International Association of Financial Crimes Investigators
10th Annual Conference "Plastic Card Fraud"
Sydney 20 May 2002
11.00 to 11.45

'Designing Appropriate Sanctions to Counteract Cross-border Plastic Card Fraud'

Russell G. Smith
Australian Institute of Criminology

1. Introduction

Plastic card fraud in the twenty-first century is no longer a domestic problem for financial institutions, merchants, consumers and law enforcement agencies but is now of global concern. Developments in payment systems enable transactions to be carried out with ease across borders and plastic cards are one of the primary means of gaining access to accounts regardless of where the customer is located. In Europe, for example, the relaxation of borders and the introduction of the Euro have led to a substantial increase in cross-border transactions, and associated fraud.

Similarly, developments in electronic commerce have meant that a much higher proportion of transactions are carried out without cards actually being present. By 2005, MasterCard International estimates that 52 per cent of its transactions will be carried out through remote services, rather than at point of sale (Lisker 2001). In Europe, the proportion of fraud on United Kingdom-issued plastic cards committed outside the United Kingdom, doubled during the 1990s and will soon amount to one third of all losses (Levi 2000). Fraudsters are clearly making use of the many new opportunities that have been created through the increase in international card-based transactions and the corresponding weaknesses in fraud control measures that they entail.

KPMGs latest Fraud Survey (2002), for example, noted an increase in the number of international criminals coming into Australia and New Zealand, committing major fraud and then leaving with the proceeds of their crimes. The report also found an increase in the involvement of criminal gangs in external fraudulent attacks on financial institutions through the use of stolen cheques and falsified identification documents. Of the 148 respondents with international operations, 23 per cent had experienced fraud in the preceding two years involving A$30 million. The most prevalent types of fraud within respondents' off-shore operations were credit card fraud and theft of inventory.

In the European Union, plastic card counterfeiting is estimated to cost EUR600 million or 0.07 per cent of industry turnover (Lakeman 2001), while much of the increase in plastic card fraud has related to card not present transactions conducted by telephone and the Internet.

Unlike crimes involving personal violence in which the offender and the victim have to be present together in one place at one time, economic criminals and their victims can be located anywhere in the world—and sometimes never meet in person. Occasionally, the offender and the victim may be located in one jurisdiction, but the mechanics of the commission of the offence may entail an international component, or involve confederates in a third country. This gives rise to various legal problems in determining exactly where the offence occurred, which country has jurisdiction to deal with it, as well as problems for financial crime investigators and police of locating offenders, obtaining evidence (often in foreign languages), and in seeking extradition of offenders.

It is also important to recall that there may be many different types of offenders involved in plastic card fraud. These include street robbers at the lowest level of organisational networks who steal cards; skilled offenders who have the technological expertise to skim, counterfeit, and alter cards; offenders who work within organisations who are able to steal account information for use by others; dishonest merchants who misuse customer account information; offenders who use counterfeit cards to withdraw cash or to obtain goods and services illegally; and those who control and organise the activities of other actors in the illegal pipeline. Each of these categories of offenders operates in slightly different ways, is subject to different motivations and will respond differently to legal sanctions that might be imposed. To speak of a singular category of plastic card fraudster is, therefore, inappropriate.

2. Rational Choice Offenders

The difficulties associated with prosecuting cross-border plastic card fraud are such that hard decisions have to be made about whether or not to embark on a prosecution in the first place. If relatively small sums are involved it may well not be cost-effective to expend further funds in investigating and in prosecuting the matter.

This raises the difficult problem of when it is appropriate to take criminal proceedings and whether the results obtained, in terms of conviction and punishment, warrant the costs involved.

In 1764, the Italian criminologist, Cesare Beccaria described the purposes of punishment as being 'to dissuade the criminal from doing fresh harm to his compatriots and to keep other people from doing the same' (Young 1986, p. 23). In any discussion of the effectiveness of punishment, it is important to distinguish between these two forms of deterrence, namely that which is directed at the individual offender (special deterrence) and that which applies to other members of the community (general deterrence).

The primary motivation of fraudsters now, as in Beccaria's time, remains the same, namely cupidity in obtaining money through unlawful means. The explanations offered also remain the same: greed in supporting a particular lifestyle, necessity in feeding an addiction to drugs or gambling, envy, or curiosity in seeing how far security systems can be compromised.

There is clear evidence that the courts and the community rely upon the imposition of criminal sanctions as being a deterrent to crime, both individually and generally (see Flanagan and Longmire 1996). Indeed, deterrence is legislatively specified as one of the purposes for which sentences may be imposed by courts in various jurisdictions (e.g. *Sentencing Act* 1991 (Vic.) s. 5(1)(a)), and is often relied upon by courts as a justification for imposing a sentence of imprisonment for serious offences (see Fox and Freiberg 1999).

In determining whether legal sanctions have any deterrent effect, consideration needs to be given to a number of factors. First, whether offenders are influenced by matters which are not directly relevant to their offending behaviour, such as the likelihood of detection, arrest and a particular punishment being imposed, secondly, whether offenders are, in fact, aware of the probability of detection, arrest and particular punishments being used or know of sentencing policies and practices generally, and thirdly, whether they are minded to act upon any such knowledge by modifying their behaviour or propensity to commit crime. Serious doubts have been expressed concerning each of these matters.

A large body of research has sought to test the so-called rational choice perspective of offending, namely, whether offenders weigh up in advance of committing crimes the positive and negative factors relevant to a course of criminal conduct, and then make a rational decision that seeks to maximise their net gains (see Clarke and Felson 1993).

An example of the kind of calculations that plastic card offenders might make when deciding to commit either plastic card fraud or armed robbery was described by John Newton who undertook an extensive study of organised plastic card counterfeiting in 1994.

> The attractions of plastic fraud to the criminal are clear. It is a low-risk, highly profitable venture. . . . There is no need to obtain firearms to commit the offence. There is little chance of being caught in the act and absolutely no chance of being shot by police, which is a hazard of committing an armed robbery in any country. . . . If criminals are caught it is difficult and costly to prove the case against them in court. If there is a suitable criminal offence in the country concerned . . . which is by no means certain, and criminals are convicted, the chances of them being sent to prison are about even. If they are sent to prison, their sentence will be substantially less than one they would receive for armed robbery (Newton 1995, p. 101).

The decision-making employed by offenders relates to all aspects of criminal justice processing—namely, whether their crime will be detected by investigators, whether they will be arrested, extradited, granted bail, required to undergo a jury trial, convicted, what sentence will be imposed, and how that sentence will be carried out, for example, in a maximum security city prison or in a low security country institution, and at what point parole will be obtained.

Offenders may also weigh up rationally the likelihood of other consequences of their wrongdoing occurring—namely, whether they will lose their job, lose professional registration, be barred from being a company director, be unable to obtain work on release from prison, be forced to sell their home, suffer marital problems, health problems, and loss of respect amongst family, friends, and peers.

Research into the rational-choice perspective of offending has, however, produced largely inconclusive findings. Surveys of offenders have sought to identify the matters taken into account at the time the crime was committed (see Cornish and Clarke 1986) while other studies have sought to assess the impact of sanctions on rates of recidivism (Weisburd and Waring 2001, p. 150). Both have found that offenders do not generally take the risk of punishment into account when deciding whether or not to commit crimes.

In Western Australia, for example, Harding (1990) surveyed 469 prisoners who were serving sentences for violent crimes and found that some knew of the penalties associated with using a firearm in a robbery and made a rational choice to carry out the offence nonetheless. Unfortunately, ninety-one per cent of offenders who carried a firearm in robberies said that they would carry a gun the next time they committed a robbery—thus providing little deterrent effect of imprisonment.

A study in the United States which examined the motivations of offenders who carried out serious property crimes, involved a survey of sixty offenders who were serving at least their second term of incarceration for offences such as burglary and armed robbery (Tunnell 1996). All sixty respondents in the study reported that they and nearly every thief they had ever known simply did not think about possible legal consequences of their actions. Although the offenders

knew that they were doing wrong and tried to avoid arrest, thirty-two did not know the penalty attaching to their act until after their arrest. Thirty-six of the respondents said that the possibility of incarceration was no threat to them and the remainder did not perceive it as being a great threat. Thus, incarceration could not be said to have acted as a deterrent to the majority of these serious repeat property offenders.

In a study of official re-offending rates amongst a sample of white collar offenders sentenced by federal courts in the United States, a similar finding was obtained, namely that imprisonment did not influence the likelihood of re-offending for those convicted of white collar crimes. Prison sentences did not have a specific deterrent effect on re-arrest whether in terms of the likelihood, timing, frequency or type of recidivism (Weisburd and Waring 2001, p. 113).

Some groups of offenders may be particularly unlikely to be influenced in their offending behaviour by the possibility either of detection or the threat of subsequent incarceration. For example, where crime is committed out of extreme need, under duress, through the influence of alcohol or drugs, or because of an addiction to gambling, it is unlikely that such offenders will have regard to the possibility of arrest and punishment when determining whether or not to carry out the crime in question (Fox and Freiberg 1999). For them, rational decision-making regarding the possibility and nature of punishment is unlikely to be present at the time of offending. It is, therefore, important to consider the individual circumstances of the offence and the offender when assessing any potential deterrent effects.

The extensive criminological research on the effects of deterrence is inconclusive regarding the influence which different types of sanctions have with respect to the prevention of crime. Even incapacitation (that is, removing offenders from the community by keeping them in detention) may be of little importance in reducing crime as others in the criminal community may simply take the place of those incarcerated (see Chan 1995, p. 10). The courts, legislators and the public, however, generally believe that the possibility of incarceration being imposed does act as a deterrent to crime. This is particularly the case with respect to general deterrent effects, although less so with respect to marginal deterrent effects, that is, the effect which increasing a penalty has on the likelihood that offenders will be deterred more effectively from committing that offence (Zimring and Hawkins 1973).

The Victorian Sentencing Committee, which conducted a thorough review of the research available at the time, arrived at the following conclusions with regard to the deterrent effect of increasing penalties (Victoria, Attorney-General's Department 1988, p. 77):

> It may be accepted on the basis of the available evidence and common sense that the existence of a penalty system in force through the criminal justice system will result in a general deterrent effect in the commission of crime. . . There is no evidence to support the proposition that there is any marginal deterrent effect in either increasing a specific penalty imposed on a given offender; [or] increasing by legislative means the general level of penalties applying for a given offence. . . There is no means of accurately assessing any marginal deterrent effect that may exist in given situations.

In the case of organised criminal activity, such as that involving cross-border plastic card fraud, rational choice may play a greater role than in other types of violent or property crime. Large scale counterfeiting operations require planning and consideration of the costs and benefits including the possibility of punishment being imposed. Organised criminals who embark upon cross-border crime, however, can be fairly certain that prosecution will be difficult and costly for

the authorities and thus, that they may well escape punishment. Some organised groups plan their activities carefully so that the risk of detection is low, that those responsible for organising operations are less likely to be arrested, and that prosecution will be difficult even if arrest does occur. They do this by moving operations regularly, changing *modus operandi*, making use of false identities, and perpetrating fraud on many occasions, each involving relatively small sums.

This somewhat pessimistic view about the effectiveness of criminal sanctions may lead to the conclusion that it unnecessary for victims to report crimes to the police at all. It is important to recall, however, that if crimes are not reported, not investigated and do not result in punishment, then any deterrent effects—however small—are likely to be diluted and those individuals who do rationally consider the consequences before offending, will be more likely to see the possibility of punishment as remote, and thus more likely to offend.

In order to prevent and to deter crimes of this nature, therefore, there is a need for as many cases as possible to be dealt with formally and for judicial outcomes and other consequences of wrongdoing to be widely publicised.

3. Jurisdiction Shopping

One consideration that rational-choice offenders may take into account in deciding whether or not to offend is the likelihood that they will be prosecuted. In the case of cross-border crimes where the offender is located in a different jurisdiction from the victim, a rational-choice offender may select a jurisdiction that will minimise the chances of prosecution.

Difficulties in investigation and prosecution can occur because of policies of bank secrecy in particular countries that make it difficult to obtain evidence from financial institutions, because mutual assistance arrangements do not exist between the countries in which the offender and victim are located, because of an unwillingness or inability on the part of police to investigate these types of crime, or the absence of extradition treaties with the country in which the offender is located when arrested. Other impediments to prosecution include the cost of sending law enforcement officers abroad to assist in an investigation, and the cost of bringing witnesses from abroad to testify in proceedings, which may both be prohibitive. There may also be problems of language, geographical distance, lack of knowledge of foreign legal systems, time differences, telecommunications and technological differences, and expense. These are all substantial impediments to embarking on a prosecution.

There may also be significant legal impediments which must be overcome. Some countries do not have laws that proscribe the possession of counterfeit cards or card embossing machines, and offenders may choose these countries in which to base their operations (Newton 1995, p. 38). Other offenders may continually move their operations in order to make detection difficult. The laws of evidence may also make evidence obtained in one country unable to be used in criminal proceedings in another country. These problems are not, however, new and international law has had to cope with the complexities of jurisdictional issues and conflicting substantive and procedural laws for hundreds of years in prosecutions involving sea piracy, slavery, hijacking, war crimes, and other offences that have an international component.

The result is that some offenders may be able to commit their crimes with relative impunity and be unable to be dealt with.

Those few fraudsters who think rationally about the consequences of offending could also target victims in countries that have the lowest maximum penalties for relevant offences or those in which sentencing practices result in comparatively low terms of imprisonment being imposed for the types of offences being contemplated.

In the field of money laundering, these notions have been clearly demonstrated with some nations being seen as safe jurisdictions in which to base criminal activities.

In the case of plastic card fraud, this is also likely to be the case, at least with respect to large scale, organised activities. Offenders in China, for example, where the death penalty exists for serious fraud offences, would clearly be well-advised to target victims in Australia where, in some states, they would receive a few years' imprisonment, or less, for offending, if they were able to be prosecuted at all.

The main responses to jurisdiction shopping by offenders are, first, sharing of information between law enforcement and regulatory agencies and, secondly, harmonisation of laws internationally.

In terms of cooperation between agencies, in July 2000, an important initiative began when the United States Federal Trade Commission (FTC) entered into an agreement with the Australian Competition and Consumer Commission to provide access to the FTCs *Consumer Sentinel* database of consumer complaints. This now permits regulators in the United States, Canada, and Australia to share information about consumer complaints and to assist each other in cross-border prosecutions—such as those involving Internet sales and on-line auctions.

Information networks within and between law enforcement agencies also need to be used, so that when an investigation begins, contact can be made immediately with the appropriate person in another country's corresponding department. Secure Intranets, such as that used by the Australian Bureau of Criminal Intelligence, are an excellent way in which this can be achieved. They can also be used to share 'Fraud Alert' information and to exchange intelligence needed in investigations.

Twenty-four hour response centres are now being established in many countries. These centres, which are to be used for genuine emergencies only, enable requests for real-time computer investigations to be handled at any time of the day or night in the participating country. In Australia, the Australian Federal Police handles such requests and refers queries to relevant state and territory police services of other Australian Federal Police regional offices (Geurts 2000).

In another initiative in the United States, the Federal Bureau of Investigation and the National White Collar Crime Centre have co-sponsored the establishment of a central repository for complaints relating to Internet fraud. The Internet Fraud Complaint Centre (IFCC) hopes to ensure that Internet fraud is able to be addressed at all levels of law enforcement (local, state, and federal).

The IFCC was created to identify, to track, and to investigate new fraudulent schemes on the Internet on a national and international level. IFCC personnel collect, analyse, evaluate, and disseminate Internet fraud complaints to the appropriate law enforcement agency. The IFCC provides a mechanism by which Internet fraud schemes are identified and addressed through a criminal investigative effort. The IFCC also provides analytical support, and aid in the development of training modules to address Internet fraud. The information obtained from the

data collected provide the foundation for the development of a national strategic plan to address Internet fraud.

In the European Union, Europol, which was created in 1998 and based in the Hague, is an information clearing house and analysis centre with law enforcement liaison officers in various member states. It aims to increase cooperation and communication between and among law enforcement agencies in member states rather than acting as a European police service (Sussmann 1999, p. 480).

In 1996, the G-8 countries established a group of experts ('The Lyon Group') to examine better ways in which to fight international crime. The Group produced forty recommendations that were endorsed by the G-8 heads of state at the Lyon Summit in June 1996. This group has met regularly and has discussed ways of enhancing the ability of law enforcement agencies to investigate and prosecute international crime. In January 1997 it created a sub-group to look specifically at high-technology crime and this sub-group has examined law reform, investigatory, and procedural issues to do with prosecuting cross-border computer crime (Sussmann 1999).

The G-8s High-Tech Crime Group, as it is known, has also recommended the establishment of cooperative arrangements between public sector police and regulatory agencies and the private sector. For example, there is a need for telecommunications carriers and ISPs to make certain information available to investigators on production of an appropriate search warrant. Ideally, such arrangements need to be uniform across jurisdictions.

One example of a cooperative venture involving public and private sector bodies is the Cybercrime Unit created by the International Chamber of Commerce's Commercial Crime Bureau in London in 1999. This brings together law enforcement bodies such as Interpol, Scotland Yard, and the FBI, as well organisations within the private sector including major financial institutions and businesses. The Unit acts as a clearinghouse for information on electronic crime and passes details of frauds and solutions between companies and the police.

Cooperative cross-border ventures to deal with money laundering have also been established. The International Money Laundering Information Network (http://www.imolin.org/organiza.htm) is an Internet-based network assisting governments, organisations and individuals in the fight against money laundering. IMoLIN has been developed with the cooperation of the world's leading anti-money laundering organisations that include the Commonwealth Secretariat, the Council of Europe, the Financial Action Task Force, Interpol, the United Nations Office for Drug Control and Crime Prevention's Global Program against Money Laundering, the European Commission, and others. The Egmont Group of the Financial Action Task Force also coordinates the activities of various Financial Intelligence Units globally.

4. International Conventions

Turning to the question of harmonisation of laws, we have also seen some important developments take place in recent years that are relevant to the prosecution of financial crimes.

International conventions need to deal not only with substantive laws relating to crimes of dishonesty, but also jurisdictional and procedural laws concerning mutual legal assistance. In particular laws concerning search and seizure need to be consistent and complementary internationally so that police can obtain evidence from other jurisdictions.

Law reform is, however, essentially a matter for each individual nation. As the Lord Chancellor, Lord Halsbury observed in 1891 in the case of *Macleod* v *Attorney-General of New South Wales* ([1891] AC 455, 458), 'all crime is local'. This does not mean, however, that parliaments should reform laws in total disregard of reforms introduced elsewhere. In the case of cross-border financial crime, all aspects of the judicial process would be facilitated if as much uniformity as possible were introduced in relevant laws. This would prevent jurisdiction shopping and would also enhance uniformity of sanctioning and reduce some of evidentiary difficulties that arise in proceedings.

Achieving uniformity of legislation is, however, neither simple nor quick. In a survey carried out by McConnell International (2000), the laws in 52 countries were examined. Of the countries surveyed, only thirteen (25%) had up-dated their laws relating to computer-related fraud (including Australia).

The creation of multilateral treaties is also not without problems. The Council of Europe's *Convention on Cybercrime* (2002) took almost five years to appear. It was adopted by the Committee of Ministers of the Council of Europe on 8 November 2001 and opened for signature on 23 November 2001 in Budapest.

The Convention is the first international treaty to address criminal law and procedural aspects of various types of criminal behaviour directed against
computer systems, networks, or data and other types of similar misuse. As such it provides a framework for international reform in this area.

Some of the articles in the Convention that are relevant to cross-border plastic card fraud include:

> Article 6—Misuse of devices
> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
> (a) the production, sale, procurement for use, import, distribution or otherwise making available of:
>
> > (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
> > (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
>
> (b) the possession of an item referred to in paragraphs (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
>
> Article 7—Computer-related forgery
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if

it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8—Computer-related fraud
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
(a) any input, alteration, deletion or suppression of computer data;
(b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

On 15 November 2000, another milestone was achieved with the adoption by the United Nations of the *Convention Against Transnational Organised Crime.* The Convention is intended to provide a legal framework for concerted action against organised crime, and the basis for the harmonisation of national legislation. It contains provisions requiring the criminalisation of certain conduct (including participation in an organised criminal group, money laundering and corruption), as well as provisions on corporate liability, special investigative techniques, witness and victim protection, cooperation between law enforcement authorities, exchange of information on organised crime, training and technical assistance, and prevention at the national and international levels. To date 141 countries have signed to Convention, including Australia which signed on 13 December 2000 at Palermo.

The Convention offers great potential for enhanced cooperation among countries with respect to implementation of anti-money laundering measures, confiscation of criminal assets, promotion of extradition and mutual legal assistance mechanisms, and the application of modern technology in the fight against crime.

It is important for as many countries as possible to ratify these conventions in order for safe havens for criminals to be removed and for prosecution and punishment of crime that takes place across jurisdictional borders to be enhanced.

Allied to the harmonisation of laws, is the need to harmonise other aspects of business practices in order to provide a global environment in which economic crime is difficult to perpetrate and yet simple to detect. Bodies such as the International Accounting Standards Committee (IASC), for example, help to promote uniform accounting practices and procedures within the business community that seek to reduce the risk of improper conduct being engaged in. Similarly, international professional bodies have a role to play in creating uniform ethical practices globally which militate against fraud (Braithwaite and Drahos 2000, p. 121).

5. Australia's Legislative Responses

In Australia, a package of measures was adopted in the later 1980s to facilitate the prosecution of organised crime and serious fraud. These included the *Mutual Assistance in Criminal Matters Act* 1987 (Cth) which established mechanisms to facilitate international cooperation between investigators with respect to obtaining evidence, the location of witnesses and suspects, the execution of search and seizure warrants, the service of documents, the forfeiture of property and recovery of fines and various other matters; the *Proceeds of Crime Act* 1987 (Cth) which enables investigators to follow the trail of the illegal proceeds of crime internationally and to confiscate

assets (with a new *Proceeds of Crime Bill* currently before Federal Parliament including civil forfeiture provisions); the *Financial Transaction Reports Act* 1988 (Cth), establishes a government agency to monitor the movement of large-scale cash transactions and regulates the manner in which accounts with financial institutions are created; the *Extradition Act* 1988 (Cth) which extended Australia's ability to enter into extradition arrangements internationally; and the *Telecommunications (Interception) Amendment Act* 1987 (Cth) which extended the ability of agencies to undertake electronic surveillance for law enforcement purposes; and the *National Crime Authority Act* 1984 (Cth) which created a law enforcement agency to deal with serious and organised crime.

At present in Australia each jurisdiction has its own laws and rules governing dishonesty. Examples include theft, obtaining a financial advantage by deception, making a false instrument, fraudulent misappropriation, obtaining money by false or misleading statements, obtaining credit by fraud, false pretences, fraudulent personation, forging and uttering, using a false instrument and many others. Many of these laws are complex, unclear and contradictory and impede the successful investigation and prosecution of fraud, particularly that which takes place across jurisdictional borders (see Lanham 1997).

The Commonwealth criminal law relating to economic crime has recently been amended by the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000* (Cth). Various offences are specified including the offence of obtaining property or a financial advantage by deception (Division 134) and certain other offences involving fraudulent conduct (Division 135). This legislation also amends the law governing geographical jurisdiction to facilitate the prosecution of cross-border criminal activity.

Legislation was enacted on 25 November 1999 to accommodate electronic transactions with the Commonwealth. The *Electronic Transactions Act* 1999 (Cth) provides broad, technology-neutral provisions which constitute a basis for more specific legal changes which will be introduced subsequently.

Although Australia is not a party to the European Convention on Cybercrime, it has enacted many of its articles in the form of the *Cybercrime Act* 2001 (Cth.) which was assented to on 1 October 2001 and commenced on 21 December 2001. This Act inserts a new Part relating to Computer Offences into the Commonwealth *Criminal Code Act* 1995 and provides model laws concerning a range of computer-related offences and jurisdiction that should address many of the problems that arise in prosecuting crimes of dishonesty committed electronically. The substantive offences in the *Cybercrime Act* 2001, however, only apply to situations in which a 'telecommunication system' or 'Commonwealth computer' is involved. Although limited in its Commonwealth focus, the Act significantly improves the scope for prosecuting cyber criminals by introducing substantive offences and procedural provisions consistent with those of the Convention. Whilst a significant improvement, there still remains some uncertainty in relation to the scope of a warrant; the ability to intercept e-mails prior to delivery; obtaining data not on premises; extra-territorial searches; and mutual assistance orders (see Ghosh 2002).

The advent of computer-related crime has meant that a number of countries are now enacting laws with extra-territorial effect—so as to permit prosecutions in respect of crimes and offenders located in some other jurisdiction as long as there is some connection with the country that enacted the law.

In terms of procedural reform, a number of improvements could be made. These include: taking early steps to ensure that evidence and facts are agreed and admitted wherever possible; streamlining interviewing procedures and using teleconferencing technologies for interviewing; using documentary evidence in preference to oral testimony wherever possible; overcoming the barriers to the use of computer-generated evidence; ensuring that evidence is not altered or destroyed before it is able to be obtained from another country; ensuring that police have access to the plain text version of encrypted files, either by requiring the suspect to disclose the encryption key, or by employing trusted third parties to hold copies of private encryption keys which can then be used by law enforcement on production of a warrant.

An additional problem is that the current multiplicity of rules makes difficult the task of effective communication of the content of those rules to business professionals and members of the public alike. As has been argued in England, reform of the substantive law regarding fraud 'could radically reduce the time and money spent on trials; increase successful prosecutions, thereby deterring many would-be fraudsters; and be a coherent foundation for preventive regulation' (Page 1997, p. 30).

6. Sanctions

In Australia, the following judicial punishments are currently available in most jurisdictions: fines; restitution and compensation orders; forfeiture and disqualification (confiscation); unsupervised release (suspended, deferred, conditional sentences); supervised release (probation, community service, intensive corrections) and custodial orders (either full time or periodic).

In other countries, more extreme sanctions exist such as mutilation and capital punishment. In Jiddah, Saudi Arabia, for example, in May 2000, the penal authorities beheaded seven Nigerians and cut off the right hands and left feet of three others who committed an armed bank robbery (Associated Press 2000). In China, people continue to be sentenced to death for a variety of non-violent economic crimes ranging from tax evasion and value added tax fraud, counterfeiting, embezzlement to credit card theft. For example, in March 1997, Wang Hua was given a death sentence with a two year reprieve for alleged credit card theft of US$62,650. In Yunnan province, on 24 December 1997, Yang Weixiang was executed for allegedly embezzling US$72,289 from the bank where he worked (see Amnesty International 1998).

I am not recommending that Australia should introduce the death penalty for credit card fraud, but it could explore alternative sanctions.

In addition to judicial punishments, there are other consequences of wrongdoing which may be invoked: adverse publicity; professional disciplinary sanctions; civil recovery action; injunctive orders and, most recently, various forms of reconciliation or community conferencing which are being evaluated at present.

Judicial punishments have been described as operating within an enforcement pyramid in which the most severe penalties, which are seldom used, sit at the top of the pyramid, whilst the least severe penalties, which are frequently used, fall near the base of the pyramid. Other non-judicial regulatory responses such as warnings form the base of the pyramid in that they are used most often (*see* Ayres & Braithwaite 1992, p. 35). The perceived severity of individual sanctions depends, however, upon the individual circumstances of the offender. Disqualification as a company director, may, for example, be a far more effective sanction to impose for dishonesty

than a severe fine. Similarly, adverse publicity can have profound effects in terms of shaming an offender in the community, perhaps more so than undertaking anonymous community service.

It has been argued that compliance with laws is best able to be achieved where the most severe forms of punishment, such as incarceration, are available but seldom used. In the words of Ayres and Braithwaite, 'the more sanctions can be kept in the background, the more regulation can be transacted through moral suasion, the more effective regulation will be' (1992, p. 19). The maximum penalties which attach to serious financial crimes already reflect the seriousness of such conduct with lengthy terms of imprisonment and substantial fines being available.

Little research has been carried out in Australia on the manner in which white collar offenders are dealt with following a criminal trial. In a study undertaken of a sample of fifty completed cases handled by the Major Fraud Group of the Victoria Police between January 1990 and October 1994, it was found that 68 per cent of offenders were sentenced to terms of imprisonment, usually less than five years, 14 per cent received good behaviour bonds, 11 per cent received suspended terms of imprisonment, 4 per cent were fined and 3 per cent received community-based orders (Krambia-Kapardis 2001, p. 100). These cases included, however, some of the most serious fraud offences prosecuted in Victoria.

It has been argued that white collar offenders tend to receive non-custodial sentences more often than custodial sentences owing to the fact that they are often first-time offenders, have cooperated with the police, have made financial restitution for their offences, may have suffered other consequences of their wrong-doing such as professional disqualification, and are invariably proficiently represented by senior legal practitioners who are able to describe their clients' mitigating circumstances in the most favourable light to the judge. Some, such as Alan Bond, were previously persons of high standing in the community.

Research supports the view that it is not the type of sentence which determines an offender's future criminal career, but rather various social and personal factors including access to employment and family and community support. Recidivism rates for offenders who have received community-based penalties, for example, do not significantly differ from recidivism rates for offenders who have experienced incarceration. Recidivism rates tend, however, to be higher for offenders who have been sentenced for more serious offences regardless of the type of sanction received, while offenders who have undergone community-based penalties suffer fewer adverse effects from the experience, which may cause them to re-offend, than offenders who have undergone incarceration.

It is widely known that increasing the certainty of detection through more effective and efficient policing has far greater deterrent effects than increasing the use of incarceration, or indeed other sanctions

Recent research has demonstrated, however, that it is not always necessary to impose the most severe sanctions in order to maximise deterrent effects. Weisburd and Waring (2001), for example, found that financial penalties deter future offending by white collar criminals far more than does imprisonment. The process of detection, investigation and arraignment for a white collar offender is likely to produce similar deterrent effects as is actually serving a term of imprisonment.

Arguably, more imaginative sanctions ought to be applied to financial offenders. Braithwaite (1992, p. 170), for example, describes the utility of using so-called 'equity fines' in which

companies are ordered to issue a certain proportion of new shares which are given to victims or to the state. For example, if a court ordered a corporate offender to issue one new share for every 100 already issued, the market value of all shareholdings would be reduced by 1 per cent. The company would still be able to operate although shareholders would be penalised. Other possible sanctions include corporate probation, adverse publicity and community service. These are all able to be used within the existing sanctioning structure, although require a little imagination by prosecutors and judges.

7. Conclusions

This paper has identified some of the problems associated with using the criminal justice system to deter cross-border plastic card fraud. Some problems are capable of resolution through continued international cooperative efforts of law makers, police and investigators. Others, such as the eradication of jurisdictional safe havens will take longer to achieve and will require concerted international effort.

In the short-term, it remains necessary for cases of serious fraud to be investigated and prosecuted and for successful judicial outcomes to be widely publicised. Only then will that small group of organised criminals who make decisions about where, when and how to offend on the basis of some rational calculation, gradually come to realise that the return on their investment in perpetrating this type of crime may not be as great as they once believed it to be.

Sanctions should, however, be applied appropriately. Often substantial terms of imprisonment may not be the most effective and efficient means of achieving deterrence. Applying alternative sanctions, including those that entail civil and financial consequences, may be a better way of reducing plastic card fraud than always seeking to impose the most severe penalty of incarceration.

In addition, rather than increase spending on the wider use of incarceration, prospective offenders would more effectively be deterred through increased efforts at fraud prevention and enhanced rates of detection and reporting of offences. Increased spending on law enforcement activities might first be directed at detecting crime quickly and with certainty, and publicising this fact. In addition, increased spending on education, training in business ethics, and fraud prevention initiatives would produce benefits in terms of reducing fraud to complement expenditure on the incarceration of individuals.

Plastic card fraud, and particularly those forms that involve an international component, need to be addressed using a range of strategies that extend from environmental measures that make crimes more difficult to commit to the use of judicial sanctions that seek to reduce the rewards derived from criminal conduct and to persuade those offenders who do make rational choices when deciding to offend, that the costs involved might, in fact, outweigh any benefits to be derived.

8. References

Amnesty International 1998, *People's Republic of China: The Death Penalty in 1997*, Amnesty International, New York.
http://www.amnestyusa.org/ailib/aireport/ar99/exit.cgi?http://www.amnesty.org/ailib/aipub/1998/ASA/31702898.htm (visited 19-4-02)

Associated Press, 2000, 'Saudi Arabia Beheads Seven Nigerians'.
http://cnn.com/2000/WORLD/meast/05/13/saudi.beheading.ap/index.html (visited 16 May 2000).

Ayres, I. & Braithwaite, J. 1992, *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press, New York.

Braithwaite, J. 1992, 'Penalties for White-Collar Crime', in *Complex Commercial Fraud*, Grabosky, P. N. (ed.), AIC Conference Proceedings No. 10, Australian Institute of Criminology, Canberra, pp. 167-71.

Braithwaite, J. and Drahos, P. 2000, *Global Business Regulation*, Cambridge University Press, Cambridge.

Chan, J. 1995, 'The Limits of Incapacitation as a Crime Control Strategy', *Contemporary Issues in Crime and Justice*, New South Wales Bureau of Crime Statistics and Research, no. 25.

Clarke, R. V. and Felson, M. 1993, 'Introduction: Criminology, Routine Activity, and Rational Choice', in Clarke, R. V. and Felson, M. 9eds.), *Routine Activity and Rational Choice'*, Advances in Criminological Theory, vol. 5, Transaction Publishers, New Brunswick, pp. 1-14.

Council of Europe (2002), *Convention on Cybercrime*, European Treaty Series No 185, Budapest, 23 November 2001, Council of Europe, Starsbourg (http://conventions.coe.int/treaty/EN/projets/projets.htm)

Cornish, D. B. and Clarke, R. V. (eds.) 1986, *The Reasoning Criminal: Rational Choice Perspectives on Offending*, Springer-Verlag, New York.

Fox, R. and Freiberg, A. 1999, *Sentencing: State and Federal Law in Victoria*, 2nd ed., Oxford University Press, Melbourne.

Geurts, J. 2000, 'The Role of the Australian Federal Police in the Investigation of High-Tech Crimes', *Platypus Magazine: The Journal of the Australian Federal Police*, March, http://www.afp.gov.au/publica/platypus/mar00/intfrd.htm (visited 5 February 2001).

Ghosh, A. 2002, 'The Cybercrime Act 2001: Implementing the European Union's Cybercrime Convention', Paper presented at the RSA Conference, San Jose, 16-22 February.

Harding, R. W. 1990, 'Rational-Choice Gun Use in Armed Robbery: The Likely Deterrent Effect on Gun Use of Mandatory Additional Imprisonment', *Criminal Law Forum*, vol. 1, no. 3, pp. 427-50.

KPMG 2002 *Fraud Survey*, KPMG Sydney.

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

Lanham, D. 1997, *Cross-border Criminal Law*, John Libbey & Co, Sydney.

Lakeman, P. 2001, 'Mechanisms for International Cooperation: Interpol's Universal Classification System for Counterfeit Payments Cards', in Broadhurst, R. G. (ed.), *Proceedings of the Asia Cyber Crime Summit*, Hong Kong, 25 -26 April, Centre for Criminology, University of Hong Kong.

Levi, M. 2000, 'The Prevention of Plastic and Cheque Fraud', A Briefing Paper Prepared for the Home Office Research, Development and Statistics Directorate, London.

Lisker, J. S. 2001, 'Electronic Commerce Fraud: Risk Assessment and Prevention', in Broadhurst, R. G. (ed.), *Proceedings of the Asia Cyber Crime Summit*, Hong Kong, 25 -26 April, Centre for Criminology, University of Hong Kong.

McConnell International 2000, 'Cybercrime and Punishment? Archaic Laws Threaten Global Information'. http://mcconnellinternational.com/services/CyberCrime.htm (visited 30 January 2001).

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

Page, F. 1997, 'Defining Fraud: An Argument in Favour of a General Offence of Fraud', *Journal of Financial Crime*, vol. 4, no. 4, pp. 287-308.

Sussmann, M. A. 1999, 'The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium', *Duke Journal of Comparative and International Law*, vol. 9, no. 2, pp. 451-89.

Tunnell, K. D. 1996, 'Let's Do It: Deciding to Commit Crime', in Conklin, J. E. (ed.), *New Perspectives in Criminology*, pp. 246-58, Allyn and Bacon, Boston.

United Nations 2000, *Convention Against Transnational Organised Crime*, Document: A/55/383, United Nations, Palermo. http://www.odccp.org/palermo/convmain.html

Victoria, Attorney-General's Department 1988, *Report of the Victorian Sentencing Committee*, Government Printer, Melbourne.

Weisburd, D. and Waring, E. 2001, *White Collar Crime and Criminal Careers*, Cambridge University Press, New York.

Young, D. 1986, Translation of Beccaria's *On Crime and Punishments*, Hackett Publishing Co., Indianapolis.

Zimring, F. E. and Hawkins, G. J. 1973, *Deterrence: The Legal Threat in Crime Control*, University of Chicago Press, Chicago.