AUSTRALIAN INSTITUTE OF CRIMINOLOGY

INTERNET-RELATED FRAUD: CRISIS OR BEAT-UP?

Dr Russell G Smith
Australian Institute of Criminology

Paper presented at the
4th National Outlook Symposium on Crime in Australia,
New Crimes or New Responses
convened by the Australian Institute of Criminology
and held in Canberra 21-22 June 2001

Introduction

The increased use of the Internet over the preceding decade has created considerable apprehension in the international community that it is being used to perpetrate various forms of fraud and economic crime. Fears that the Internet has become an insecure environment in which to transact business have been widely discussed in the public media and the academic community alike and may have retarded the development of on-line commerce. It has also been argued that traditional legal responses to Internet-related fraud are both ineffective and inappropriate to deal with such an international phenomenon. But have these views distorted the true position?

This paper evaluates the currently-available evidence to support the proposition that Internet-related fraud has reached crisis point; and the opposing evidence that demonstrates that the problem has been greatly exaggerated and over-emphasised in public discourse. The evidence will be discussed from three perspectives: empirical and statistical studies; how the law and law enforcement agencies have coped; and whether a crisis exists from the victim's point of view.

Some reasons are advanced for the posited distortions in the representation of Internet-related fraud and some ideas offered as to how the problem may be discussed more objectively and moderately in the future. To begin, however, we need to define some key concepts and terms.

Internet-Related Fraud

For present purposes, Internet-related fraud shall be taken to mean any dishonest activity that involves the Internet as the target or means of obtaining some financial reward. Consumer fraud relating to the Internet primarily takes place when goods and services are advertised on Web sites and the consumer is not provided with the product purchased. In this sense, Internet-related fraud is similar to traditional forms of misleading and deceptive conduct in the terrestrial marketplace. The only difference is the widespread extent which the dissemination of information can take.

One area of growing concern relates to the provision of Internet services. As consumers continue to increase their use of the Internet, so the number of complaints about Internet Service Providers (ISP) has also increased. In Australia, for example, complaints to the Australian Competition and Consumer Commission have included allegations of overbilling, inadequate detail when billing, failure to supply technical support and other services as represented, failure to connect consumers to the Internet as agreed, not honouring requests to disconnect, the need to have a credit card to obtain services, attempts to avoid consumers' legal rights and misrepresentations about the speed of Internet access and the experience of the Service Provider (ACCC 1999). In the United States a particular problem being investigated by the Federal Trade Commission has involved allegations of failure to disclose the terms of free trial offers when offering on-line services (Starek and Rozell 1997 pp. 692). This is usually dealt with as breach of contract, although criminal fraud may also be involved.

A related problem arises where a person visits a Web site that manipulates the telephone billing system and results in large international calls being billed. One case involved a company which advertised 'free' erotic photographs on the Internet. In order to see the images, the user was required to download software which, once installed, took control of the user's modem, cut off the local ISP, and dialled a number in the former Soviet Republic of Moldova in Eastern Europe. The line remained open until the computer was turned off resulting in the user incurring large international telephone charges which were shared between the fraudster and the Moldovian telecommunications company. The fraud was detected through regular surveillance of customers' telephone accounts and the Federal Trade Commission was able to obtain an order requiring the defendants to place US$1 million in an escrow account pending resolution of the case (*Federal Trade Commission* v *Audiotex Connection Inc* E.D.N.Y. Filed 13 February 1997).

Dishonesty can also arise in connection with payment systems (see Smith 1999). Here, the most profound problems are said to occur when one pays for goods and services by disclosing one's bank account details and other personal information to a merchant, who may then choose to use the information for unauthorised purposes.

Consumers can also be the perpetrators of fraud. As with other types of telecommunications, it is possible to steal Internet-related services by entering into a contract with an ISP and a telephone carrier, and then failing to pay for the services provided. Consumers are also able to defraud merchants by entering into commercial transactions, obtaining the goods and services in question, and then defaulting on payment. Making use of a false identity or using someone else's bank account are the usual means of carrying out such conduct.

Fraud involving on-line commerce may also take place between business entities themselves, such as wholesalers and importers, and between government agencies and members of the public, such as where publicly-funded benefits are provided to receipients after on-line claims have been made.

Finally, in the realm of business and government activities, unauthorised use of the Internet itself could be described as fraud with losses occurring in respect of loss of time and productivity. In a number of widely-reported cases, employees have been disciplined or dismissed for using workplace computers inappropriately. In New Zealand, for example, four employees of the Department of Child, Youth and Family Services were dismissed for inappropriate use of the Internet which included gaining access to pornographic material (Anonymous 2000).

The Meaning of Crisis

A crisis is a time of acute danger or suspense. In critical care in hospitals, for example, patients are catered for who face imminent danger of death or whose illnesses have reached a decisive moment in which more intensive forms of therapy are required than previously. To have reached crisis point, there has generally been a progression from bad to worse with innovative and intensive responses being required.

In the on-line world, a crisis could be said to have occurred when one's computer stops working. This could take place through an interruption of the power supply, or because a malicious code such as a virus or worm has interfered with the proper functioning of the computer. A crisis in Internet fraud could also be seen to arise when a user receives a bill for thousands of dollars that relates to unordered goods or services obtained fraudulently by someone else on-line. If we are to believe the media, then such dishonesty is rife on the Internet.

The Meaning of Beat-Up

In British country life, if one speaks of a beat-up this will usually describe the activities of farm workers going about the countryside seeking to rouse game by creating a noise. In the media, a beat-up is a news story whose prominence and importance greatly exceeds the available supporting evidence. For the purposes of our discussion, the characterisation of Internet fraud as a beat-up simply means that it has been exaggerated far beyond any material available to justify the problem.

Interested Parties

Who, then, is responsible for beating-up the notion of Internet fraud, and what benefit is to be derived from distorting the seriousness of the problem? There are groups within society who stand to benefit considerably from propagating each of these perspectives and it is as well to be aware of their interests in order to evaluate the objectivity of the positions they espouse.

The Media

The first group with an interest in describing Internet fraud as being at crisis point and responses to it as out of control, are those in the news and entertainment media. Successful news copy invariably emphasises the seriousness of crime, both economically and in terms of its frequency of occurrence. Stories about new technologies also attract attention, and so the combined impact of reports describing the ever-expanding problem of Internet fraud invariably makes profit for media corporations. Although some sections of the media have focussed on the 'good news' stories of Internet payment system security achievements, the war stories of individuals losing fortunes on the Internet continue to attract attention.

Criminal Justice Personnel

Critics of the police have often raised the possibility of police manipulating statistics and reports of their work in order to paint a devastating picture of the seriousness of the crime problem—merely in order to justify their existence and to increase public funding for their work. An Internet fraud crisis, of course, has the direct consequence that funding for specialist crime squads is likely to be increased—although this seems not to have occurred to any great extent to date. This could, of course, reflect the absence of a crisis—at least in the eyes of politicians and those responsible for allocating funds. Alternatively, it could indicate entrenched neglect of funding for police services, particularly in the area of sophisticated crime.

Governments

Governments, too, have an interest in emphasising the problems associated with the Internet, as they can then offer solutions and receive kudos for solving an intractable problem. On the one hand, it is possible for politicians to deflect attention away from other more pressing issues, such as drug and violent crime problems, by focusing on the extent of Internet fraud. On the other hand, governments which seek to enhance on-line procurement and electronic commerce, such as the payment of benefits on-line, have a keen interest in ensuring that the problem of Internet fraud is not overstated. In 2000, for example, the National Office for the Information Economy in conjunction with the Australian Computer Society (2000), published a Report entitled *The Phantom Menace: Setting the Record Straight About On-Line Credit Card Fraud for Consumers* in which facts favourable to the proposition that Internet shopping was safe for consumers were outlined and explained.

Computer Security Industry

Those in the computer security industry who manufacture devices such as encryption software and biometric user authentication systems (for example, fingerprint scanners attached to keyboards or iris scanners on computer monitors), have much to gain from representations of Internet fraud being more serious than it actually is. One of the growth industries for the twenty-first century will be computer security and the more people that are concerned about security, the more products will be sold. An example of the marketing potential of computer security was the Year 2000 problem in which the global cost of avoiding the problem was estimated to be US$920 billion according to the Gartner group. In Australia alone, A$12 billion was spent on the Year 2000 problem and its solutions—where the only reported incidents seemed to be the failure of ticket machines on some buses in Tasmania and South Australia (Gettler 2000). The precautions adopted may, however, have been effective in preventing other more profound consequences.

On the other hand, those who manufacture computer hardware and software have an interest in ensuring that Internet fraud is not overstated as fear of victimisation may lead to a reduction in Internet usage and thus to a loss of sales. Individuals who may be called on-line zealots also have much to gain from ensuring that the public feel safe and secure when using digital technologies.

Digital Luddites

Another group could be described as Digital Luddites—namely, those who eschew modern technological developments and who favour more traditional means of communicating and living. Clearly, if Internet fraud is seen as being problematic, this improves the position of those who have refrained from using new technologies. In particular, where individuals have refrained from conducting transactions on-line through fear of being defrauded, the assertion that such crime has, in fact, taken place, vindicates their position exactly.

Fraudsters

Finally, potential fraudsters may seek to derive a benefit from the risks of Internet fraud being under-estimated. If members of the public continue to use the Internet regardless of the risks, and are complacent concerning on-line security, then Internet fraud may be all that easier to commit.

The Evidence

Empirical Evidence - Crisis

The statistical information that we have on Internet fraud comes mainly from victimisation surveys carried out in the business community, and extrapolated estimates of loss by business analysts. Police statistics in this field are generally not specific enough to permit an analysis of the means by which fraud occurs, such as through the use of the Internet.

Over the last few years, business victimisation studies have found increased levels of concern amongst those surveyed about the risk of Internet-related fraud as well as actual levels of victimisation.

The latest international fraud victimisation survey conducted by Ernst and Young in October 1999, surveyed 10,000 senior executives in major organisations in fifteen countries, of whom 739 replied (Ernst and Young 2000). Although the response rate of seven per cent was exceedingly low, thus making the findings of limited generalisability, some indications of the seriousness of Internet fraud were apparent. Four out of ten respondents considered that unauthorised or improper use of the Internet constitutes computer fraud, although almost two thirds of those from high-technology organisations considered misuse of the Internet to be fraud. Eighty-two percent of these high-technology industry respondents thought that Internet fraud was likely or very likely to occur within their organisation.

In the United States, the newly established Internet Fraud Complaint Centre—organised by the United States Department of Justice and the Federal Bureau of Investigation (2001)—received 19,490 complaints relating to Internet fraud from the time of its establishment on 8 May 2000 and 30 November 2000. The average monetary loss per complaint was US$665.00 with 49 per cent of complaints relating to auction fraud. Complaints were received from 106 countries, most coming from the United States, Canada, Australia, and the United Kingdom. This could, of course, merely be indicative of countries with the highest Internet usage.

Various government agencies also monitor Internet-related fraud. In 1999, Internet Fraud Watch reported an estimated 2 million instances of credit card fraud taking place with respect to on-line purchases in Europe, with a 600% increase in Internet fraud complaints occurring in the United States since 1997 (Philippsohn 2000).

In the United States, over 18,600 complaints were registered on the Federal Trade Commission's fraud database 'Consumer Sentinel' in 1999, more than double the number in 1998—when 8,000 were registered (United States, Department of Justice 2000).

In a telephone survey of 1,006 on-line consumers conducted for the National Consumers League in the United States between April and May 1999, twenty-four per cent said they had purchased goods and services on-line. Seven per cent, which represents six million people, however, said that they had experienced fraud or unauthorised use of credit card or personal information on-line (Louis Harris and Associates Inc 1999).

Finally, in a worldwide clean-up operation of the Internet, involving the Office of Fair Trading in Britain and its counterparts in twenty-two other countries, 1,159 potential 'get rich quick' schemes were found being advertised on Internet sites (Office of Fair Trading 1998).

Empirical Evidence - Beat-Up

Although some of these figures are indeed disturbing, they need to be placed in context. It has been estimated, for example, that some US$2.85 trillion is obtained each year from organised criminal activities such as trafficking in drugs, guns, and people, illegal gambling, fraud, embezzlement, extortion, and other criminal enterprises (Walker 1999). Thus, the losses attributable to Internet fraud are of less significance that when considered in isolation.

The increase in Internet fraud also needs to be considered in light of the substantial increase in usage of the Internet. Internet usage surveys carried out by the Australian Bureau of Statistics (1998, 1999, 2000), for example, have found an increase of fifty-two per cent in the number of adults in Australia who had gained access to the Internet between November 1998 and May 2000—4.2 million adults (31 per cent of the adult population) to 6.4 million adults (46 per cent of the adult population).

The surveys also found a 180 per cent increase in the number of adults who had used the Internet to purchase or order goods or services for their own private use between November 1998 and May 2000—(286,000 or 2.6 per cent of adults in the twelve months to November 1998 to 802,000 adults (6 per cent of Australian adults) in the 12 months to May 2000 (a 2.4 per cent increase in the percentage of the adult population). The percentage of Internet shoppers who paid for goods and services by disclosing their credit card details on-line, increased only minimally from 80.5 per cent in November 1998 to 81 per cent in May 2000.

In addition, many of the problems associated with Internet fraud relate only to a relatively small proportion of the world's population. Even in Australia, only six per cent of the population used the Internet to purchase goods or services on-line last year.

In terms of electronic funds transfers, the statistics complied by the Australian Securities and Investments Commission (2000) on the operation of the Electronic Funds Transfer Code of Conduct show that there has been an increase from 42 to 64 complaints made under the Code per million transactions between 1998-99 and 1999-2000. In 1999-2000, there were 106,719 complaints out of 1,655,362,481 electronic transactions. In percentage terms, this represents a very small number indeed.

Finally, a number of the surveys that have been conducted cannot be said to have examined the incidence of Internet fraud objectively. Some have used clearly leading questions when asking respondents about their experiences. Others have been overly general in seeking information—often not even defining or explaining what Internet fraud actually means. For example, the National Consumers League in the United States found that American consumers lost US$3.2 million to on-line scams in 1999 alone. However, 97 per cent of cases involved consumers paying for goods using cheques and money orders, making the on-line component of the fraud simply the fact that the goods were advertised electronically (National Office for the Information Economy and the Australian Computer Society 2000). In essence, these were no more than traditional cases of cheque or money order fraud.

Legal Issues and Law Enforcement - Crisis

If we look at Internet fraud from the perspectives of the law and policing, there is, indeed, some evidence of a crisis, rather than a beat-up.

In terms of the law itself, a number of problems have emerged which have created difficulties for the successful prosecution of Internet fraud. Their nature has sometimes been remarkably simple, however, such as the omission of laws that proscribe deception of computers as opposed to human actors, thus making ATM-related fraud sometimes difficult to prosecute (*Kennison* v *Daire* (1986) 160 CLR 129, High Court of Australia, 20 February 1986).

As these problems grew, a variety of solutions was adopted. This has created problems itself as laws are now variable and conflicting across different jurisdictions. Many countries have also not reformed their laws. McConnell International (2000), for example, recently carried out a survey of laws in 52 countries and found that thirty-three of the countries surveyed had not yet updated their laws to address any type of computer crime. Of the remaining countries, nine had enacted legislation to address five or fewer types of computer crime, and ten had updated their laws to prosecute six or more of the ten types of computer crime identified.

Many law enforcement agencies have reported increased instances of Internet-related crime being reported to them for investigation. Although not all computer crime cases referred to the Australian Federal Police involved Internet fraud, over the last ten years the computer crime case load has increased substantially as we can see from Figure 1 (see Geurts 2000).

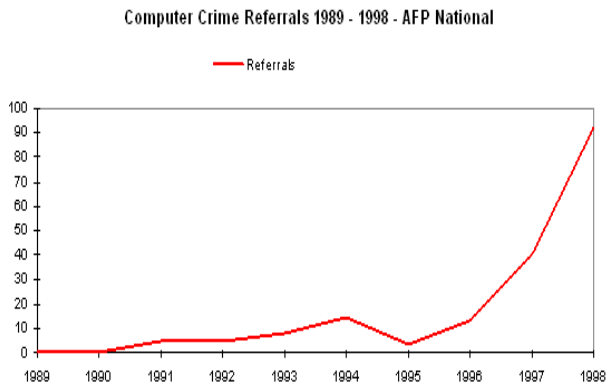

Figure 1
Computer Crime Referrals 1989-1998 - AFP National
Source: Geurts 2000.

Law enforcement agencies have generally found the investigation of such cases to be costly, slow, and difficult. There have been relatively few successful prosecutions and sentences have tended to be in the lower range of severity for white collar offences. Police computer crime squads tend to be composed of interested amateurs who acquire considerable experience and expertise during the course of investigations. Often their skills are recognised by the private sector to which they invariably gravitate in the pursuit of more remunerative positions.

The crisis, in the policing Internet fraud, however, lies not so much in the difficulty of investigation, but in the acquisition and retention of sufficient personnel to undertake the work. Unlike some other police services, the Australian Federal Police has had some success in retaining computer forensic specialist officers through the use of flexible remuneration policies, opportunities for ongoing professional development, and access to new and updated equipment (Australian Federal Police 2000, p. 19).

Finally, considerable problems have arisen in the investigation of Internet fraud that involves cross-border activities. Even if evidence is able to be adduced, problems of locating and extraditing an accused person from other jurisdictions remain. This adds considerably to the cost of law enforcement and delays the completion of matters.

Legal Issues and Law Enforcement - Beat-Up

Although much has been written about the inadequacy of the law to deal with Internet-related fraud, a good deal has already been achieved. The commonwealth government, for example, has introduced the *Electronic Transactions Act* 1999 to facilitate electronic delivery of services by government and the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act* 2000 (Cth No. 137) has also begun the process of harmonisation of dishonesty offences throughout Australia which will greatly facilitate prosecutions in this area. Similarly, a Discussion Paper on the reform of computer-damage offences and questions of jurisdiction (Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2000) represents an important development in legal reform in the area of on-line crime.

Internationally, the Council of Europe's *Draft Convention on Cybercrime* (2000) and the G-8 Countries' High-Tech Crime Group established in 1996 (Sussmann 1999), are two examples of significant achievements in this area.

Although the process of law reform relating to Internet fraud has been slow, it is, arguably, quicker than in other areas of law—notably corporations and taxation law. Many of the legal issues concerning Internet fraud involve wider issues of relevance to other types of cross-border crime—particularly those that involve economic offending. The seriousness of the Internet fraud law reform problem is, therefore, not substantially different from other areas of international law.

The problem of Internet fraud for law enforcement agencies also needs to be placed in context. Although Internet-related crime investigations often involve voluminous information and data trails, so do other crimes. The prosecution of Martin Bryant following the Port Arthur shooting, for example, involved 1,200 witnesses, more than 2,000 relevant reports, more than 2,700 photographs, and a further 2,000 exhibits (Fife-Yeomans 1998).

In fact, the investigation of Internet-related crime is facilitated precisely because information is recorded digitally. Police are able to search extensive databases and compile computer-generated models to assist with investigations. Often digital data trails are easier to follow and more apparent than paper trails of evidence.

There are also now numerous international arrangements in place relating to mutual assistance designed to help law enforcement deal with cross-border investigations. Although these are often slow and costly, the difficulties are not essentially any different in the case of Internet fraud than in the case of other cross-border prosecutions involving international crime. Police and prosecutors have had to deal with international criminals for hundreds of years in cases involving piracy, illegal immigration, drug trafficking, and smuggling, not to mention serious fraud.

Victims - Crisis

Although well-publicised media reports of Internet fraud could be said to have beaten-up the problem unduly, many individuals have suffered severe consequences—and from their perspective, at least, the problem is of critical concern.

Individuals have lost substantial sums through on-line scams and some businesses have been crippled through external denial of service attacks or through intellectual property infringements (Grabosky and Smith 1998, Grabosky, Smith and Dempsey 2001). According to the *Straits Times* (8 November 1999), for example, a copy of the recent James Bond Film *The World is Not Enough*, was available free on the Internet before its official release, representing a serious loss of potential revenue.

In one Australian case, a 27 year old male, known as 'Optik Surfer', who had been working as a computer networking consultant, was refused employment with an ISP in January 1994. In March 1994, he took revenge by illegally obtaining access to the company's computer network using the user account and password of the company's technical director. He then gained access to the company's database of 1,225 subscribers and publicised their credit card account details by disclosing them to various journalists and also by altering the company's Home Page on 17 April 1994 by including a message that the company's security system had been compromised. The publicity resulted in the company losing more than $A2 million in lost clients and contracts. It was required to change its business name and sold the Internet access part of its business to another ISP. The ofender was sentenced to three years' imprisonment (with 18 months' suspended) on 27 March 1998 (R. v *Stevens* Unreported decision of the New South Wales District Court, 27 March 1998; appeal to the New South Wales Criminal Court of Appeal dismissed [1999] NSWCCA 69).

Victims - Beat-Up

Proportionally, however, the instances of Internet fraud that have affected individual victims have been relatively few, particularly in view of the extensive use made of the Internet and electronic funds transfers between financial institutions and customers.

In addition, many of the problems of Internet fraud are not essentially new. Take the case of the manipulation of sharemarkets through the use of new technologies. In 1867, for example, a Wall Street stock broker collaborated with Western Union telegraph operators to counterfeit messages which reported bankruptcies and other financial disasters supposedly befalling companies whose stock was traded on the New York Stock Exchange. When the share prices were driven down, the wiretappers then purchased their victims' stock (O'Toole 1978, p. 97).

Last year, much the same strategy was employed by a 24 year old man who lived in a Melbourne suburb who manipulated the share price of an American company by posting information on the Internet and sending E-mail messages around the globe that contained false and misleading information about the company.

On 8 and 9 May 1999, he posted messages on Internet Bulletin Boards in the United States and sent more than four million unsolicited E-mail messages, colloquially referred to as spam, to recipients in the United States, Australia and in other parts of the world. The messages contained a statement that share value of the company would increase from the then current price of US$0.33 to US$3.00 once pending patents were released by the company, and that the price would increase up to 900 per cent within the next few months. The effect of the information was that the company's share price on the NASDAQ doubled, with trading volume increasing by more than ten times the previous month's average trading volume. The offender had purchased 65,500 shares in the company through a stock broking firm in Canada several days before he transmitted the information. He sold the shares on the first trading day after the transmission of the information and realised a profit of approximately A$17,000.

The Australian Securities and Investments Commission prosecuted the offender for distributing false and misleading information with the intention of inducing investors to purchase the company's stock. He pleaded guilty and was sentenced to two years' imprisonment on each of three counts, to be served concurrently. The Court ordered that 21 months of the sentence be suspended upon his entering into a two-year good behaviour bond with a surety of $500 (*Australian Securities and Investments Commission* v *Steven George Hourmouzis*, Unreported decision of the County Court of Victoria, 30 October 2000, Stott J).

Arguably, then, the Internet merely enables traditional forms of crime to be carried out more extensively than in the past, and although the methodology may be novel, the ultimate objective is well known.

Conclusions

On the basis of the evidence considered and the arguments canvassed, it may be concluded that some aspects of Internet fraud represent a serious problem—although arguably not yet in the category of 'crisis'—while other matters have been unnecessarily characterised as problematic.

Statistics

In terms of the empirical data available, Internet fraud is of no greater concern than other types of economic crime—although it needs to be stressed that our knowledge base is at present, seriously deficient.

Legal Issues and Law Enforcement

So far as the law is concerned, we have seen that a number of the problems that have arisen in proscribing objectionable on-line conduct have been overcome—although novel uses of the Internet are creating new problems all the time. Some effective and adaptable models have been proposed and tried for dealing with Internet fraud throughout the 1990s and arguably the legal problems that exist at present are not insurmountable.

From a law enforcement perspective, Internet fraud has created definite problems, mainly to do with the trans-jurisdictional nature of many on-line scams and the difficulties associated with investigation and prosecution in multiple jurisdictions. Levels of expertise and funding within law enforcement agencies are also inadequate to deal with many instances of Internet fraud and in some areas could be described as being in a state of crisis.

Victims

From a victim's point of view, Internet fraud is certainly a serious problem. Substantial losses may be suffered with little or no chance of recovery as offenders may be located in overseas jurisdictions, or may simply be unable to be located at all. The number of victims suffering at the hands of on-line criminals, however, is relatively small, making the impact of the problem in the community as a whole of medium importance only.

As we have seen, there are those who stand to benefit both from the depiction of Internet fraud as being in a state of crisis as well as being of less seriousness and a beat-up. It is important to implement change carefully and deliberately, not overreacting to unusual single instances that come to light, but ensuring that reforms are introduced in such as way as to deal with the specific problem at hand and guarding against the unintended consequences of legislative and preventive measures. In this way, the critical aspects of Internet fraud may be controlled and the exaggerated and unfounded problems ignored.

Towards More Informed Debate

How, then, can the discussion of Internet fraud become more informed and moderate?

The starting point comes with improved standards of information. Better and more extensive research needs to be carried out not only locally, but also internationally. One idea, for example would be to include Internet fraud in the next round of the International Crime Victims Survey (see van Kesteren, Mayhew, Nieuwbeerta, and Bruinsma 2000).

Government statistical and census agencies could also play a role in conducting surveys of the population as they are well-placed to undertake research objectively. The Australian Bureau of Statistics, for example, could ask some questions about Internet fraud and security in its regular surveys on household use of information technologies.

Evidence also needs to come from those within the industry rather than outside commentators. Persuading financial institutions and merchants to be frank in disclosing Internet fraud experiences is by no means simple, but some appropriate sharing of information needs to take place.

With improved levels of information and more accurate surveys of Internet fraud, we may then be in a position to direct resources appropriately to combat the problem. This may ensure that those who seek to obtain scarce crime prevention resources are not provided with funding merely on the basis of their self-interested reports of the extent of the problem.

References

Anonymous 2000, 'IT 1 News', *The Age (Melbourne)*, 11 July, p. 2.

Australian Bureau of Statistics 1998, *Household Use of Information Technology, Australia 1998*, (Cat. No. 8146.0), Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 1999, *Household Use of Information Technology, Australia 1999*, (Cat. No. 8146.0), Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 2000, *Use of the Internet by Householders, Australia*, February and May 2000 editions (Cat. No. 8147.0), Australian Bureau of Statistics, Canberra.

Australian Competition and Consumer Commission (ACCC) 1999, *Internet Service Providers* <http://www.accc.gov.au/docs/catalog.htm> (visited: 30 April 1999).

Australian Federal Police 2000, *Annual Report 1999-2000*, Australian Federal Police, Canberra.

Australian Securities and Investments Commission 2000, *Complaints Made Under the EFT Code of Conduct 1999-2000*, ASIC, Sydney.

Australian Securities and Investments Commission v Steven George Hourmouzis (Unreported decision of the County Court of Victoria, 30 October 2000, Stott J).

Council of Europe 2000, *Draft Convention on Cybercrime*, (Draft N° 25 REV.5), European Committee on Crime Problems, Committee of Experts on Crime in Cyber-Space, 22 December 2000, Council of Europe, Strasbourg (http://conventions.coe.int/treaty/EN/projets/projets.htm)

Ernst & Young 2000, *Fraud: The Unmanaged Risk*, Ernst and Young, London.

Federal Trade Commission v Audiotex Connection Inc (E.D.N.Y. Filed 13 February 1997).

Fife-Yeomans, J. 1998, 'Info Warriors: The Frontline Against Cybercrime', *Platypus Magazine: The Journal of the Australian Federal Police*, No 59, June, pp. 24-5.

Gettler, L. 2000, 'From Apocalypse to Y2K Yawn', *The Age (Melbourne)*, 30 December, p. 12.

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 2000).

Grabosky, P. N. and Smith, R. G. 1998, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Federation Press, Sydney / Transaction Publishers, New Brunswick.

Grabosky, P. N., Smith, R. G., and Dempsey, G. 2001, *Electronic Theft: Crimes of Acquisition in Cyberspace*, Cambridge University Press, Cambridge.

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

Louis Harris and Associates Inc 1999, *Consumers and the 21st Century: A Survey Conducted for the National Consumers League*, Louis Harris and Associates Inc, New York.

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

Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2000, *Damage and Computer Offences: Discussion Paper, Chapter 4*, Commonwealth Attorney-General's Department, Canberra.

National Office for the Information Economy and the Australian Computer Society 2000, *The Phantom Menace: Setting the Record Straight About On-Line Credit Card Fraud for Consumers*, National Office for the Information Economy and the Australian Computer Society, Canberra.

Office of Fair Trading 1998, 'Internet Scams Deleted, Sweep Identifies 'Get Rich Quick' Schemes', *Fair Trading Magazine*, Spring, Office of Fair Trading, London.

O'Toole, G. J. A. 1978, *The Private Sector: Private Spies, Rent-A-Cops, and the Police-Industrial Complex*, W. W. Norton and Company Inc., New York.

Philippsohn, S. 2000, 'An Overview of Electronic Crime in the 21st Century', *Intersec: The Journal of International Security*, April, http://www.afp.gov.au/ecrime/21c.htm (visited 16 January 2001).

R. v Stevens (Unreported decision of the New South Wales District Court, 27 March 1998; appeal to the New South Wales Criminal Court of Appeal dismissed [1999] NSWCCA 69).

Smith, R. G. 1999, 'Internet Payment Systems and their Security Risks', *Journal of Financial Crime*, vol. 7, no. 2, pp. 155-60.

Starek, R. B. and Rozell, L. M. 1997, 'The Federal Trade Commission's Commitment to On-Line Consumer Protection', *Journal of Computer and Information Law*, vol. 15, pp. 679-702.

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.

United States, Department of Justice 2000, *Internet Fraud: Appendix B*, Report of the Criminal Division's Computer Crime and Intellectual Property Section http://www.cybercrime.gov/append.htm (visited 5 July 2000).

United States Department of Justice and Federal Bureau of Investigation 2001, 'Internet Fraud Complaint Centre', http://www.ifccfbi.gov/ (visited 16 January 2001).

van Kesteren, J., Mayhew, P., Nieuwbeerta, P., and Bruinsma, G. 2000, *Criminal Victimisation in Seventeen Industrialised Countries: Key Findings from the 2000 International Crime Victims Survey*, ICVS Working Group, Vienna.

Walker, J. 1999, 'How Big is Global Money Laundering?', *Journal of Money Laundering Control*, vol. 3, no. 1, pp. 25-37.