PLASTIC CARD FRAUD

Russell G. Smith and Peter Grabosky
Australian Institute of Criminology

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

The plastic card industry is being targeted by organised criminal enterprises from around the world. In the past, Australia's physical isolation from the rest of the world protected us, to some extent, from fraud trends which were taking place elsewhere. Computers, telecommunications systems, and international travel, now allow Australia to experience the same kinds of fraud as occur in other developed countries. This paper considers one particular form of fraud which is endemic overseas, and which is likely to become a substantial problem for Australian law enforcement and regulatory agencies in the years to come - namely, plastic card fraud, or crimes of deception committed through the use of credit cards, debit cards, and stored value cards. It will also consider the opportunities for this kind of fraud which the Sydney Olympic Games will create, and how best to guard against such crime.

As we approach the year 2000, plastic card payment systems are being used much more extensively than in the past. One of the reasons for the development of these systems was the desire to reduce the security risks associated with having large amounts of cash held by banks, merchants and individuals. Unfortunately, as with other areas of regulation, a novel crime prevention strategy has created new risks which may have far worse consequences than the problem that was intended to be avoided.

Plastic card payment systems can be grouped into three categories: cards used to pay before, at the time of, and after conducting a transaction.

The first category relates to stored value cards which have value recorded on them electronically prior to customers using them to conduct transactions. Stored value cards may be "memory only", which are loaded with value and used to conduct specific transactions, such as making phone calls, and are then disposed of after use; or "smart cards" which have computer chips to store data and in some cases a microprocessor to process data. In Australia, there are between 1.5 and 2 million smart cards in use, while worldwide there are over 420 million in use. At the Atlanta Olympic Games, approximately two million Visa Cash Cards were distributed, and each of the various forms of plastic card are likely to be in wide circulation at the Sydney Olympics in 2000.

The second category relates to debit cards which permit transactions to be conducted and bank accounts debited immediately via online connections made between Automated Teller Machines (ATM) and Electronic Funds Transfer at Point of Sale (EFTPOS) terminals and banks. Since 1989, there has been a substantial increase in the number of EFTPOS terminals in Australia. At 30 June 1997, they numbered 169,739 and were used to conduct some 1,442 million transactions in the year ending March 1997. There were also 7,816 ATMs in operation in Australia. For the first time in Australia, the number of EFTPOS transactions has exceeded the number of ATM withdrawals (Australian Payments System Council 1997).

The final category relates to credit cards which are used to purchase goods and services on the understanding that payment will be made at some point in the future. In 1992, there were almost 10 million major credit cards in use in Australia, and approximately one-third of retail purchases in Australia are now made through credit cards (Australian Payments System Council 1995).

To what extent, then, are these payment systems abused?

PLASTIC CARD VULNERABILITIES

In one survey conducted in the United States in 1993, a group of 14 credit card fraudsters admitted to employing over 100 different ways of using credit cards to obtain funds dishonestly (Jackson 1994, p. 37). What follows is a brief survey of some of the more important vulnerabilities of plastic card payment systems.

Alteration and Counterfeiting

The first area of vulnerability lies within the card itself. Ever since plastic cards were introduced, attempts have been made to alter or counterfeit them in order to obtain funds illegally.

Cards used to perpetrate fraud are generally lost or stolen cards which could be used intact or altered by re-embossing and re-encoding, or counterfeit cards that are entirely new. In order to counterfeit a card it is necessary to know the details of a current valid cardholder -- hence the desire of offenders to obtain legitimate credit card details from sources such as the Internet (a method which is being used increasingly by offenders in Australia). Blank, white plastic cards are then embossed with stolen numbers, the magnetic stripe is encoded with matching numbers, and the signature panel on the card installed. Identifying logos and colour printing are added to mimic a real card.

Sometimes information on the card's magnetic strip is obtained is "card skimming". This is when a legitimate card is obtained for a few seconds to enable it to be passed over a magnetic tape reader so that a counterfeit copy may be made.

Another technique is "buffering", which involves modifying the information stored in the magnetic strip of the card or obtaining security codes electronically.

Although magnetic stripe cards are relatively easy to forge, smart cards are more difficult to counterfeit, but there are claims that they are not absolutely tamper-proof.

Asian Organised Counterfeiting

Offenders most involved in counterfeiting seem to belong to organised groups which emanate from the region bounded by Malaysia, Indonesia, Hong Kong and Thailand. A United States report on Asian organised crime noted Chinese criminal groups based in Hong Kong were responsible for 40 per cent of the world's counterfeit credit card losses, which are estimated to cost business between $A1 billion and $A2 billion per annum (United States Senate 1993, pp. 44-5).

In Canada, the Asian-based organised crime group known as the "Dai Huen Jai" , or Big Circle Boys, and is estimated to have a membership of 50,000, has been responsible for over 90 per cent of the plastic card fraud in Canada (Mativat & Tremblay 1997, p. 177).

An English study of 186 plastic card fraudsters found that 89 per cent were of ethnic Chinese origin (Newton 1995, p.5).

There has not been a great deal of credit card counterfeiting carried out in Australia, although counterfeit credit cards manufactured in Hong Kong are said to be readily available in Australia to organised crime groups. There have also been reported instances of school-aged offenders

successfully counterfeiting plastic cards. In 1996, counterfeit credit cards were estimated to cost Australian banks between $5 million and $6 million per annum (Hay 1996).

Application Fraud

Perhaps the weakest link in the security chain of plastic cards, however, relates to the manner in which they are issued. Frauds relating to the issue of cards may be perpetrated in one of two ways.

First, so-called "true name fraud" occurs when an offender obtains the personal details of a real person and uses them to acquire credit cards in that name. The offender then uses the cards to purchase goods for which the liability passes to the legitimate cardholder.

The second type of fraud involves the use of false identification details, which are used to obtain a legitimate card in a false name by individuals who later default on payment and abscond. Offenders now use desktop publishing equipment to fabricate identification documents which are then used to satisfy the 100 points of identification required. In Victoria, recently, an offender opened 42 separate bank accounts making use of false identification documents. When arrested, he had created 41 false birth certificates, 41 false student identification cards and a driver's licence. These were used to open false bank accounts, register a business name, obtain Medicare refunds, and defraud various retailers.

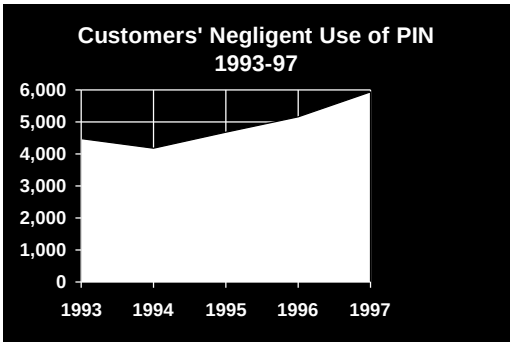
Application fraud traditionally accounted for only a small percentage of plastic card fraud cases with card issuers being quite successful in taking preventive action. In England, for example, between 1991 and 1993, losses sustained through application fraud declined more than 50 per cent, due to a range of security initiatives (Newton 1995, p. 20). More recently, in Australia, however, application fraud is increasing, principally through the use of counterfeit identification documents.

PIN Fraud

Other vulnerabilities arise out of the way that the individual making use of the card authenticates his or her identity when using the card. This is mainly a problem with debit cards used in electronic card reading machines, which can verify the identity of cardholders by requiring them to enter a PIN or password. In order to enhance the security of the system, the user's PIN is encrypted before it travels through the network, thus making it difficult for the PIN to be discovered by hacking into the network.

A more substantial security risk arises from the manner in which the PIN is communicated to the cardholder, recorded and remembered by the cardholder, and used by the cardholder at a terminal during a transaction. Although cardholders are clearly warned of the dangers associated with disclosing their PIN, writing it on the card, or keeping it in the same place as the card, a considerable proportion of cardholders refuse to heed such advice, thereby placing themselves at risk of loss - for which they will be personally responsible. Figure 1 shows the increase in the number of complaints relating to customers' negligent use of PINs in Australia recently.

Figure 1. *Number of Complaints where Customer liable because of negligent Use of PIN, 1993-97, Australia*



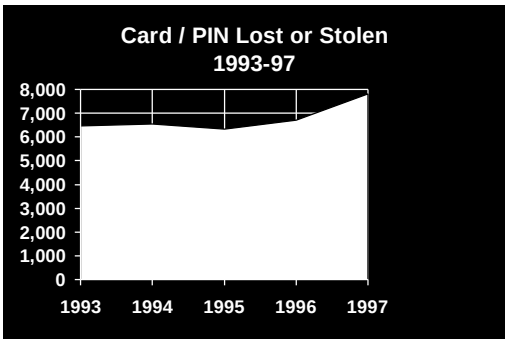
Often, however, cardholders may disclose their PINs unwittingly or through understandable exploitation by confidence tricks. Occasionally, violence may be used to coerce cardholders into disclosing their PIN or telephoto lenses may be used to observe customers when they key in their PIN in a public place. In 1987, for example, a group of schoolboys in Perth were apprehended after manufacturing cards and obtaining PINs by observing cardholders through binoculars (Tyree 1990, p. 264).

Misuse of Cards

The final area of vulnerability arises out of the way in which cards are used or misused.

First, fraud can be facilitated if cards are lost or stolen. In Australia, between 1993 and 1997, the number of complaints made to the Australian Payments System Council arising out of lost or stolen cards or PINs increased from 6,466 to 7,814 (*see* Figure 2).

Figure 2. *Number of Complaints where Card or PIN was lost or stolen, 1993-97, Australia*



As we have seen, offenders may also alter cards or manufacture counterfeit cards. Occasionally, this may occur on a wide scale. In England, for example, an operation mounted by the Metropolitan Police Organised Crime Group led to the seizure of 100,000 forged, plastic cashpoint (ATM) and credit cards, as well as various computers and equipment used to insert information on magnetic strips (Anonymous 1996, p. 4).

Fraud can also be perpetrated by cardholders exceeding the cash transaction and credit limits of cards, or by using company or government cards for unauthorised purposes. Such fraud often involves substantial losses to large businesses or government departments.

In the 1994 survey of the fraud experienced by 477 medium to large-sized businesses in Victoria, for example, 41 cases that involved the fraudulent misuse or theft of company credit cards were reported. Estimated losses amounted to $70.9 million (Deakin University 1994, p.12).

In 1994, the Australian National Audit Office conducted an audit of a sample of transactions undertaken with the Australian Government Credit Card (Commonwealth of Australia, Australian National Audit Office 1994). From November 1987, when the card was introduced, until March 1994, there were 46 serious cases of fraud reported involving amounts totalling $1.8-$2 million.

Most of the frauds related to the unauthorised purchase of goods to be used for private purposes, or for travel and hospitality which had been paid for from other sources.

Credit card fraud is also carried out on the Internet. At present, most commercial transactions which take place on the Internet are undertaken by customers purchasing goods and services by disclosing their credit card details. It has been estimated that transactions valued at approximately $A640 million took place on the Internet in 1995, and by 2005 global online commerce is expected to reach between $A97 billion and $A238 billion.

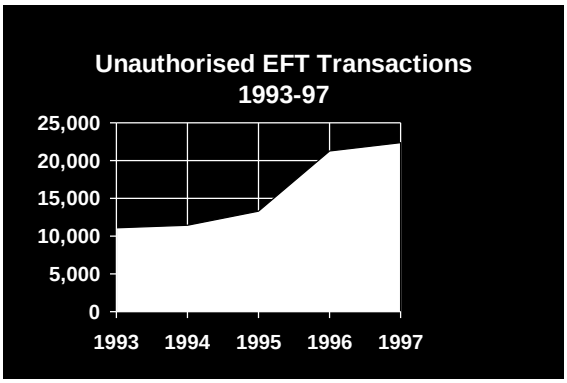
Credit card information is illegally obtained either by hacking into databases of account numbers which are held by Internet service providers, or by intercepting account details which travel in unencrypted form. In Sydney, on 27 March 1998, for example, a computer hacker was sentenced to 18 months' imprisonment for having illegally obtained access to an Internet Service Provider's database of credit card holders and published details relating to 1,225 cardholders resulting in the business losing more than $2 million (R. v *Stevens* unreported decision of the NSW District Court, 27 March 1998). There are also many online scams perpetrated by customers who make use of false credit card details, as well as merchants who fail to honour online agreements.

ATMs and EFTPOS terminals have also been targeted by offenders who have done everything from stealing entire ATMs laden with cash, using stolen cards and PINs to make unauthorised cash withdrawals, to interfering with bank computers in order for sums in excess of account credit balances to be withdrawn. In the United States it has been estimated that 40 per cent of ATMs have been subjected to fraud with losses ranging from between $A12,800 and $80,600 (Sullivan 1987, pp. 187-8).

On occasions, substantial sums have been lost in individual incidents. In Italy, for example, one fraud which involved three ATM transactions resulted in a bank losing $A5.1 million.

Although electronic funds transfers at point of sale are only relatively recent innovations now used around the world, there are some indications that their security systems have been breached. In Australia, since 1993, the number of unauthorised electronic funds transfer transactions (EFT) has continued to increase, particularly between 1995 and 1996 (*see* Figure 3).

Figure 3. *Unauthorised EFT Transactions*, 1993-97, Australia*



But with 1.44 billion EFT transactions conducted in the 12 months to 31 March 1997, the number of unauthorised instances is proportionally small.

Stored value cards are also used for a variety of fraudulent activities. Card readers could be programmed to deduct more value from the card than the amount authorised by the legitimate user, or sales staff could intentionally deduct higher amounts than they are authorised to deduct. Sums which are rounded off to the nearest five cents might be skimmed to the terminal owner's advantage.

Finally, stored value cards could be stolen and, if unprotected by a PIN, or if the PIN is able to be compromised, the value might be removed from the card. Smart cards might also be used for money laundering and tax evasion, and for fraud carried out via counterfeit cards.

PLASTIC CARD FRAUD PREVENTION STRATEGIES

There are four primary strategies which can be used to prevent plastic card fraud.

Action by Card Issuers

Card issuers can adopt a wide variety of strategies to reduce the risk of plastic card fraud. The most pressing need is for financial institutions not to issue cards to individuals unless they are satisfied of their identity. Although the 100 point system for opening accounts is a starting point, this needs to be used properly with primary documents such as birth certificates being thoroughly checked and validated. The primary identification documents themselves might need to be produced in such a way as to reduce the possibilities of counterfeiting.

Various procedures could also be adopted to ensure that plastic cards are not stolen and that cards and PINs are communicated securely to customers. Banks could also assist merchants by notifying them promptly of stolen cards and PINs. For example, banks now have a centralised fraud reporting and investigation agency for plastic cards, Cardlink Services Limited, which maintains close liaison with the police. Cardlink investigates cases of fraudulent use of cards in each state and territory of Australia, and gathers evidence which is then forwarded to police (Van-Rhoda 1991, p. 127).

Cards could also be required to display the holder's photograph, while security procedures could be enhanced for those involved in the legitimate manufacture of cards to ensure that

PVC sheets, dyes, embossers and encoders are not stolen and used for counterfeiting (*see* Duncan 1995, p. 26).

One of the main strategies used to prevent EFTPOS fraud has been simply to lower floor limits (the transaction value at which authorisation is required from banks before the card can be accepted).

Finally, various transaction monitoring strategies have been suggested to minimise losses through smart card fraud by quickly identifying fraudulent transactions and limiting the maximum value of transactions (AUSTRAC 1996).

Action by Merchants

Frauds involving merchants constitute a large problem for financial institutions as merchants or their employees are ideally placed to permit access to computer networks and to alter transaction details. Bonney (1992, pp. 6-8) discusses various ways to prevent credit card fraud including the conduct of random authorisation checks of merchants' bank accounts and sales voucher records, as well as merchants advertising the fact that steps are being taken to prevent credit card fraud in their premises, and closer examination of the security features of cards by sales staff when transactions are being conducted.

Merchants should also obtain a delivery address and telephone number when orders are placed by telephone and then call the number to verify the information provided; obtain proof of identity from individuals who collect goods purchased by credit card and inspect the credit card used; and ensure that deliveries of goods are made to the person who placed the order (*see* Van Leeuwen 1996).

Finally, merchants should examine any suspicious behaviour and appearance of customers. This might involve customers selecting purchases rapidly; being dressed inconsistently with the nature of the purchases selected; customers who split purchases between various slips in an attempt to forestall authorisation calls to issuers; customers seeking to rush a transaction; customers who make a purchase and then return for more later; customers who make multiple purchases all under the floor limit; and customers who buy many of the same items but in different colours and sizes (Grau 1992, p. 39.5).

Unfortunately, it is often not possible for merchants to use all of these techniques through fear of deterring potential customers.

Action by Cardholders

Protection of one's card, PIN or password is the primary crime prevention strategy which card holders need to take. Although consumers are advised not to disclose their PIN, keep it with their card, or write it on the card, studies have revealed that between 20 and 70 per cent of people fail to adhere to such advice (Sullivan 1987, p.189, n.19).

Where these strategies have been consistently implemented, substantial reductions in fraud can occur. In Britain, for example, the use of a variety of strategies designed to prevent plastic card fraud resulted in a 41 per cent reduction in such fraud overall between 1991 and 1994, while losses occurring at retail points of sale were reduced by 49 per cent during the same period. Losses from cards lost or stolen in the post were reduced by 62 per cent between 1991 and 1994 (Webb 1996, pp. 24-5).

Technological Solutions
A wide range of technological solutions have also been devised in order to reduce the security risks associated with plastic card payment systems.

Terminal Safeguards - ATM and EFTPOS terminals need to be manufactured in such a way as to ensure that access cannot be gained to cables, and that reserves of cash cannot be stolen in the case of ATMs. Machines should also be located in secure places where users are protected both physically, as well as against shoulder-surfing, to obtain PINs. Barriers can be fitted to ATMs and horizontal key pads used to prevent shoulder-surfing in accordance with Australian Standard AS 3769, which governs the positioning of ATM and EFTPOS devices where PIN entry is required.

Protections Against Card Counterfeiting - Various strategies have been devised to enhance the security of plastic cards and to make them more difficult to alter or counterfeit. These include the use of security printing, micro-printing, holograms, embossed characters, tamper-evident signature panels, magnetic stripes with improved card validation technologies, and indent printing. Although such protections against card counterfeiting have deterred many potential offenders, organised criminal groups - who are often as technologically adept as those in the security industries - have often been successful in defeating new security measures.

Card Restrictions - As an alternative to target hardening, the risk of large-scale fraud through the use of plastic cards could be reduced by placing limits on the size of card-based transactions or the amounts of money that may be stored on plastic cards. There could also be a limit on the life of the cards.

Cardholder Verification - Some of the strategies devised to improve cardholder verification include the use of cards which have a photograph of the user; laser engraved signatures; longer PINs; and various biometric means of verifying identity, such as signature, fingerprint, palm, lip, ear or retina scanning (Sullivan 1987, p. 189). The costs and volume of data required to be stored online to enable comparison for any potential user might, however, be prohibitive.

Fraud Detection Software - Software has also been devised which is able to analyse plastic cardholder spending patterns in order to alert individuals to the presence of unauthorised transactions. Merchant deposit monitoring techniques also exist to uncover claiming patterns of corrupt merchants. One software package called PRISM (Proactive Fraud Risk Management) is used to detect credit card fraud carried out through the use of lost cards, stolen cards, counterfeit cards, fraudulent applications, cards never received, mail order, phone order and catalogue sales and merchant fraud. The cost is between $384,000 and $1.92 million depending on system requirements and configuration (Nestor Inc. 1996). While initial installation costs may be high, the benefits obtained through the prevention and detection of fraud make the use of such systems worthwhile for large organisations.

Improved Cryptography - Finally, cryptography, which is the mainstay of electronic banking security systems, could be improved to protect ATM transmissions and data held in stored value cards. This is currently being explored to secure online electronic cash systems by joint ventures such as MasterCard and Visa International's Secure Electronic Transaction Protocol, which uses public key encryption to protect data from being comp-
romised, and is expected to be fully operational shortly.

OLYMPIC VULNERABILITIES

When Sydney hosts the Olympic Games in September 2000, there will be hundreds of thousands of visitors coming to Australia. Among them will be some who may seek to perpetrate plastic card fraud and others who, unfortunately, will be the victims of such fraud.

The opportunities for the commission of fraud at the Olympics will arise out of a number of circumstances. Firstly, people will be bringing a wide variety of types of plastic cards with them to Australia which may be unfamiliar to local merchants and accepted for use even though they are illegitimate.

During the Barcelona Olympics, for example, plastic card counterfeiters produced a Visa "Olympia" card with five rings and the Visa logo, which Visa actually never produced - the whole idea being a fabrication (Mativat & Tremblay 1997, p.174).

Individuals visiting Australia might be unfamiliar with English and with some of our transaction systems, and so are vulnerable to deception. Cards used during the Olympic Games will principally be for retail purchases, which is the transaction type most frequently targeted for credit card fraud (Bonney 1992). Financial institutions are hoping to avoid many retail frauds by requiring customers to use stored value cards instead of credit cards. Offenders may, however, be visiting Australia for relatively short periods of time, so enabling them to offend and then leave the country immediately under their cover of being an Olympic tourist.

Conclusion

The solution to plastic card fraud, and particularly that which might occur at the Sydney 2000 Olympic Games, will ultimately depend upon the adoption of a range of strategies, both technological and strategic, in which close cooperation would exist between all those involved in providing and using systems. This includes financial institutions, retail merchants, and individual users.

Policy-makers should recognise that the plastic card industry is being deliberately targeted by organised criminal enterprises from around the globe. The perception that it is only an industry problem is no longer sustainable. The key to reducing plastic card counterfeiting and disrupting organised criminal enterprises is the establishment of a meaningful partnership between industry, merchants and law enforcement agencies.

Those involved in running card payment systems need to be prepared to exchange pertinent, sensitive and timely information with law enforcement agencies to enable them to target corrupt merchants and other organised criminals involved in plastic card counterfeiting productively.

Strategic planning to enable this to be done, should be carried out now if the vulnerabilities of the Sydney 2000 Olympic Games are to be avoided.

Note: This paper was first published by the first-named author in the Australian Institute of Criminology's Series *Trends and Issues in Crime and Criminal Justice*, No. 71, in July 1997.

References

Anonymous 1996, "Police crack inter-national credit card forgery ring", *CJ International*, vol. 12, no. 5, p. 9.

Australian Payments System Council 1993-97, *Annual Reports 1992-97*, Reserve Bank of Australia, Sydney.

AUSTRAC (Australian Transaction Reports and Analysis Centre) 1996, *Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board*, Commonwealth Law Enforcement Board, Canberra.

Bonney, R. 1992, *Preventing Credit Card Fraud*, New South Wales Bureau of Crime Statistics and Research Crime and Justice Bulletin No. 17, NSW Bureau of Crime Statistics and Research, Sydney.

Commonwealth of Australia, Australian National Audit Office 1994, *The Australian Government Credit Card: Some Aspects of its Use*, Audit Report No. 1, 1993-94, Project Audit, AGPS, Canberra.

Deakin University 1994, *Fraud Against Organisations in Victoria*, Deakin University, Geelong.

Duncan, M. D. G. 1995, "The future threat of credit card crime", *RCMP Gazette*, vol. 57, no. 10, pp. 25-6.

Grau, J. J. (ed.) 1992, *Criminal and Civil Investigation Handbook*, 2nd ed., McGraw-Hill Inc., New York.

Hay, J. 1996, "Smart cards open a Pandora's Box of scams", *Queensland Sunday Mail*, 19 May, pp. 20-1.

Jackson, J. 1994, "Fraud masters: Professional credit card offenders and crime", *Criminal Justice Review*, vol. 19, no. 1, pp. 24-55.

Mativat, F. & Tremblay, P. 1997, "Counter-feiting Credit Cards", *British Journal of Criminology*, vol. 37, no. 2, pp. 165-83.

Nestor Inc. 1996, "Proactive fraud risk management: Neural network based credit card fraud detection from Nestor Inc." Internet http://www.nestor.com/rmd.htm

Newton, J. 1995, *Organised Plastic Counterfeiting*, HMSO, London.

Sullivan, C. 1987, "Unauthorised automatic teller machine transactions: Conse-
quences for customers of financial institutions", *Australian Business Law Review*, vol. 15, no. 3, pp. 187-214.

Tyree, A. L. 1990, *Banking Law in Australia*, Butterworths, Sydney.

United States Senate, Permanent Subcommittee on Investigations of the Committee on Government Affairs 1993, *The New International Criminal and Asian Organized Crime: Report*, United States Government Printing Office, Washington.

Van Leeuwen, H. 1996, "A surge in credit card fraud", *Financial Review*, 24 September, p. 49.

Van-Rhoda, T. 1991, "Credit card fraud", *Journal of the Australasian Society of Victimology*, Special Edition, April, pp. 127-9.

Webb, B. 1996, "Preventing plastic card fraud in the UK", *Security Journal*, vol. 7, pp. 23-5.