AUSTRALIAN AND NEW ZEALAND SOCIETY OF CRIMINOLOGY
Brisbane 8-11 July 1997
CRIME POWER AND JUSTICE

CRIME PREVENTION IN THE DIGITAL AGE

Russell G. Smith*

I - INTRODUCTION

Since Wheatstone and Cooke first patented their system of communication by the means of electromagnetic impulses carried over wires in 1837, crimes have been committed through the misuse of telecommunications equipment. Every technological development has provided a new opportunity for criminality which has often been utilised to obtain property and financial advantage by deception.

The challenge for law enforcement policy makers is to keep ahead of offenders who are often as technologically skilled as the people who create telecommunications and computer security systems. Indeed, some offenders have had a history of working in the telecommunications industry themselves. Rather than wait until offenders devise new ways of utilizing technology for fraudulent purposes, regulatory agencies including law enforcement bodies need to have strategies in place which will anticipate new forms of criminality and prevent them from being carried out.

This paper will consider how best to regulate the provision of telecommunications so as to minimise opportunities for the commission of fraud. In order to illustrate the nature and extent of the problem, the paper will focus on three areas in which telecommunications systems have been misused to enable fraudulent activities to be carried out: first, telemarketing, secondly, the provision of telephone services and finally, the transfer of funds electronically.

The paper will provide a brief description of the ways in which fraudulent activities in each of these areas have been perpetrated, an estimate of the extent of the problem and an analysis of the various crime prevention strategies which have been adopted and which could be used in the future to control the problem.

II - THE NATURE AND EXTENT OF THE PROBLEM

1. Telemarketing Fraud

Direct marketing, by post or telecommunications, is increasing as a medium of commerce in Australia. In 1995, telemarketing comprised twenty-five per cent of the volume of the A$4.5 billion Australian direct marketing industry, and nearly half of adult Australians have received a telephone call relating to telemarketing activities (Australian Telecommunications Authority 1995, 10). In recent years, the use of the telephone for selling goods, services, and investment products, as well as for soliciting charitable contributions, has been significantly enhanced by innovations in information technology. The more familiar of these innovations are ones which permit the storage and retrieval of telephone numbers, automatic high speed dialling, and the transmission of recorded solicitations. Telemarketing has become much more efficient than direct mailing or door to door sales.

As we approach the 21st century, the telephone is being complemented as a medium of electronic commerce by the Internet and by commercial on-line services (Buckeridge and Cutler 1995). Globally, at present the Internet consists of 15,000 computer networks linked to twenty million users in over 175 countries, numbers which are expanding daily. Around half a million Australians are already connected to the Internet, some through educational and business enterprises and others privately at home through the use of modems connected to personal computers. In the near future, broadband services will be made available such as those which enable interactive video images to be transmitted and received across fibre optic cables using digital technology which will make services provided on the Internet more attractive to users.

Commercial sites and advertisements have begun to proliferate on the Internet although unfortunately, not all of these advertisements are legitimate. Fraudulent and deceptive advertisements may originate from and be accessible to individuals anywhere in the world and although these are similar to fraudulent solicitations by telephone or fax, the fundamental difference is that Internet solicitations tend to be less targeted, and less personal than using traditional media.

By the year 2001, it has been estimated that the value of Internet commerce will range from between 6 and 600 billion dollars, the actual size depending upon the extent to which secure and accessible Internet payment systems operate. The potential for telemarketing fraud created by such an extensive commercial environment is, therefore, significant.

There are no estimates of the magnitude and cost of telemarketing fraud in Australia, although some anecdotal evidence does exist. In the United States, however, the Attorney General of the United States and the Chairman of the Federal Trade Commission suggest that the cost of telemarketing fraud in the United States is about US$40 billion per year. Lesser estimates place the cost of telemarketing fraud as high as US$15 billion (Kertz and Burnette 1992).

The logistics of traditional telemarketing fraud are basic. Organized telemarketing fraudsters establish temporary telephone banks, commonly termed

'boiler room' operations. From these locations, they contact individuals at random, or in specifically targeted groups. Fraudulent schemes are as varied as the human imagination. The basic fraud entails an offer which appears to be (and is) too good to be true, accompanied by a request for an 'up front' payment. The fundamental strategy of the fraudster is to persuade the victim to pay in advance by cheque or credit card for the product or service in question. The fraudster then either provides a grossly inferior product, or fails to deliver altogether.

Fraudsters may request payment in readily negotiable form such as money orders, sent by overnight courier, and immediately convert the instrument to cash upon receipt. A note of urgency can be introduced in order to convey the impression that 'supplies are limited', or that 'the offer is about to expire'.

There are two basic forms of telemarketing fraud. The first targets a small number of individuals, often drawn from specific backgrounds, such as professionals, or the affluent elderly, with a view to scoring a few big hits. The second type targets a large number of individuals, and aims at a relatively low return from a large number of victims.

The offer of investment products promising astronomical returns is a familiar example of the first type of fraud. Investment frauds can be based on an endless variety of products, including 'rare' coins ostrich chicks, health cures, gemstones, art, oil and gas leases, interests in oil wells, cellular telephone licenses, precious metals, and more. A recent example of an advance fee fraud involved a group of Nigerians requesting assistance from gullible foreigners in moving non-existent funds allegedly belonging to the Federal Government of Nigeria out of Nigeria in order to avoid government confiscation of the funds.

Prospective victims were advised of huge contracts for purchase of vehicles, computers, agricultural machinery, etc. at various State Ministries. Other prospective victims were informed of the availability of millions of dollars from fictitious or allegedly existing and unclaimed estates of deceased individuals or from previously fulfilled contracts in Nigeria which were available for claim by relatives of the deceased. The proposals required the use of a bank account outside Nigeria to which many millions of dollars would be credited in the expectation that the assistance given would be rewarded by retention of a proportion of the funds, usually ten per cent. The proposals also required the initial transfer of an establishment fee to enable the transaction to proceed which was then stolen and the rest of the transaction not completed.

Nigeria developed a comprehensive and effective response to the fraud in which the main objectives were to create an awareness of the risk and increase prosecutions and recoveries in cases where funds were lost, reducing losses and intercepting various attempts. One organisation in Iceland has also undertaken a comprehensive investigation of the frauds using the Internet (see International

Investigation Services Home Page http://www.islandia.is/~njall/nig/nigeria.html. See also Main and Stretton 1994).

Developments in telecommunications have begun to provide the basis for, as well as the medium of, telemarketing fraud. High-pressure promotion of paging licenses and pay-per-call investment schemes began to proliferate in the United States during 1995.

Advances in telecommunications technology have for some time permitted random automatic dialling. Alternatively, fraudsters may focus on a particular target group, such as senior citizens, medical practitioners or wine enthusiasts. Machine readable mailing lists of periodicals with a specialized readership or associations with a defined membership are often obtainable, as are the 'electronic white pages'. A system called Automatic Number Identification (ANI) automatically identifies and stores the number from which one is dialling. By matching these phone numbers with other computerized lists and street directories, one's name and address can often be discovered. Professional fraudsters in the United States compile special phone lists according to demographic characteristics of residents, and even trade 'sucker' phone lists containing the names of victims who have fallen for previous scams. Currently available information technology permits very sophisticated matching and refinement of lists, to enable increasingly precise targeting of prospective victims.

Although many fraudulent pitches are quite direct, the Internet provides a vehicle for more insidious marketing. 'Disguised advertising' on the Internet is difficult to recognize because it is not always apparent that a product is being advertised. Bulletin boards and chat forums may contain comments or statements about the quality or the performance of products or services. These may in fact be advertisements.

The development of telecommunications technology now enables telemarketing fraud to be perpetrated from across the world. Cost considerations, which in the past tended to confine telemarketing fraud to a relatively proximate location, are no longer prohibitive. Telephone calls can originate anywhere, and verification of the bona fides of the caller is that much more difficult. The recent emergence of Internet commerce extends the reach of marketing, for both legitimate as well as illegitimate purposes.

2. Telephone Services Fraud

At present, Telstra which is Australia's largest telecommunications carrier, has some 8.6 million customers who make around twenty-five million calls a day (Harris 1995). There are approximately 3 million mobile telephone subscribers in Australia who spend between $10 and $500 a month on their calls, thus creating a market estimated to be worth $3.5 billion a year (Crowe 1996: 16).

By the year 2000, the Bureau of Transport and Communications Economics has estimated that mobile telephone sales will have reached between five and seven million while Optus has forecast this to be closer to eight million (O'Neill 1996: 22). Unfortunately, not all of these customers will be willing to pay for the services they obtain.

In Australia, the Australian Federal Police has uncovered a number of telecommunications frauds in recent years some of which have resulted in prosecutions being conducted and terms of imprisonment being imposed.

In 1992, for example, two Chinese Nationals living in Australia were prosecuted for manufacturing devices designed to intercept public telephone lines enabling calls to be made without charges being incurred (Australian Federal Police 1993: 18). Later, in February 1993, a man was sentenced to eight years' imprisonment for his part in an fraud involving more than $400,000 in which he operated an international switchboard providing cheap calls between the Middle East, Australia and elsewhere (ibid. 16). 1994 saw a large increase in reports of stolen telephone services including one case involving six individuals who used a company's telephone system to make ISD calls resulting in the company losing approximately A$50,000 (Australian Federal Police 1994: 21).

In Victoria, recently, two English language students from China were convicted of defrauding Telecom (now Telstra) of approximately A$24,000. In 1992 they illegally connected an electronic device to wires within Telecom 'pits' adjacent to public telephone booths which caused nine separate 0055 information numbers repeatedly to ring. For every call made, Telecom received thirty-five per cent of the call charge while the service provider received the remaining sixty-five per cent, of which a proportion was paid to the offenders as information providers. By causing a constant stream of calls to be made to the numbers, the offenders were able to deflect some A$167,000 of Telecom's money to the service providers who then paid part of this into various bank accounts opened by the offenders in false names (R. v *Liang and Li* [1985] 82 A Crim R 39).

Internationally, the losses being sustained through theft of telephone services are even more substantial than in Australia. Recent British Telecom statistics cited by Schieck (1995: 2-5) suggest that in 1990, security failures at BT cost approximately the equivalent of A$595 million of which A$58 million related to four main types of billing fraud (see below). Telephone fraud in the United States is estimated to amount to the equivalent of A$5.3 billion annually while in 1993, the cable television industry in the United States lost nearly A$6.6 billion from theft of premium and basic services (ibid. 2-5). Olson (1994: 12) cites some recent examples of telecommunications fraud in which an American chemical company lost the equivalent of A$900,000 in three weeks while an Ohio manufacturer lost A$400,000 over one weekend.

Mobile telephone fraud is a recent area of particular concern. Frauds involving cellular telephones have been carried out using both traditional techniques which were used to obtain fixed wire services free, such as the use of false identities when engaging services, as well as novel approaches which make use of technological flaws in security procedures. Some may be relatively simple such as making calls from a stolen handset which, if unprotected by a PIN, will be billed to the legitimate subscriber until such time as the theft is notified and the service withdrawn.

More sophisticated offenders have used a variety of illegal techniques to create counterfeit cellular telephones which are able to be used to make calls with charges being billed to legitimate owners of the telephones. Unauthorised access to the network is gained initially by ascertaining the Electronic Security Number / Mobile Identification Number (ESN / MIN) combination used in a mobile telephone. Electronic scanners are used which are capable of reading these numbers while they are being transmitted through the airwaves. Such devices store the numbers obtained and then load them into computer software ready for programming into another telephone (Brooks and Davis (1994: 67-8). Alternatively, security numbers can be obtained directly from manufacturers and retailers who have less than adequate security procedures in their offices (Sulc 1994: 63).

Although a number of instances of cloning have occurred in Australia, the problem is largely confined to the United States and Britain at present. In Britain, for example, cloning is said to have increased by five hundred per cent during the period August 1994 to August 1995 with over 4,000 incidents per month (United Kingdom, Industry and Government Study Group on Mobile Phone Fraud 1995).

In the United States, Brooks and Davis (1994: 67) estimate that cellular telephone fraud is costing a million dollars a day to the industry with the equivalent of A$900 million a year lost on illegal calls actually detected. In Britain, the Parliamentary Office of Science and Technology (1995: 28) estimates that between 12,000 and 15,000 analogue and up to 1,000 digital mobile telephones are stolen each month and that up to forty per cent of car break-ins in London are for the purpose of stealing a mobile telephone. The British Industry and Government Study Group on Mobile Phone Fraud has also estimated that the total quantifiable direct costs to the mobile telephone industry and its customers of mobile telephone fraud is in excess of the equivalent of A$250 million. Mobile telephone subscription fraud, alone, is estimated to amount to the equivalent of A$144 million per annum or one per cent of network turnover (United Kingdom, Industry and Government Study Group on Mobile Phone Fraud 1995).

In Victoria, there has been a threefold increase in the number of mobile telephones stolen from 1,943 in the financial year 1994-95 to 6,322 in the period July 1995 to January 1996. During the same period, the increase in

ownership of mobile telephones in Victoria more than doubled from an estimated 495,000 in the year 1994-95 to 1.17 million in the year 1995-96 (Adams 1996).

One of the largest telecommunications frauds ever discovered involved a group of Palestinians in the occupied territories of Israel who made long-distance calls to other Middle-Eastern countries while having the calls charged to cellular telephone subscribers in Arizona. This arose out of an Israeli law which prohibited calls being made to nearby countries due to security risks thus forcing the Palestinians to adopt alternative means to make calls to their friends and relations. One United States Secret Service operation which took place in Phoenix, Arizona in January 1992 resulted in the recovery of thirty-five cellular telephones and ten thousand microchips and notebooks filled with electronic codes. In nineteen days it was estimated that 57,000 calls had been diverted through Arizona with United States telecommunications companies losing the equivalent of up to A$1.3 million in long-distance charges and air time (Ramirez 1992: D1).

3. Electronic Funds Transfer Fraud

A wide variety of telecommunications-based systems exist which enable funds to be transferred electronically. One international Belgian organization, for example, the Society for Worldwide Interbank Financial Telecommunications (SWIFT), connects over 5,000 financial institutions in over 80 countries. By the early 1990s it carried over one million messages a day (Mackrell 1996: 35).

As a potential target for fraud on a large scale, these systems hold great attraction by reason of the large sums of money they carry. In Australia, for example, international funds transfers amounted to A$50 billion in 1995 which is two thirds of the total value of payments exchanged between banks. Retail electronic transfers accounted for A$1 billion in 1995 or one per cent of the total (Australian Payments System Council 1995, *Annual Report 1994-95*: 43-4).

Payments of small sums of money may be made electronically by way of direct debit in which payments are made directly from the payee's account to the recipient's bank or by way of credit transfer in which a payor advises his or her bank to debit his or her account with a sum which is electronically credited to another account. All such systems create a security risk if procedures are not in place to verify the availability of funds which are sought to be transferred or if account access controls are not in place. It is usual for plastic cards to be used to initiate such transactions which creates a potential for fraud if counterfeit or stolen cards are used.

In Australia, the first bank card was issued in 1974, followed shortly thereafter by MasterCard and Visacard. By 1992, there were almost ten million major credit cards in use in Australia (Bonney 1992: 1): 23). Plastic cards contain between one and three magnetised tracks which permit the identification of the user and

enable the user to conduct a transaction from a location distant from the central data base, such as a bank. Data processing associated with magnetic stripe cards takes place in the central data base unlike computer chip cards or so-called ‘smart cards’ in which data are stored and processed on the card itself.

Plastic cards are used for a wide variety of transactions. Credit cards permit card holders to obtain goods and services immediately with the card issuer providing funds to the merchant from the card holder’s account which may be held in credit or debit. If the card is stolen or a counterfeit made, it is possible dishonestly to obtain goods and services, including cash, on credit up to specified transaction ceiling amount until such time as the fraud is detected and authorization to use the card is withdrawn.

Magnetic stripe debit cards permit transactions to be conducted and bank accounts debited immediately through the use of on-line connections between the terminal being used and the bank. Two types of debit card terminals are commonly used: Automated Teller Machines (ATMs) and terminals which permit Electronic Funds Transfer at Point of Sale (EFTPOS).

ATMs are electronic vaults which enable users to withdraw or deposit money or obtain other banking services. They contain a supply of cash and other products such as cheque books, a Personal Identification Code reader, and disk drives for recording transactions when the machine is off-line or not connected to the host-computer at the bank’s head office. The main security risks associated with the use of ATMs relate to unauthorised transactions, that is, individuals gaining access to accounts and receiving cash from accounts other than their own or obtaining greater sums than their credit balance permits. Since 1989, there the number of ATM terminals in Australia has increased more than fifty per cent from 4,073 in 1989 to 6,175 on 30 June 1995 (Australian Payments System Council 1995: 29).

EFTPOS transactions are carried out using terminals connected to a merchant’s cash register which enable customers to pay for goods or to withdraw cash electronically via their bank’s computer. Transactions are carried out by the customer keying in a PIN to a terminal which then communicates details of the credit or debit through the EFTPOS network to the customer’s bank. Similar security checks are conducted as for an ATM transaction in order to verify the card, the card user and the credit balance available in the customer’s account when the transaction is made. Since 1989, there has been a much greater increase in the number of EFTPOS terminals in Australia (494%) than the number of ATM terminals while the number of EFTPOS transactions has also shown a substantial increase (254%). At 30 June 1995, there were 68,034 EFTPOS terminals in Australia which were used for 340 million transactions (Australian Payments System Council 1995: 29).

Some magnetic stripe cards can be loaded with value and then used to purchase goods and services. Such cards have been in use for many years now for purchasing telephone calls, transport services or other small items such as photocopies. The security risks associated with stored value cards are very similar to those of currency in that cards may be stolen and used immediately, although often only for a single type of transaction.

Smart cards are plastic cards which have electronic logic to store data and in some cases a microprocessor that can process data. The first smart card was developed in France and patented by Roland Moreno in 1974. Smart cards can be contact (which are activated when terminals touch a smart card reader) or contactless (which are activated by radio waves when passed near a transmitter). They may be memory only cards or processor cards depending on the extent of function given to the chip. The main security risk associated with smart cards lies in the way in which data are encrypted. If the card's code encryption system fails, the whole system will fail (Levy 1994: 177).

The latest generation of smart cards, known as super smart cards, contain a microprocessor, a keyboard, a liquid crystal display and a power source which enables the card to be used independently of a card reader (Commonwealth of Australia, Human Rights and Equal Opportunity Commission 1995: 11). A simplified version of this is being used by MasterCard in its Canberra trial with a 'Pocket Teller' being used in which cards may be read, the latest credit balance displayed and the last ten transactions recalled (MasterCard 1996).

Finally, Optical Memory Cards have been developed which can store optical images using laser light technology. These cards can store large amounts of data, up to 200 megabytes or 80,000 pages. Stored information cannot, however, be altered as it is kept in a ROM (Read Only Memory) (Commonwealth of Australia, Human Rights and Equal Opportunity Commission 1995: 12).

Various commercial activities are also able to be carried out using telephone and on-line connections. Telephone banking, for example, permits customers to obtain account balances, order statements, transfer funds between accounts and pay certain bills by the use of telephones. Security is provided by the use of passwords, PIN authentication, transaction codes and encryption of data in much the same way as an ATM system operates (Commonwealth of Australia, Bureau of Consumer Affairs 1995: 26).

The Internet is also being used to conduct business, mostly by customers purchasing goods and services by disclosing their credit card details (see Cavazos and Morin 1994 for a discussion of on-line business transactions generally). Transmitting credit card information in an unprotected electronic environment such as the Internet is perceived as a significant security risk by many and has led to new encryption systems being devised to protect the transmission of account numbers.

Electronic funds are also able to be stored on computers as well as on cards enabling funds to be transferred through telecommunications networks such as the Internet. A number of companies have started electronic cash systems including Digicash in the Netherlands and CyberCash Inc. in the United States. Digicash has since opened an office in Australia (McCrea 1996: 39). The Digicash system operates as follows. A banknote is created by a user on a personal computer and sent to the bank with its note number blinded out. The bank signs the banknote electronically and then returns it to the user who divides out the blinding factor. The user can now spend the electronic banknote at a merchant, who in turn deposits the note online for verification to prevent double spending (i.e. copying of notes by users).

The proliferation of electronic funds transfer systems has enhanced the risk that such transactions will be intercepted and funds diverted. Existing systems such as ATMs, and EFTPOS technologies have already been the targets of fraudulent activity. In 1991, the American Bankers' Association published the following estimates of annual losses due to financial fraud in the United States (converted to Australian dollars, Holland 1995: 88):

Credit card fraud	A$922 million
ATM fraud	A$23 million
Cheque fraud	A$13 million
On-line fraud	A$6 million

Most of the large scale electronic funds transfer frauds which have been committed have involved the interception or alteration of electronic data messages transmitted from bank computers (see Meijboom 1988: 27 and the English case of R. v *Thompson* [1984] 1 WLR 962 and the Australian case of *Director of Public Prosecutions* v *Murdoch* [1993] 1 VR 406). A recent example involved a group of Russian computer hackers who allegedly attempted to steal the equivalent of more than A$13 million from Citibank's electronic money transfer system. In May 1995, Vladimir Levin, a 34 year old Russian computer expert, was arrested in London and on 17 August 1995 he appeared in a London court charged with electronically robbing Citibank's cash management system from St Petersburgh of the equivalent of A$518,000. It was alleged that Levin was working in the Russian firm, AO Saturn, where he manipulated the computers at Citibank to transfer funds to accounts in Finland, Israel and Bank of America (Anonymous 1995; Holland 1995: 88). United States officials applied to have him extradited to the United States to stand trial.

In January 1996, another Russian involved in the alleged fraud, Alexei Lachmanov, aged 28, pleaded guilty to offences relating to his role in a scheme. The charges against Lachmanov alleged that in August 1994 he told co-conspirators in Russia about his personal accounts in Tel Aviv, Israel. The co-conspirators had gained unauthorized access to the Citibank Cash Management

System, which allows Citibank customers to gain access to a computer network and transfer funds from their Citibank accounts to accounts at other financial institutions. Lachmanov admitted to transferring funds from accounts to five Tel Aviv banks, and attempting to withdraw the equivalent of A$1.2 million from those accounts. Three other members of the gang have pleaded guilty to a variety of offences (Kennedy 1996).

Although extremely large sums may be stolen through the illegal interception of banking funds transfer systems, most frauds take place through the use of plastic cards. In Britain, plastic card fraud cost the industry the equivalent of A$260 million in 1993 with the largest losses being due to cards which are never received, lost or stolen. Credit cards and debit cards account for the greatest percentage of losses (Newton 1995: 20, 23).

Webb (1996: 23) describes the scope of the problem of credit card fraud in Britain. Between 1988 and 1990, the total cost of credit card fraud increased 126 per cent while the number of cards issued during this period increased only thirty per cent. The equivalent of A$170 million was lost through lost or stolen cards, A$60 million through cards lost or not received in the mail, A$6 million through counterfeit cards, and A$15 million through other frauds. Eighty per cent of frauds using plastic cards took place at retail point of sale (A$195 million), with the equivalent of A$30 million lost through international transactions taking place outside the UK, A$10 million through ATMs, and A$17 million at bank counters (p. 24).

In New South Wales, of all fraud incidents recorded by police, credit card fraud represented fifty-nine per cent in 1991. Between 1989 and 1990, the total number of credit card fraud incidents was at least 25,000 per annum. These figures underestimate the extent of the problem, however, as reporting rates for credit card fraud are extremely low (Bonney 1992: 1).

A variety of techniques are used to perpetrate ATM fraud most involving plastic cards and illegally obtained PINs. In the United States it has been estimated that forty per cent of ATMs have been subjected to fraud with losses ranging from between the equivalent of A$13,000 and A$82,000 (Sullivan 1987: 187-8).

An indication of the extent to which ATM fraud occurs in Australia is provided in the statistics of transaction complaints given in the Australian Payments System Council *Annual Report 1994-95* (1995). During the year 1994-95, 13,321 unauthorised transactions took place. Of these, 6,347 occurred due to cards of PINs being stolen, 4,635 occurred in circumstances in which cards or PINs had not been lost or stolen and 2,339 were due to other causes such as transactions which took place prior to cards being issued. Examples of the types of frauds perpetrated through the misuse of plastic cards in ATMs include *Kennison* v *Daire* ((1986) 160 CLR 537), R. v *Evenett* ([1987] 2 Qd R 753) and R. v *Baxter* ([1988] 1 Qd R 537).

In the year 1994-95, 746 complaints were resolved in favour of institutions owing to customers having acted fraudulently or illegally, which represents a twelve per cent increase on the previous year (666). 4,681 complaints were resolved in favour of institutions, however, by reason of customers negligently dealing with PINs. During the same year, only three complaints involved fraudulent conduct by employees of institutions, fourteen involved fraudulent conduct by employees and agents of merchants, while one complaint involved a card which was either forged, faulty, expired or cancelled.

The Australian Payments System Council *Annual Report 1994-95* (1995: 29) also records statistics of EFT system malfunctions which have increased rapidly over the last three years. In the year 1994-95, for example, 34,565 EFT system malfunctions were recorded which is twenty-nine per cent more than for the previous year (26,789). There has also been an increase in the number of unauthorized transactions reported. In the year 1994-95, these numbered 13,321 which is sixteen per cent more than for the previous year (11,490).

III - CRIME PREVENTION STRATEGIES

In deciding how best to approach the problem of telecommunications fraud, policy makers may choose to proceed down a variety of paths. One is to take legislative and administrative action to deal with the problem before it becomes unmanageable. Coutorie (1995: 27) states this position well.

> High technology crime has not yet directly affected many individuals in society and law enforcement administrators have been reluctant to dedicate much of their limited resources to this arena of crime. If nothing is done until it becomes politically important enough to target, law enforcement will be hopelessly behind the learning and technology curves to address the problem. Enormous resources, at enormous expense, and the use of outside law enforcement will have to be brought to bear to control it.

Already some of these fears have been realised in relation to mobile telephone fraud and some argue that it is already too late to introduce regulatory reforms. An alternative path requires policy makers to take a more cautious approach. This could best be achieved by self-regulation in the industries concerned and by a realisation that both the providers and users of services have a role to play in protecting their own interests and in preventing illegality for the benefit of all concerned.

Beginning with those crime prevention strategies which entail minimal amounts of state intrusion, the following strategies have been suggested as ways of controlling the three types of telecommunications fraud under consideration.

1. Technological Countermeasures

Telemarketing Fraud

A variety of restrictions can be imposed on telemarketers to minimise the likelihood of their making improper or illegal contact with members of the public. These include restricting hours for calling, providing silent telephone numbers, adopting caller identification systems and employing various blocking devices.

An alternative avenue of assistance exists in the market itself which may deliver products to assist individuals to defend themselves against telemarketing activity. As already mentioned, computer security is a thriving industry. Enormous profits will fall to those who successfully develop various technologies for protecting telecommunications systems against unwarranted intrusions.

Telephone Services Fraud

The primary strategy adopted by the telecommunications industry to deal with telephone services fraud has been the adoption of technological means to prevent continuing abuse of systems. The case of cellular mobile telephones is a good example of how continual technological improvement has been used to combat the ingenuity of criminals in obtaining services for free.

Some of the target hardening strategies which manufacturers, carriers and providers have adopted to control mobile telephone fraud include the use of software to detect calls being transmitted from a counterfeit telephone at the same time as another legitimate source (call collisions), to block the receipt of calls from cloned telephones altogether, velocity checks which are able to determine whether a telephone has moved too fast between serving areas to be legitimate, toll access restrictions to prevent unauthorised access to international dialling, unusual activity analysis to detect unusual usage patterns as an indication of fraud, dialled-number analysis which allows the carrier to block out high-risk countries or individual numbers, analysis of time of day, minutes of usage or credit activity for abnormal patterns of usage, radio frequency fingerprinting which measures the characteristics in a telephone's signal, and voice print matching which compares the subscriber's voice print with that recorded at the cell site (see: Sulc 1994: 65; Walters and Wilkinson 1994: 7; Young: 35). In the United Kingdom, however, the Parliamentary Office of Science and Technology (1995: 29) has observed that the use of some of these strategies may be difficult to implement with nearly two million telephones on each analogue network and the fact that service providers need access to network operators' billing data in real time rather than with the current twelve-hour delay.

Elsewhere, it has been reported that mobile telephone security numbers are being protected by devising viruses which will infect systems which gain unauthorised

entry into a chip (Anonymous 1993). New digital telephones which adopt the Cellular Industry Standard IS-54 will also be much more difficult to clone (Walters and Wilkinson 1994: 6). Systems are also in place which enable cellular telephones to be locked by the use of a PIN when the telephone is not in use allowing incoming calls still to be received but if the telephone is stolen out-going calls will not be able to be made (Cellular One 1994). Finally, various systems are being trialed to identify mobile telephone transmissions by the use of digital signatures (Brooks and Davis 1994: 68).

Each of these technological strategies carries with it further costs which, inevitably, will be passed on to customers. Because it is the customers who are the ones who suffer losses arising out of fraudulent activities, manufacturers, carriers and service providers may be reluctant to incur costs themselves in devising such crime prevention strategies.

Electronic Funds Transfer Fraud

A wide range of technological solutions have been devised in order to reduce the security risks associated with electronic funds transfer systems. They have been used at all stages of electronic transactions involving both transfers of funds and plastic card transactions.

Terminal Safeguards

Crime prevention needs to be focussed on areas of particular weakness in electronic systems and the most obvious target for electronic funds transfer systems is the computer terminal at which transactions are carried out.

As is the case with telephone kiosks, ATM and EFTPOS terminals need to be manufactured in such a way as to ensure that access cannot be gained to cables and reserves of cash cannot be stolen (Tyree 1990: 267). Machines should also be located in secure places where users are protected both physically as well as against ‘shoulder surfing’ to obtain PINs through the use of barriers, horizontal keypads, shields and hoods (Sneddon 1995: 44). Some ATMs have been placed in bank foyers with restricted card access and video surveillance equipment while others have even been placed under armed guard. Systems have also been designed which monitor vital points of an ATM for signs of physical attack. Although Australian Standard AS 3769 governs the positioning of ATM and EFTPOS devices where PIN entry is required, some older terminals which fail to comply with these standards are still in use.

Another strategy adopted by the First National Bank of South Africa in Johannesburg involves the use of voice-activated ATMs, although these present problems for individuals who are unable to hear messages clearly (due to hearing loss or traffic noise) or who have foreign language difficulties (Sneddon 1995: 44, n. 38).

Protections Against Card Counterfeiting

Newton (1995: 61) describes various crime prevention strategies which have been used to prevent plastic card counterfeiting. 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. Smart cards, of course, are much more difficult to copy than ordinary magnetic stripe cards. Unfortunately, all of these card authentication devices have been overcome by organised criminals except for computer chip circuitry in smart cards which has yet to be fully counterfeited successfully.

Card Restrictions

As an alternative to target hardening, a number of writers have suggested that the risk of large scale fraud and money laundering using smart cards could be restricted by placing limits on the amounts of money that can be stored on cards. Mackrell (1996: 34), for example, suggests that stored value cards should have a modest limit placed on the maximum value that can be stored on them, especially if they are to be used for card-to-card transfers. There could also be a limit on the life of the cards which would restrict their usefulness for hoarding and money laundering. In addition, it has been suggested that floor limits which apply to cards be reduced in order for transactions other than those involving very small sums to be checked with a bank on-line prior to completion.

Cardholder Verification

One of the greatest areas of risk associated with the use of plastic cards relates to the manner in which card holders' identities are verified. Some of the most recent suggestions for improving security in this area 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: 189). The costs and volume of data required to be stored on-line to enable comparisons to be conducted for any potential user may, however, make such techniques prohibitive.

Masuda (1996) provides an examination of a credit card crime prevention strategy employed since 1993 by Tops Appliance City Inc. in New York called 'Cardwatch'. This involves a computer network in a chain of retail stores in which credit card applications are checked by photographing the applicant digitally, recording the applicant's signature and other identifying information such as driver's licence, telephone and social security numbers, present address and current or last place of employment. This information is then used for future purchases and also when the customer collects merchandise (p. 17). Such an approach employs two fundamental checks on identity: something an account holder possesses (the card) and something that an account holder is (photograph etc). Because information is recorded about the individual, offenders are reluctant to take out accounts fraudulently. Cardwatch resulted in a ninety per cent reduction in credit card fraud losses over a seventeen month period following its introduction with a fifty-seven per cent reduction in per fraud loss.

Fraud Detection Software
A number of organisations are now providing software for use in the prevention of electronic funds transfer fraud. The success of such an approach depends upon the extent to which the software cannot be interfered with or modified. Software has also been devised to analyse plastic cardholder spending patterns in order to alert individuals to the presence of unauthorised transactions and also merchant deposit monitoring techniques to detect claiming patterns of corrupt merchants.

Nestor Inc., for example, provides software called PRISM (Proactive Fraud Risk Management) which is used to detect credit card fraud such as lost cards, stolen cards, counterfeit cards, fraudulent applications, cards never received, mail order, phone order and catalogue sales and merchant fraud. It is designed for use by credit card issuers, credit card processors, credit card acquirers, Merchant Banks and anyone who has over 500,000 cardholder accounts. It costs between the equivalent of A$389,000 and $1,943,000 depending on system requirements and configuration (see: Nestor Inc. 1996).

Improved Cryptography
A cryptographic system is a set of functions that are parameterized by keys and used for secrecy or authenticity. Encryption conceals data from anyone who does not know the secret key needed for decryption. Cryptography is, however, a double-edged sword in the field of electronic commerce as it is able to protect data from unlawful interference while at the same time concealing illegal activities from lawful investigation (Denning 1995: 330-5).

Cryptography is still employed as a mainstay of electronic banking security systems. Sullivan (1987: 194), for example, cites some of the recent developments in cryptography designed to improve bank security for ATMs. New algorithms have been devised which are buried in computer chips such that any attempt to read the code will destroy the chip.

2. Information and Education

Education has long been considered as one of the most effective ways of reducing the threat of criminality. Both children and adults need constructive training in the ethics of high technology and the undesirability of manipulation of technological systems for entertainment or financial gain (see, for example, Bequai 1987: 39). Walters and Wilkinson (1994: 7) similarly stress the importance of training and awareness of employees in fraud prevention strategies. They argue that there is a need for employee screening processes and fraud awareness training and that support vendors, sales agents and retailers need to be held accountable for fraud which results from their negligence.

Telemarketing Fraud

The best safeguard against telemarketing fraud would appear to be self defence and the most important means of controlling telemarketing fraud is the provision of information to prospective victims. Basic information to encourage wariness about overinflated claims should be widely available. As far as possible, such information should be packaged in a manner which educates the unwary without inspiring the predatory. Crime prevention information should prevent crime, not facilitate it.

A wide range of government and non-government agencies are involved in providing information to consumers. In the United States these include the Federal Trade Commission which produces an abundance of literature for general public consumption about consumer risks, rights and remedies. Other agencies include the Alliance Against Fraud in Telemarketing, the American Association of Retired Persons, the Commodity Futures Trading Commission, the Communications Fraud Control Association, the Council of Better Business Bureaus, the Direct Marketing Association, the Federal Communications Commission, and the Federal Trade Commission, the High Technology Crime Investigation Association, the Industry Council for Tangible Assets, the National Association of Bunco Investigators, the National Association of Consumer Agency Administrators, the National Charities Information Bureau, the National Council Against Health Fraud, the National Futures Association, the National Insurance Crime Bureau and Professionals Against Confidence Crime.

On-line services carry great potential for alerting the community in general, and individual consumers in particular, to the risks of fraudulent commerce. Web sites which alert prospective consumers and investors to possible scams are just as accessible as the sites which house fraudulent offerings. Where successful investigations and / or prosecutions are achieved, Web publicity can also be used for deterrent effect.

Telephone Services Fraud

A wide range of information is available to the users of telephone services alerting them to the risk of fraud and suggesting strategies for them to adopt to prevent victimisation. Companies such as Bell Atlantic (1996), Pacific Bell (1996) and Cellular One (1994), for example, offer advice to customers as to how telephone fraud may be prevented. Some recommended practices include noting the presence of frequent wrong numbers or hang-up calls, observing difficulties in placing outgoing calls, difficulties in retrieving voice mail messages and having incoming callers constantly receiving busy signals or wrong numbers. Some fraud prevention strategies which are recommended for customers to adopt include checking bills for unusual calls, keeping ESN and MIN numbers secure, locking telephones with a PIN when not in use, not leaving telephones unattended in cars, using only authorised technicians and eliminating international dialling capabilities of telephones when not being used.

Electronic Funds Transfer Fraud

In the field of electronic banking, one of the most effective strategies used to control crime is the education of the public as to the nature of the security risks which are present and how they may protect themselves. Sneddon (1995: 47), for example, stresses the need for members of the banking public to realise that their plastic card and PIN represent their electronic signature and need to be protected as such. Sneddon goes on to recommend that financial institutions use audio and visual electronic media to publicise the need for security such as by community service announcements on radio or television.

In the United Kingdom, one particularly effective plastic card fraud prevention strategy called 'Cardwatch' involved a high profile publicity and education campaign by the Association for Payment Clearing Service including posters, leaflets, and television and radio coverage to raise public awareness of the problem and to encourage card holders to take more care of their cards (Webb 1996: 24).

3. Self Regulation

Organizations which provide telecommunications services are well-placed to ensure that the potential for fraudulent use of their services is minimised. Indeed, sub-section (1) of section 47 of the *Telecommunications Act 1991* (Com) requires carriers 'to do their best to prevent telecommunication networks and facilities . . . from being used in, or in relation to, the commission of offences against the laws of the Commonwealth and of the States and Territories'. Although this does not permit a carrier to disconnect a service to a subscriber in breach of the rules of procedural fairness (see *Telstra Corporation Limited* v *Kendall* [1994] 55 FCR 221, discussed by Watts 1995), organisations are obliged to take obvious precautions such as conducting reasonable identification checks on new subscribers by requiring readily verifiable information to be provided.

Although accounting for only a relatively small proportion of illegal activities, conduct committed through internal security breaches or by the conduct of industry personnel may be prevented by ensuring that reliable and trustworthy staff are employed and that staff are adequately remunerated and have good working conditions, thus making them less desirous of engaging in illegal conduct. Internal organisational controls such as separation of duties and rotation of duties should enable misconduct by employees to be more easily identified. Specific training and ethical education of staff may also alert employees to the fact that security arrangements are in place within organisations.

In the United States, where obvious fraud prevention steps have not been taken by carriers, some subscribers have argued in civil proceedings that they should not

be held personally liable for fees incurred by reason of telecommunications fraud where the carrier has acted negligently in failing to ensure that systems operate securely. In one case in 1990, a company refused to pay an account totalling the equivalent of A$551,000 which had been improperly incurred and counterclaimed against the carrier in the sum of A$13 million for loss suffered as a result of the carrier's neglect in failing adequately to warn it of vulnerabilities in its PABX system which had enabled 30,000 unauthorised calls to be made. (*Mitsubishi* v *AT&T Communications*. See Cook 1991: 174 and Flanagan and McMenamin 1992: 63).

Some examples of the ways in which institutions can assist in reducing the risk of telecommunications fraud include the following.

Telemarketing Fraud

While the sheer volume of telecommunications traffic may preclude scrutiny of all content, many service providers now require signed undertakings as a condition of service that the user refrain from illegal activity, as well as from a range of lesser breaches of protocol, which may include telemarketing fraud. Breaches of these undertakings may result in termination of services, a powerful sanction.

Faced with the threat of heavy-handed attempts by government to impose regulation on Internet communications, various industry groups are developing codes of practice, to reduce the likelihood of some of the more egregious abuses of cyberspace. One recent code proposed by the Western Australian Internet Association requires service providers to adhere to the following requirements:

> I, as an online service provider shall not:
> (a) Knowingly permit those parts of my system under my control to have publicly available for downloading files which infringe copyright or contain unlawful material, provided that the provision of cache, mailbox or directory usage to users shall not constitute permission to misuse such facilities;
> (b) Knowingly permit a user to engage in criminal activity using access to my system, provided that such activity is identified as criminal by competent law enforcement authorities . . . (Jones 1995, 22).

Such a highly-qualified undertaking, while laudable in its intent, may be insufficiently strong to deter all illegality. Codes of conduct also have limited enforceability in an unregulated system.

Telephone Services Fraud

In relation to mobile telephone offences, some carriers have refused to permit subscribers to use SIM cards on other countries' networks without first having

undergone special credit checks. In the United States, carriers initially dealt with roaming frauds by blocking calls made to those countries most frequently called by offenders such as Columbia and the Dominican Republic. In France, network operators only permit international use of mobile telephones at the specific request of a subscriber, while in the United Kingdom, Cellnet only allows international use of mobile telephones to specified customers. Vodafone has a fraud prevention strategy of automatically routing high-cost international calls via operators who check upon the identity and credit rating of the caller, while Vodac, the service provider owned by Vodafone, has now introduced a system whereby the SIM card can only be used with the mobile telephone it was purchased with. Some have also argued that the SIM card system should be abolished and that all SIM data should be anchored in the circuit boards of mobile telephones (Purton 1994: 24). In Australia, Vodac, has produced a database of stolen mobile telephone IMEI numbers which enables stolen handsets to be identified prior to connection to the Vodafone network and insurance is offered to customers when they first purchase their mobile telephone (Anonymous 1996: 15). All of these strategies are aimed at carriers and service providers taking decisive action to protect themselves as well as their subscribers.

Electronic Funds Transfer Fraud

Financial institutions are able to adopt a wide variety of self-help strategies which may reduce the risk of electronic funds transfer fraud. Financial institutions need to ensure that in-house security procedures are adopted and that staff are checked for security breaches. Often, electronic fraud requires the involvement of confederates with inside knowledge of the institution's security and computer procedures.

Various procedures have also been adopted to ensure that plastic cards are not stolen and that PINs are communicated securely to customers. In Britain, for example, independent couriers were introduced to prevent mail interception of cards while it is now common to ask customers to collect their cards from a branch (Webb 1996: 24). Where the postal service is used, cards and PINs are sent separately. Banks are also able to assist merchants by notifying them of stolen cards and PINs. Again in Britain, a National Hot Card File was created by which details of lost and stolen cards were quickly transmitted to retail outlets.

One of the main strategies used to prevent EFTPOS fraud has been to lower floor limits (the transaction value at which authorisation is required from banks before the card can be accepted). This means that many more transactions now require bank approval than in the past. By 1996, it is planned that forty-five per cent of transactions will require bank approval.

Banks and card issuers may protect themselves against plastic card fraud in a variety of ways. Banks in Australia, for example, now have a centralised fraud reporting and investigation agency, Cardlink Services Limited, for plastic cards

which has close liaison with the police. Cardlink Services 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: 127).

Codes of conduct have often been used in the banking and credit industries to prevent fraud and to resolve disputes between institutions and customers. Codes have the dual function of acting as a form of education and publicity for both institutions and customers as well as providing a statement of recommended practice which may be relied upon to resolve individual disputes. Codes of conduct are, however, only going to be an appropriate regulatory mechanism where financial institutions or system operators are involved. If electronic money or stored value cards are used, then only the consumer and the merchant will be involved.

In Australia, the *Electronic Funds Transfer Code of Conduct* was introduced in 1989 and revised in 1990. All Australian suppliers of EFT have agreed to comply with the code which is limited to transactions involving an EFT plastic card and a PIN only (para. 1.1), thus excluding home banking. Paragraphs 5.2 to 5.4 of the code exempt the card holder from liability in respect of fraudulent or negligent conduct on the part of card issuers' employees or agents; forged, faulty, expired or cancelled cards; losses occurring prior to receipt of the card or PIN; unauthorised transactions occurring after notification; and losses resulting from unauthorised transactions where it is clear that the cardholder has not contributed to the losses. Paragraph 5.5 limits the cardholder's liability to A$50 or the balance of the account or the loss at the time of notification of loss or theft of the card. Paragraphs 5.7 to 5.9 deal with the cardholder's liability where loss or theft of a card is not notified or where the cardholder has not secured a PIN.

Another code which has relevance to electronic transactions involving banks is the *Code of Banking Practice* of November 1993. This code sets out the privacy requirements which banks are obliged to adhere to in dealing with customers and also specifies the various rights and duties of banks and customers.

These codes provide a wide range of rules which both institutions and users are required to adhere to in order to ensure that fraud is minimised and that disputes are fairly resolved.

4. Self-Help

Both individuals and organizations are able to take a range of positive steps to protect themselves against the three forms of telecommunications fraud described in this paper. The exercise of simple prudence based on an understanding of telecommunications systems will suffice in many cases although more sophisticated crime prevention advice and products are also provided by one of the world's growth industries of today, namely computer security. In addition to more rigorous management practices and the introduction

of more sophisticated password and verification procedures, new technologies such as biometric security devices and anomaly detection computer software help alert users to system weaknesses and enhance the security of computer systems themselves.

Citizens' groups can also be useful in detecting and reporting some forms of telecommunicatiions fraud. The Guardian Angels 'Cyber Angels' division recruits volunteers to patrol cyberspace in search of a range of illegal and objectionable content, including fraud schemes and software piracy. Information gathered from volunteers is then forwarded to law enforcement authorities.

Telemarketing Fraud

Some of the ways in which to avoid becoming a victim of telemarketing fraud include being wary of buying from telephone callers whom one doesn't know and always requesting a written description of the product in question and the terms of sale before entering into an agreement and transmitting funds. Consumers should withstand the seller's pressure for an immediate purchase or investment and, instead, conduct research with respect to the background of the caller. In case of investments or large purchases, it is wise to ask questions and seek information from a variety of sources. If solid information about the company and the investment are not available, one should think twice about the purchase.

One should also take extreme care in disclosing one's PIN or credit card number. There is some risk attached in divulging this information to any person or institution whose integrity may be in question. At present, communication over the telephone is relatively secure. The Internet, however, is much more vulnerable, although presumably encryption technology can soon be expected to improve security.

It is also possible to screen one's incoming calls with an answering machine, accepting those which one wants, and ignoring the remainder. This will provide some safeguard against high-pressure sales tactics. Silent telephone numbers provide some protection against unwanted callers, but do not protect against random dialling technology. Similarly, the disclosure of a silent number to a commercial organization may lead to its wider circulation. When one divulges one's telephone number in response to a newspaper advertisement or fills out a card asking for more information about an investment, or when one signs up for a contest or drawing, a phone number is usually requested.

Telephone Services Fraud

Users of telephone services are able to take many steps to detect illegality before it becomes a major problem or to avoid victimisation completely. Delaney (1993: 35.4) discusses various strategies aimed at preventing Private Automatic Branch Exchange (PABX) fraud, for example, including making the person

responsible for the system look for early warning signs, such as rapidly increased use, system slow-down due to excessive use, outgoing calls to foreign countries or unusual areas, and high off-hour utilisation. Similarly, Cook (1991: 176) suggests assigning one person to oversee the PABX system, daily monitoring of the system, limiting the number of people with access to the PABX long-distance code, changing the code frequently and checking for multiple failed attempts to gain access to the system.

In relation to cable television, Schieck (1995: 3-4) suggests that subscribers check billing records to ensure that they are being billed correctly, protect passwords and have different passwords for different levels of access, periodically change passwords, remove people from access to systems when they leave employment, conduct regular audits of services and educate suppliers, cable operators and the public as to the laws which apply and the problems of theft of cable services.

Electronic Funds Transfer Fraud

Most electronic payments systems require the use of a PIN or password in order for users to gain access. Protection of security numbers is, therefore, the primary crime prevention strategy.

Plastic card holders are best placed to protect themselves by taking basic security precautions to ensure that cards are not stolen. This includes not leaving them in public places unattended and ensuring that they are reclaimed after use. Consumers are also told not to compromise their security by disclosing PINs, keeping them with cards, or writing them on cards. Studies reveal, however, that between twenty and seventy per cent of people write their PIN on the card or on a piece of paper carried with the card (Sullivan 1987: 189, n. 19).

Where such strategies have been consistently implemented, substantial reductions in fraud have taken place. In Britain, for example, the use of a variety of strategies designed to prevent plastic card fraud resulted in a forty one per cent reduction in such fraud overall between 1991 and 1994, while losses occurring at retail points of sale were reduced by forty nine per cent during the same period. Losses from cards lost or stolen in the post were also reduced by sixty two per cent between 1991 and 1994 (Webb 1996: 24-5).

Frauds in which merchants are involved constitute a large problem for financial institutions as merchants are ideally placed to permit access to computer networks and to alter transaction details. Newton (1995) discusses various strategies to prevent merchant abuse in relation to plastic card fraud. On the other hand, merchants are well-placed to prevent frauds being committed by customers, such as by conducting random authorisation checks of bank account details, advertising the fact that steps are being taken to prevent fraud and ensuring that sales staff examine cards closely when they are being used (Bonney 1992: 6-8).

5. Co-Ordinated Law Enforcement

Given the substantial dark figure of telecommunications fraud, it is important to gather as much information on patterns and trends as can be made available. Encouraging victims to come forward with details of their experience is the obvious first step. Systematic sharing of information across jurisdictions is also important as many offences take place internationally. Communication and coordination between agencies is essential, especially when matters may be of interest to a variety of agencies, including police fraud investigators, companies and securities regulators and consumer affairs agencies. The necessity for co-ordination becomes particularly important in a federal system, where a variety of law enforcement and court systems exist.

In the United States, for example, the National Fraud Information Centre maintains a data base dedicated to telemarketing fraud which allows law-enforcement officials desk-top access to information about consumer complaints, ongoing investigations, and active or recent cases against alleged perpetrators of telemarketing fraud. Consumers can add their own complaints to this database, which is now available to nearly one hundred law-enforcement agencies as well as being on the Internet. The United States Securities and Exchange Commission also maintains a Web site (http://www.sec.gov/enforce/comctr.htm) and invites on-line reporting of incidents of suspected securities fraud.

Law enforcement as we have come to know it is inhibited by a range of fiscal, technological and extraterritorial considerations. Nevertheless, procedures and practices are being developed, and increasingly shared, for the investigation of telecommunications-related crime. Two examples of somewhat unconventional, undercover 'sting-type' operations carried out by the Federal Bureau of Investigation in an effort to thwart telemarketing fraud, are as follows.

In operation 'Senior Sentinel', a number of senior citizens were recruited by the FBI through the American Association of Returned Persons to record telephone calls made to them by fraudulent telemarketers. The recorded calls were catalogued and indexed, and provided evidence in an investigation which resulted in charges being made against more than one hundred suspects throughout the United States (Gembrowski and Dahlberg 1995).

Another FBI investigation imitated the techniques of telemarketing fraudsters by having agents pose as salespersons for automatic dialling equipment. As part of their 'trial service offer' the agents prevailed upon the fraudulent telemarketers in question to record their sales pitch. Subsequent 'field tests' of the pre-recorded message elicited calls from other FBI agents posing as consumers interested in the advertised product. These 'victim-agents', upon receipt of the products, were then able to testify about the false or deceptive representations recorded by the

telemarketers. The operation, code named ‘Disconnect’, was a coast-to-coast operation involving eighteen field offices and resulted in the arrest of over two hundred suspects (United States, Department of Justice, Federal Bureau of Investigation 1994).

The difficulties associated with mounting these and other operations to combat telecommunications fraud are such that conventional enforcement seems destined to be reserved for only the most serious breaches of the law.

To the extent that international telecommunications-related crime is amenable to international enforcement, it will require concerted international co-operation. Past performance in the context of other forms of criminality would suggest that this cooperation is unlikely to be forthcoming except in the relatively infrequent types of illegality where there is widespread international consensus about the activity in question, and about the desirability of suppressing it.

At the end of the day, those few offenders who commit offences with and / or against telecommunications systems and who are successfully prosecuted, tend not to receive penalties severe enough to discourage others from following in their footsteps. While the offenders in question might be personally chastened, the existing criminal process would appear not to deliver much in the way of general deterrence.

IV - CONCLUSIONS

International fraud of a more conventional nature has proved to be a very difficult challenge for law enforcement. Telecommunications-related fraud poses even greater challenges. There may be a lack of agreement about whether or not the activity in question is criminal at all, who has committed it, whether in fact it has been committed, who has been victimised because of it, who should investigate it and who should adjudicate and punish it.

There is a significant danger that premature regulatory interventions may not only fail to achieve their desired effect, but may also have a negative impact on the development of technology for the benefit of all. Over-regulation, or premature regulatory intervention may run the risk of chilling investment and innovation. Given the increasingly competitive nature of the global marketplace, governments may be forced to choose between paternalistic imperatives and those of commercial development and economic growth.

The challenge facing those who would minimise telecommunications fraud is to seek a balance which would allow a tolerable degree of illegality in return for creative exploitation of the technology. At this early stage of the technological revolution, it may be useful for individuals, interest groups and governments to articulate their preferences and let these serve as signals to the market. Markets may be able to provide more efficient solutions than state interventions.

The solution to telecommunications fraud will ultimately depend upon the adoption of a range of strategies both technological and strategic in which close cooperation will exist between all those involved in providing and using telecommunications systems. This includes telecommunications carriers and service providers, financial institutions, retail merchants and individual users.

Where weaknesses in security procedures became apparent, systems need to exist which will permit these weaknesses to be drawn to the attention of those most able to solve the problems effectively. In ensuring that particular weak points in security systems are identified and weaknesses solved, it is likely that technology will provide the most effective initial response, although technology is only as effective as those programming and using it.

*** Dr Russell G. Smith is a Research Analyst with the Australian Institute of Criminology, GPO Box 2944, Canberra, ACT, 2601. E:mail Russell.Smith@aic.gov.au**

ACKNOWLEDGMENTS

This research was funded in part by a grant from the Telstra Fund for Social and Policy Research in Telecommunications. The material in this paper on telemarketing fraud was kindly provided by Dr Peter Grabosky, Director of Research at the Australian Institute of Criminology. I also wish to acknowledge with thanks the assistance of Paul Wright, Greg Williams and Dennis Challinger.

REFERENCES

Adams, D. 1996, "Thieves Answer Call for Mobile Phones", *The Age*, 25 May, p. A3.

Anonymous 1993, "Phone Fraud Crack-Down Not Enough", *Mobile Asia-Pacific,* December, p. 15.

Anonymous 1995, "Russians Score Electronic Heist", *St Petersburg Times* 19 August 1995, p. E1.

Anonymous 1996, "Vodac's Database Latches on to Stolen Mobile Telephones", *Canberra Times*, 29 April, p. 15.

Australian Federal Police 1993, *Annual Report 1992-93*, AGPS, Canberra.

_____ 1994, *Annual Report 1993-94*, AGPS, Canberra.

Australian Payments System Council 1994, *Annual Report 1993-94*, Sydney, Reserve Bank of Australia.

_____ 1995, *Annual Report 1994-95*, Sydney, Reserve Bank of Australia.

Australian Telecommunications Authority (AUSTEL) 1995, *Telemarketing and the Protection of the Privacy of Individuals*, Australian Government Publishing Service, Canberra.

Bell Atlantic 1996, "Outfox Phone Fraud!!", Internet http://www.bell-atl.com/security/fraud/index.htm.

Bequai, A. 1987, *Technocrimes*, Lexington Books, Lexington.

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

Brooks, T. and Davis, M. 1994, "Are Your Phone Bills Fraud Free?", *Security Management*, vol. 38, no. 4, pp. 67-8.

Buckeridge, R. and Cutler, T. 1995, *The Online Economy: Maximising Australia's Opportunities from Networked Commerce*, Cutler and Co., Melbourne.

Cavazos, E. A. and Morin, G. 1994, *Cyberspace and the Law: Your Rights and Duties in the On-Line World*, The MIT Press, Cambridge.

Cellular One 1994, "Cellular Fraud Facts", paper presented at the *International Crime Stoppers Conference*, Hawaii, September. See also: Internet http://www.wireless101.com/new/fpf/fraud.htm

Commonwealth of Australia, Bureau of Consumer Affairs 1995, *A Cashless Society? Electronic Banking and the Consumer: Issues Paper No. 1*, Australian Government Publishing Service, Canberra.

Commonwealth of Australia, Human Rights and Equal Opportunity Commission 1995, *Smart Cards: Implications for Privacy*, Information Paper No. 4 of the Privacy Commissioner, AGPS, Canberra.

Cook, W. J. 1991, "Paying the Bill for Hostile Technology: PBX Fraud in 1991", *Computer Law and Security Report*, vol. 7, no. 4, pp. 174-7.

Coutorie, L. E. 1995, "The Future of High-Technology Crime: A Parallel Delphi Study", *Journal of Criminal Justice,* vol. 23, no. 1, pp. 13-27.

Crowe, D. 1996, "Wrong Numbers", *Financial Review,* 15 February, p. 16.

Delaney, D. P. 1993, “Investigating Telecommunications Fraud”, in Grau, J. J. (ed.), *Criminal and Civil Investigation Handbook*, 2nd ed., McGraw-Hill Inc., New York.

Denning, D. E. 1995, “Crime and Crypto on the Information Superhighway”, *Journal of Criminal Justice Education*, vol. 6, no. 2, pp. 323-36.

Flanagan, W. G. and McMenamin, B. 1992, “For Whom the Bells Toll”, *Forbes*, August 3, pp. 60-4.

Gembrowski, S. and Dahlberg, T. 1995, “Over 100 Here Indicted After Telemarketing Fraud Probe Around TheU.S.”, *The Source*, 8 December, Internet http://www.sddt.com/files/library/95headlines/DN95_12_08/DN95_12_08_02.html.

Harris, D. I. 1995, Interview with General Manager, Telstra Corporate Security, at Melbourne Head Office of Telstra, on 12 December 1995.

Holland, K. 1995, “Bank Fraud, The Old-Fashioned Way”, *Business Week*, 4 September, p. 88.

Jones, M. 1995, “A Code of Conduct”, *Internet Australasia*, vol. 1, no. 11, pp. 22-3.

Kennedy, D. 1996, “Russian Pleads Guilty to Stealing from Citibank Accounts”, Internet http://catless.ncl.ac.uk/Risks/17.61.html#subj

Kertz, C.L. and Burnette , L.B. 1992, “Telemarketing Tug-of-War: Balancing Telephone Information Technology and the First Amendment with Consumer Protection and Privacy”, *Syracuse Law Review*, vol. 43, pp.1029-72.

Levy, S. 1994, “E-Money (That’s What I Want)”, *Wired*, December, pp. 174-9, 213.

Mackrell, N. 1996, “Economic Consequences of Money Laundering”, in Graycar, A. and Grabosky, P. (eds.), *Money Laundering in the 21st Century: Risks and Countermeasures*, pp. 29-35, Australian Institute of Criminology, Canberra.

Main, A. and Stretton, R 1994, “Nigeria Calling”, *Australian Financial Review*, 1 August, p 47.

MasterCard 1996, “MasterCard Cash: A Canberra Success”, *Canberra Times*, 24 July, p. 32.

Masuda, B. 1993, "Credit Card Fraud Prevention: A Successful Retail Strategy", in Clarke, R. V. (ed.), *Crime Prevention Studies*, vol. 1, Criminal Justice Press, New York, pp. 121-34.

McCrae, P. 1996, "The Agony and the Ecstacy of E-Cash", *Australian*, 28 May, Computers p. 39.

Meijboom, A. P. 1988, "Problems Related to the Use of EFT and Teleshopping Systems by the Consumer", in Poullet, Y. and Vandenberghe, G. P. V. *Telebanking, Teleshopping and the Law*, Kluwer Law and Taxation Publishers, Deventer, pp. 23-32.

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.

Olson, B. 1994, "Phone Hacking", *Your Computer*, December, pp. 12-13.

O'Neill, J. 1996, "The Great Mobile Phone Rip-Off", *Independent Monthly*, April, pp. 20-5.

Pacific Bell (1996), "Pacific Bell LockOn: Toll Fraud Protection Services", Internet http://www.pacbell.com/products/LOCKON/lockon-3.htm

Purton, P. 1994, "Fraudsters Check Card Revolution", *The European*, 8-14 July, p. 24.

Ramirez, A. 1992, "Theft Through Cellular 'Clone' Calls", *New York Times*, 7 April: D1, D27.

Schieck, M. 1995, "Combating Fraud in Cable and Telecommunications", *IIC Communications Topics* No. 13, International Institute of Communications, London.

Sneddon, M. 1995, "A Review of the Electronic Funds Transfer Code of Conduct", *Journal of Banking and Finance Law and Practice*, vol. 6, no. 1, pp. 29-48.

Sulc, L. B. 1994, "Communicating Cellular Security Needs", *Security Management*, vol. 38, no. 4, pp. 63-5.

Sullivan, C. 1987, Unauthorised Automatic Teller Machine Transactions: Consequences 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 Kingdom, Industry and Government Study Group on Mobile Phone Fraud 1995, *Briefing Paper on Threats Posed by Mobile Phone Fraud and the Study Group's Subsidiary Recommendations*, Unpublished paper.

United Kingdom, Parliamentary Office of Science and Technology 1995, "Mobile telephone Crime", *Science in Parliament*, vol. 52, no. 6, pp. 27-30.

United States, Department of Justice, Federal Bureau of Investigation 1994, *Telemarketing Fraud*, Economic Crimes Unit, White-Collar Crimes Section, Criminal Investigation Division, Department of Justice, Washington.

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

Walters, D. and Wilkinson, W. 1994, "Wireless Fraud, Now and in the Future: A View of the Problems, Some Solutions", *Mobile Phone News*, 24 October, pp. 4-7.

Watts, K. 1995, "Crime and Carrier Punishment: Powers of Disconnection", *Australian Communications*, June, pp. 59-60.

Webb, B. "Preventing Plastic Card Fraud in the UK", *Security Journal*, vol. 7, pp. 23-5.

Young, T. H. 1995, "Wireless Bandits", *Police*, May, pp. 32-5.

Cases

Director of Public Prosecutions v Murdoch [1993] 1 VR 406 (Supreme Court of Victoria, 2 October 1992)

Kennison v Daire (High Court of Australia, 20 February 1986), (1986) 160 CLR 129.

R. v Baxter [1988] 1 Qd R 537 (Court of Criminal Appeal, Queensland, 3 July 1987)

R. v Evenett; ex parte Attorney General [1987] 2 Qd R 753 (Court of Criminal Appeal, Queensland, 3 April 1987)

R. v Liang and Li [1985] 82 A Crim R 39 (Court of Appeal, Victoria, 27 July 1995).

R. v Thompson [1984] 1 WLR 962 (Court of Appeal, Criminal Division: 22 March 1984).

Telstra Corporation Limited v Kendall [1994] 55 FCR 221 (Full Court, Federal Court of Australia, 31 January 1995).