AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 243

e-Crime Solutions and Crime Displacement

Russell G. Smith, Nicholas Wolanin and Glenn Worthington

There are, arguably, three precursors to the commission of most crimes. These are the presence of a motivated offender, an available opportunity to act illegally (in other words, the presence of a suitable target), and the absence of a capable guardian or someone who might prevent the crime from being committed. Although motivations for acting illegally may well have remained fairly constant over time, developments in computing and communications technologies have created many new opportunities for people to act illegally. At the same time, the computer security industry has increased its capacity as "electronic capable guardians".

Previous research at the Australian Institute of Criminology has documented the extensive range of opportunities that exist for electronic crime (see Grabosky & Smith 1998; Grabosky, Smith & Dempsey 2001). The traditional response has been to devise a range of situational measures that seek to make the commission of crime less attractive to potential offenders. Such measures aim to increase the levels of effort and skill required to commit offences, to create a greater risk of apprehension of offenders, and to decrease the potential rewards that offenders seek to derive from their illegal activities (Clarke 1995).

If, however, it is assumed that potential offenders act on the basis of some rational calculation to balance the likely risks against the benefits of some course of conduct then, as some crimes are seen to be more risky, other easier targets may be considered instead. This raises the potential problem of crime displacement which has been of concern for many years now.

This paper considers the potential displacement effects that may arise from the introduction of crime prevention measures designed to reduce electronic crime and how best to guard against them. Being aware of these risks will help to ensure that well intentioned efforts to reduce crime do not make matters worse.

Adam Graycar
Director

Concerns about displacement have been succinctly described by Eck (1998) as follows:

> Fear of displacement is often based on the assumption that offenders are like predatory animals (they will do whatever it takes to commit crimes just as a rat will do whatever it takes to steal food from the cupboard).

Theorists have identified six ways in which criminal activity might be displaced following situational crime prevention measures (Reppetto 1976; Hakim & Rengert 1981; Barr & Pease 1990; Hesseling 1994):

- displacement of crime to other locations (spatial);
- displacement of crime to other times or occasions (temporal);
- displacement to softer targets (target);
- displacement through different modus operandi (tactical);
- displacement to other types of crime (offence); and
- displacement to other perpetrators (perpetrator).

Although listed discretely here, new patterns of offending will sometimes involve multiple types of displacement. In addition, it must be recognised that displacement can take place not only as a direct consequence of the introduction of some crime prevention measure, but also through the creation of new opportunities for crime to be committed. The introduction of credit cards, for example, itself a

January 2003

ISSN 0817-8542
ISBN 0 642 24287 9

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au

strategy designed to prevent theft of cash, has led to new forms of crime in which card account details maintained on electronic databases are stolen.

To date, displacement research has focused on "traditional" crimes such as burglary, motor vehicle crime and vandalism. It has also looked at prostitution and some non-criminal behaviours such as suicide. Considerable research has been conducted, some of it of a higher standard than others. It has tended to show that that displacement rarely takes place, and that when displacement does occur it usually does not overwhelm other gains achieved by blocking crime opportunities (Eck 1998). Displacement-like effects may also sometimes arise because a specific crime prevention measure has not fully solved the problem or has left some opportunities for offending available.

This paper seeks to apply theories of displacement in the context of electronic crime by considering the possible counterproductive effects which electronic crime reduction techniques might have. Electronic crime is different in many respects from traditional crimes, and the concern is that displacement might be more of a problem here than for violent and property crimes. Although empirical evidence of displacement in this area is not yet available, policy-makers need to be aware of the potential risks that could arise, and researchers need to devise appropriate studies with which to measure exactly what is taking place.

Spatial Displacement (to Other Locations)

Spatial displacement is perhaps the most intuitive type of displacement. For instance, it is often suggested that incidents of burglary or robbery are simply displaced from locations in which targets have been hardened to those in which targets remain less protected. However, as Ratcliffe (2002) has recently found in a study of a burglary reduction strategy used in the Australian Capital Territory, displacement was found not to occur. This was largely because increased rates of apprehension of a limited supply of offenders decreased the overall burglary rates throughout the targeted area.

In the case of electronic crime, the physical location of offenders is sometimes less important than in the case of terrestrial crimes, as offenders are often able to gain access to networks remotely. What may become apparent, however, is that offenders will target victims in jurisdictions that have lower levels of networked security, such as some developing countries that have only recently taken up digital technologies and in which security remains a low priority (see, for example, Internet fraud risks in the Asia-Pacific region described by Smith & Urbas 2001).

Where new security measures have been introduced in particular countries, offenders may choose to go to other countries with less sophisticated security. An example of both spatial and target displacement cited by Levi (1998, p. 436) is the introduction of computer chip cards in the United Kingdom which may lead some plastic card fraudsters to target countries still using magnetic stripe cards (such as Australia), or the theft and use of cards from other countries not yet equipped with computer chips.

A related risk concerns so-called "jurisdiction shopping", in which offenders target victims in jurisdictions that have the lowest criminal penalties for computer crimes or in which extradition treaties do not exist with countries in which victims are located. For example, Onel de Guzman, who allegedly propagated the "Love Bug" virus, was unable to be prosecuted in the Philippines because the Electronic Commerce Act which prohibits computer hacking only came into force after his actions took place, and was not retrospective (Bell 2002, p. 311).

Offenders might also seek to keep incriminating data on computers in other countries. In one recent case, a computer hacker stole 485,000 credit card numbers from an electronic commerce web site and secretly stored the information on an American government agency's web site (Lehman 2000).

Temporal Displacement (to Later Times or Occasions)

Temporal displacement of crime occurs when the time at which offences take place is altered in response to the hardening of targets. In the online environment where access to computers is available throughout the day and night, temporal displacement is unlikely to occur unless some services are only available during certain hours.

The possibility arises, however, that offenders may target victims in other countries at times when it is impossible for personal telephone verification checks to be undertaken. Funds could, for example, be electronically debited from accounts at night when a company is closed and when the transaction could not immediately be identified. Cash could then be withdrawn from an ATM in another location.

A similar problem arose with early types of ATMs which permitted accounts to be overdrawn during night-time hours when the machine was "off-host" (Chapman & Smith 2001). The normal daytime security measures were thus able to be overcome.

Potential offenders may also choose to operate during times of high volume transaction traffic, hoping to hide their illicit transactions in the data stream. During peak volume periods, activity profiling software may nonetheless identify an illicit transaction but it would more likely be immersed in a greater number of false positives, thereby delaying intervention.

Target Displacement (to Related but Softer Targets)

In a Swiss study of bank robbery it was found that increased security had reduced the risk of robbery for protected banks but that this reduction had not reduced the overall number of bank robberies committed (Grandjean 1990). In other words, the robbery of targets with increased security was displaced to similar types of targets that remained relatively unprotected.

In the electronic environment, this could occur when offenders target mobile messaging devices or laptop computers that might have less security features built in or used than networked personal computers located in workplaces. Similarly, enhancing user authentication systems, such as through the use of biometric technologies, could lead to an increase in attempts to target computers with traditional (or no) authentication systems, such as passwords or personal identification numbers (PINs). Shorter passwords or lower-level encryption might also be more attractive to offenders than more secure versions.

Another concern is that as large corporations and large public sector agencies continue to improve their electronic security, offenders may target small businesses or individuals who have inadequate security precautions in place. In the case of remote access to networks, which is the area of greatest concern to corporations (see KPMG 2001), it may be that hackers will target small retail outlets with poor security in order to gain entry to larger systems. In this way, the weakest link in a security chain may be targeted. The effect may also be to displace electronic crime away from large public sector agencies to smaller organisations within the private sector.

Similarly, large private sector organisations such as financial institutions are now making use of neural networks to analyse transaction patterns with a view to detecting and preventing financial crime. Software has been devised to analyse user spending patterns in order to alert individuals to the presence of unauthorised transactions. Such expensive software is often beyond the means of smaller businesses which, as a result, could become more attractive targets for fraud.

Tactical Displacement (Adoption of a Different Modus Operandi)

One consequence of the development of electronic security systems could be that offenders may employ different methods to achieve their ends. For example, the use of sophisticated public key encryption systems may cause offenders to change their modus operandi by seeking to have key pairs issued to them in false names or making use of another person's keys without their permission. This might be a much easier way in which to perpetrate online fraud than trying to compromise the high-level encryption used in public key systems. Offenders could also seek to bribe staff within registration authorities to disclose keys that have been issued or to issue duplicates for illegal purposes.

Hardening electronic targets (for instance through the construction of firewalls and the implementation of regimes of user authentication checks) may prevent remote unauthorised access to computers with the result that offenders will seek to gain access using internal methods. This may involve external offenders co-opting or even planting agents (moles) within the organisations they target. Employees of agencies, particularly those who work in information technology departments, may be subject to bribes or threats such as blackmail or physical coercion by offenders seeking access to computers or confidential information.

In the New South Wales Independent Commission Against Corruption's (1999) Operation Anschutz, an arrangement was uncovered in which waste disposal contractors were allowed to dump waste without paying fees in return for corrupt payments to Council employees, who could manipulate the waste management computer systems. Similar risks of corruption could arise anywhere in the electronic environment where offenders may attempt to bribe government employees to over-ride computer security measures.

Enhanced network security could also lead to an increase in theft of hardware such as desktop personal computers or, more often, laptop computers and mobile messaging devices. Having hardware in one's possession may make it easier to compromise security measures than would be possible via remote access. Although there has been an increase in theft of laptop computers and mobile telephones, it is unclear whether these are stolen in order to gain access to information or simply for re-sale purposes.

A recent report of the theft of 40 laptop computers from the Department of Defence and others from the National Crime Authority and Australian Federal Police (*Sunday Sun Herald*, 31 March 2002) suggests that obtaining confidential information may have been a more likely motive than simply the re-sale of the hardware.

The use of transaction thresholds could also lead to an increase in low-value fraudulent transactions being committed that financial institutions and merchants might not be able or willing to detect. If such low-value crimes were multiplied many times, large sums could be stolen in total.

Offence Displacement (to Other Types of Crime)

Displacement to other types of criminal activity defies accurate measurement as the reason for a movement to a new type of crime could be due to factors that are not related to the hardening of particular targets. Offenders skilled in compromising electronic security measures might also be unskilled in carrying out other types of crime, particularly if violence were involved.

Offence displacement is, however, one of the more worrying consequences of target hardening, as the likely change would be away from soft economic crimes to more violent offences. For example, enhanced user authentication may result in offenders compelling victims to disclose passwords, PINs or to present fingers for biometric scanning under threat of violence (Bell 2002, p. 310). This has already occurred in connection with some ATM robberies in which users have been kidnapped or forced to withdraw cash (Smith, Nelson & Mayhew 2002). Fortunately, most biometric systems require living tissue to be presented for scanning, thus preventing the possibility that severed fingers could be used.

Similarly, once Internet banking becomes commonplace there could potentially be an increase in home

invasion in which users are compelled under threat of violence to transfer funds to offenders' accounts electronically, while accomplices wait to withdraw cash immediately from ATMs once the transaction has been processed. Already we have seen duress become a feature of some ATM robberies as offenders seek to obtain PINs under threat of violence. Home burglary could also increase if offenders sought to steal laptop computers or personal computers kept in home offices. This is potentially a serious consequence as increasing numbers of people work remotely from home in both public and private sector employment.

The possibility also exists that as a result of target hardening some organised criminals may move away from electronic crime into other types of activity, such as the drug trade or people smuggling. Displacement to entirely new areas of criminal activity is exceedingly difficult to detect because of the need to identify individuals who have changed patterns of offending specifically due to enhanced crime prevention areas in relation to one type of crime.

In an interesting study conducted in Canada (Mativat & Tremblay 1997) found high levels of specialisation amongst organised credit card counterfeiters with individuals having skills in tasks such as the fabrication of holograms or card re-embossing. Between 1992 and 1994 there was a significant increase in counterfeit card fraud. The authors examined the possibility that offenders who had previously engaged in altering stolen credit cards had shifted their activities to counterfeiting cards because of the availability of card skimming and embossing technologies. It was found, however, that the groups of individuals who were engaged in stealing and altering cards were quite different from those who engaged in counterfeiting cards, and that the displacement hypothesis was not supported. For crime displacement to occur, there needs to be much more than simply the availability of new opportunities to act illegally. There needs to be a group of individuals with appropriate skills to engage in the new types of crime and they need to have the necessary social connections to permit them to operate in a new field.

Finally, offenders may be involved in committing crimes that arise directly out of their online activities, such as gaining access to computers without authorisation, rather than simply committing theft. Infringement of privacy and intellectual property offences might also increase.

Perpetrator Displacement (to Other Offenders)

Perpetrator displacement refers to new offenders attacking a target as existing offenders are removed following the implementation of crime prevention initiatives or official action. Perpetrator displacement contemplates the situation in which a ready supply of potential offenders exists to replace others for whom the commission of crime has become too difficult through the introduction of crime prevention measures, or impossible because of imprisonment.

Owing to the presence of networked information sources among computer criminals, such as the chat rooms favoured by hackers in which details of new strategies or targets are shared rapidly across the globe, there will be a ready supply of new computer criminals who can take the place of any that are removed by official action. Related to this is the risk that as illegal strategies adopted by some offenders become unavailable, this fact will be communicated quickly so that other individuals can devise new means of overcoming the crime prevention solution. This would involve a blend of both tactical and perpetrator displacement.

Another possibility in which offender displacement may occur concerns the use of contractors. Although electronic security measures may mean that employees of organisations may be unable to act illegally, new opportunities may arise for contractors with appropriate knowledge to compromise security systems that they, themselves, might have installed.

In September 2001, for example, a financial consultant formerly contracted to the Department of Finance and Administration was convicted of defrauding the Australian government by transferring A$8.7 million electronically to private companies in which he held an interest. He did this by logging on to the Department's computer network using another person's name and password. He was also able to obscure an audit trial through the use of other employees' log-on codes and passwords. He was sentenced to seven years and six months' imprisonment, with a non-parole period of three years and six months (R. v *Muir*, Australian Capital Territory Supreme Court, 25 September 2001). Cases such as this will continue to occur unless adequate control mechanisms are used to ensure that contractors with access to secure networks remain trustworthy.

Changes in work practices introduced by information technologies may also mean that criminals need only corrupt one key individual rather than a number. For example, an employee of a motor vehicle registry may now carry out all the functions from one workstation previously undertaken by a number of staff (clerical, cash handling, records management, customer service). As a result, instead of having to trick or to corrupt a number of people in order to perpetrate a fraud, only one key official now needs to be bribed. In this sense, displacement has resulted in a smaller number of individuals being at risk of corruption, although each may be offered a higher payment.

Summary

Table 1 summarises the displacement effects which could occur as a result of crime prevenion measures designed to reduce electronic crime. The categorisation of crime prevention measures was developed by Clarke (1995, p. 109). Some of the possible situational strategies used to prevent electronic crime are listed in column 2. Column 3 provides some examples of potential displacement effects that might occur.

Policy Implications

How then, should policy-makers respond to these issues? Although some initiatives should come from government, industry should also consider how to respond to these potential risks.

First, appropriately designed and well targeted research needs to be undertaken to assess the extent to which the various forms of potential displacement outlined above actually occur. For example, more detailed research into the use of computers in financial crime is needed, as is research into the underlying causes of official corruption. In other contexts, displacement effects have been minimal, but evidence in the case of electronic crime does not as yet exist—although some pertinent examples do. Conducting research of this nature is by no means simple: displacement could occur in one or more of the identified ways, making it difficult to assess the influences of each. In addition, displacement effects might not become apparent for some time, making the use of expensive and longitudinal research necessary. Finally, because electronic crime can take place across jurisdictional boundaries, it would be necessary to have a wide-scale geographical focus to measure some types of displacement.

Second, if displacement effects are able to be demonstrated, this raises complex issues for policy-makers as to how best they should respond. Logically, if crime has been found to be displaced in some way then devising a new strategy to solve this problem might simply result in crime being further displaced with no eventual crime reduction possible.

If displacement has been demonstrated then policy-makers may be faced with choices in allocating crime control resources between various types of crime problems, including the one originally targeted and the crime problem created as a result of displacement effects. Difficult choices would then arise as to which type of crime should be targeted for enhanced crime reduction measures. For example, if biometric user authentication devices led to an increase in physical violence or incidents of duress in which victims were compelled to permit access to computers under threat of violence, it could be necessary to abandon the use of biometric systems and revert to earlier user authentication methods, such as passwords, which were less often associated with physical violence. Choices would need to be made based not only on cost but also on the need to protect individuals from violent crime.

Policy-makers may also need to consider the socio-political implications of potential displacement effects. Often only large public and private sector institutions can afford costly and sophisticated electronic crime prevention measures. For example, it has been found that generally only large financial institutions and large government agencies are able to make use of neural networks for fraud reduction purposes. If such technologies displace crime to other less well protected organisations, it may be that crime will have a disproportionate effect on smaller enterprises less able to bear the losses inflicted. Government needs to consider this when allocating crime prevention resources to large agencies.

Potential displacement effects also need to be taken into account when designing new technologies in order to reduce the potentially counterproductive consequences of target hardening and other crime control measures. One recent example is the design of early mobile phones that made cloning relatively simple. Similarly, the use of mobile phone hardware identification has only recently been introduced in order to prevent theft of handsets (Harrington & Mayhew 2001).

Policy-makers should also, arguably, consider the more positive consequences of electronic crime prevention initiatives that might, in fact, make matters better rather than worse. Clarke and Weisburd (1994)

Table 1: *Situational electronic crime prevention measures and displacement possibilities*

Crime prevention measure	Electronic crime application	Displacement possibilities
Increasing the effort		
Target hardening	Firewalls, tempest security (against electromagnetic radiation scanning), laptop anti-theft devices	Bribery/coercion of IT staff; theft of data by remote access to networks
Access control	Passwords, tokens, biometrics and encryption	Bribery/coercion of public sector or IT staff; extraction of passwords by duress
Deflecting offenders	Use of computer games and the Internet	Identification of new targets; enhanced peer group effects
Controlling facilitators	Registration of computer users with Public Key Registration Authorities, Internet service providers and carriers	Bribery of facilitators; increase in crime by insiders; identity deception to obtain registration
Increasing the risks		
Entry/exit screening	Checks on use of passwords	Bribery/coercion of public sector or IT staff; extraction of passwords by duress
Formal surveillance	Analysis of usage patterns using neural networks to analyse transaction patterns	Destruction of main fame computers and virus attacks on analytic software
Surveillance by employees	Workplace PC surveillance using CCTV	Remote and out of office hours access
Natural surveillance	Reporting of colleagues by IT personnel, reporting hotlines	Remote and out of office hours access; bribery of IT personnel
Reducing the rewards		
Target removal	Government- or industry-funded services	Bribery/coercion of IT staff; increase in public sector attacks
Identifying property	Registration of computer hardware	Theft of electronic hardware; corruption of registrars; illegal removal of identifiers
Removing inducements	Restricted publicity of crimes	Internet self-promotion and enhanced personal rewards
Rule setting	Codes of conduct for Internet use	Targeting of services outside regulatory controls

identified the possibility of "diffusion of crime prevention benefits". In some circumstances, offenders may be uncertain about the scope of prevention efforts and avoid both the blocked opportunities and similar unblocked opportunities. In the area of electronic crime, an example might be where enhanced user authentication systems not only prevent identity-related fraud but also make it more difficult to carry out money laundering operations electronically.

Finally, attempts at harmonising computer crime laws and procedures globally should continue. This might have the effect of reducing the number of so-called "safe havens" to which displaced computer criminals may gravitate.

Conclusions

Although it is premature to suggest a conclusion as to the extent of displacement following the introduction of electronic crime prevention measures, there have been some examples both of displacement effects not eventuating and also of some effects taking place. The online environment is, however, conducive in a number of ways to displacement, as many crimes are committed remotely and anonymously using technologies that can easily be adapted to circumvent new controls.

Unfortunately displacement is often difficult to detect as some forms of illegality, such as corruption of officials, may not obviously be related to the original crime problem. Similarly, diffused benefits of electronic crime solutions can also be covert and difficult to measure. Now is the time for risks and benefits of this nature to be understood and for the extent of such consequences to be documented by controlled and sophisticated research. Although displacement of electronic crime may, hopefully, be as limited as is the case with traditional crimes, efforts need to be made to guard against the possibility of this occurring, and to devise appropriate responses in advance of the problem emerging.

Acknowledgments

This paper was first presented at the New South Wales Independent Commission Against Corruption and New South Wales Ombudsman's, 4th National Investigation Symposium: Sherlock or Sheer Luck? *in Sydney, 8 November 2002.*

Pat Mayhew and two anonymous reviewers made a number of helpful suggestions on an earlier draft of this paper for which the authors are grateful.

References

Barr, R. & Pease, K. 1990, "Crime placement, displacement, and deflection", in M. Tonry & N. Morris (eds), *Crime and Justice: A Review of Research*, vol 12, University of Chicago Press, Chicago.

Bell, R.E. 2002, "The prosecution of computer crime", *Journal of Financial Crime*, vol. 9, no. 2, pp. 308–25.

Chapman, A. & Smith, R.G. 2001, "Controlling financial services fraud", *Trends and Issues in Crime and Criminal Justice*, no. 189, Australian Institute of Criminology, Canberra.

Clarke, R.V. 1995, "Situational crime prevention", in M. Tonry & D.P. Farrington (eds), *Building a Safer Society: Strategic Approaches to Crime Prevention*, University of Chicago Press, Chicago, pp. 91–150.

Clarke, R.V. & Weisburd, D. 1994, "Diffusion of crime control benefits: Observations on the reverse of displacement", in R.V. Clarke (ed.), *Crime Prevention Studies*, vol. 2, Willow Tree Press, Monsey, New York.

Eck, J. 1998, "Preventing crime at places", in L.W. Sherman, D. Gottfredson, D. Mackenzie, J. Eck, P. Reuter & S. Bushway (eds), *What Works, What Doesn't, What's Priomising*, National Institute of Justice, Washington DC.

Grabosky, P.N. & 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. & Dempsey, G. 2001, *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge University Press, Cambridge.

Grandjean, C. 1990, "Bank robberies and physical security in Switzerland: A case study of the escalation and displacement phenomena", *Security Journal*, vol. 1, pp. 155–9.

Hakim, S. & Rengert, G.F. 1981, "Introduction", in S. Hakim & G.F. Rengert (eds), *Crime Spillover*, Sage Publications, Beverly Hills, pp. 7–19.

Harrington, V. & Mayhew, P. 2001, *Mobile Phone Theft*, Home Office Research Study No. 235, Home Office, London.

Hesseling, R. 1994, "Displacement: A review of the empirical literature", in R.V. Clarke (ed.), *Crime Prevention Studies*, vol. 3, Criminal Justice Press, Monsey, New York.

KPMG 2001, *Global eFr@ud Survey*, KPMG Forensic and Litigation Services, http://www.kpmg.ca/english/services/docs/fas/efraud2001.pdf (viewed December 2002).

Lehman, D. 2000, "Feds ID hacker who stole 485,000 credit-card numbers", *InfoWorld Daily News*, InfoWorld Media Group, http://www.infoworld.com (available from http://www.factiva.com [subscriber only]; viewed October 2002).

Levi, M. 1998, "Organised plastic fraud: Enterprise criminals and the side-stepping of fraud prevention", *The Howard Journal*, vol. 37, no. 4, pp. 423–38.

Mativat, F. & Tremblay, P. 1997, "Counterfeiting credit cards", *British Journal of Criminology*, vol. 37, no. 2, pp. 165–83.

New South Wales Independent Commission Against Corruption 1999, *Weighing the Waste: An Investigation into the Conduct at Local Council Waste Depot Weighbridges at St Peters and Elsewhere*, New South Wales Independent Commission Against Corruption, Sydney.

Ratcliffe, J. 2002, "Burglary reduction and the myth of displacement", *Trends and Issues in Crime and Criminal Justice*, no. 232, Australian Institute of Criminology, Canberra.

Repetto, T. 1976, "Crime prevention and the displacement phenomenon", *Crime and Delinquency*, vol. 22, pp. 166–77.

Smith, R.G., Nelson, D. & Mayhew, P. 2002, "Robberies at automated teller machines in Australia", *Trends and Issues in Crime and Criminal Justice*, no. 228, Australian Institute of Criminology, Canberra.

Smith, R.G. & Urbas, G. 2001, *Controlling Fraud on the Internet: A CAPA Perspective: A Report for the Confederation of Asian and Pacific Accountants*, Research and Public Policy Series, no. 39, Confederation of Asian and Pacific Accountants, Kuala Lumpur/Australian Institute of Criminology, Canberra.

Dr Russell G. Smith is Deputy Director of Research at the Australian Institute of Criminology.

Mr Nicholas Wolanin is a National Task Force Coordinator at the Australian Crime Commission and an Adjunct Senior Lecturer at the Australian Graduate School of Policing. The views expressed in this paper are not necessarily those of the ACC or Charles Sturt University.

Dr Glenn Worthington was formerly a Research Analyst with the Australian Institute of Criminology and is now a Research Officer with the Australian Parliament, Department of the House of Representatives, Joint Standing Committee on Treaties.

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.

Project no: 0040