime.

It has been suggested in the media that banks frustrate law enforcers in carrying out their duties. Bankers have a duty to keep their customers' financial affairs confidential. However, like all citizens, banks have an overriding duty and that is to obey the law. Banks assist law enforcement bodies, only if this accords with the law. Further, it is essential that law enforcement bodies understand the bank's position when carrying out their roles. Law enforcement bodies may need to continue their lobbying of Government to ensure that adequate and appropriate legislative directives are in place to assist them obtaining information whilst pursuing prosecutions.

As you would be aware, the Australian Law Reform Commission is presently reviewing the Proceeds of Crime Act and related legislation including the Financial Transaction Reports Act. The Commission is to provide a final report to the Attorney-General by December 1998. One of the matters that the Commission is to consider is the need for expansion of police powers to obtain information from financial institutions for the purpose of locating proceeds resulting from criminal activities. This provides law enforcers with a timely opportunity to raise the issue of access to information and records.

There is a need for greater interaction between the representatives of the banking industry and law enforcement bodies. It is hopeful that the industry will be able to formally meet with the Police representatives immediately following the Heads of Fraud meeting to be held in Sydney in August. Members of the Australian Bankers' Association consider that this first step will lead to stronger relations between all parties.

Increased communication can only enhance the relationship between all parties and to achieve the common goal and that is to decrease the level of fraud and ensure that fraudsters are appropriately prosecuted.

Industry Exchange of Fraudster Information

Member banks of the Australian Bankers' Association are presently considering the means to exchange information on fraudsters on an industry-wide basis to assist in the detection of fraud. Discussions are presently being held with a range of service providers for the latter to provide proposals to the industry for the development of a database. A similar system was introduced in the United Kingdom a few years ago and resulted in a significant reduction in fraud losses. The industry is mindful of the need for customer confidentiality and considers that a workable outcome will be achieved. Obviously the system will be designed to accord with the law. Such a database may also be expanded in time to record the number and monetary losses arising from fraudulent activities taken against financial institutions. This would highlight the areas of greatest risk to banks and indicate fraud trends.

Conclusion

To conclude, the present and previous Commonwealth Government's initiatives with their anti-crime legislation have given Australia a reputation for stringent anti-money laundering responses. There is now a need for Government to ensure that industry is not hamstrung in its light against fraudsters. The role for all of us is to provide a climate of 'certain risk of prosecution' for those persons that carry out fraudulent activities.

REFERENCES

- American Bankers' Association, 'Check Fraud Stakes Rise' *ABA Banking Journal*, August 1997.
- Australian Federal Police, October 1997, *Comfraud Bulletin*.
- British Bankers' Association, *BBA Crimewatcher*, Issue No 18, (BBA Fraud Prevention and Intelligence Unit).
- Cheetham, Naom, 30 May 1997, 'Signature Tune for Forgers', *The Weekend Australian*.
- Churbuck, David, 27 November 1989, This Check is a Fake: Computers are user-friendly for crooks too. Are bankers prepared? Apparently not, *Forbes*.
- Coleman, Peter, 23 March 1992, Towards an Industry Wide Response to Fraud, *Preventing, Detecting and Investigating Fraud in Banks and Financial Institutions*, a conference held in Sydney.
- Crothers, Richard, March 1998, 'Credit Card Fraud Increases as Organised Crime Races towards the 2000 Olympic Games', *Platypus - The Journal of the Australian Federal Police* No. 58.
- The Economist, 25 April 1998, 'Your Flexible Foe - Fraud Dilemma'.
- Glinig, Manfred, Austrian Bankers' Association Vienna, *International Financial Fraud Bogus Banking: Organised Fraudsters Inflict Billion Dollar Losses*.
- Lunt, Penny, February 1995, 'What Truly Deters Check Fraud', *ABA Banking Journal*.
- Marlin, Steven, May 1997, 'How Safe is Cyber-banking?', *Bank Systems & Technology*,
- O'Sullivan, Orla, June 1997, 'Biometrics - Comes to Life', *ABA Banking Journal*.
- Smith, Russell G, July 1997, *Crime and Criminal Justice*, No 71, Plastic Card Fraud Australian Institute of Criminology - Trends and Issues.
- Smith, Russell G, November 1997, *Crime and Criminal Justice*, No 74, Measuring the Extent of Fraud in Australia, Australian Institute of Criminology - Trends and Issues.
- Smith, Russell G, December 1997, 'Card Games: Plastic Fraud and Misuse', *Australian Accountant*.