Trends & issues
in crime and criminal justice

No. 420 August 2011

Australian Government
Australian Institute of Criminology

Risk factors for advance fee fraud victimisation

Stuart Ross and Russell G Smith

Foreword | *Fraud is Australia's most costly form of crime with the Australian Institute of Criminology estimating that in excess of $8.5b was lost to fraud in 2005 (Rollings 2008). Consumer fraud alone has been found to cost Australians almost $1b each year (ABS 2008c). Most types of consumer fraud entail the use of so-called 'advance fee' techniques in which individuals are tricked into paying money—an 'advance fee'—upfront in order to secure an anticipated financial or other benefit at a later date. However, the promises of wealth are false and victims invariably lose their payments in full. Such scams have had a huge impact globally, with Ultrascan (2008) estimating that US$4.3b was lost to advance fee fraud in 2006. To date, however, there has been only limited research on how and why people respond to such unsolicited invitations and become victims. This paper examines the characteristics of a sample of victims of advance fee frauds to determine how their behaviour and personal circumstances might have contributed to their willingness to respond to unsolicited invitations and to their subsequent loss of money or personal information.*

Adam Tomison
Director

Advance fee scams come in many guises. Some regularly seen examples involve:

- offers to participate in business deals with wealthy individuals;
- assisting dignitaries by paying fees to move large sums of money out of a foreign country in order to receive a share of the proceeds;
- paying fees in order to receive lottery winnings, an inheritance or some other prize; or
- paying money to develop a personal relationship or marriage with someone met online.

In each case, the motivation behind the deception is to secure a payment from the victim which is paid in the expectation that a substantial benefit will follow. Of course, this fails to eventuate and the victim is left without the anticipated reward and without the funds paid in advance. Effective prevention of, and law enforcement responses to, such crimes are problematic. This form of fraud is often associated with offenders based in West Africa (and in particular Nigeria) but is now geographically widespread. The use of electronic communications makes it extremely difficult to prevent scammers from reaching potential victims, and the ability of the scammers to conduct their operations anonymously from cells in a variety of countries means that few offenders are arrested and prosecuted (Smith, Holmes & Kaufman 1999). The best approach lies with prevention, in raising awareness and in encouraging potential victims not to respond to invitations in the first place. Developing effective prevention strategies requires a sophisticated understanding of the scam typologies used and the reasons why people choose to participate. Armed with such knowledge, advice can be developed to persuade potential victims not to become involved.

Simply knowing victims' demographic and socioeconomic characteristics is insufficient to know why people respond, as prior research has found that fraud victimization cannot be reliably predicted using demographic information alone (Titus, Heinzelman & Boyle 1995; Trahan, Marquant & Mullings 2005). Instead, evidence is needed on the way in which offenders manipulate victims to form a relationship of trust conducive to the extraction of funds—often in instalments involving large sums over long periods of time. In addition, evidence is needed on the extent to which offenders seek to implicate victims in their own victimisation (Titus & Gover 2001) so as to prevent reporting of the scam once it has occurred.

Rather than selecting potential victims on the basis of their observed wealth or ability to pay, such as occurs with corporate fraudsters or burglars, advance fee fraud offenders disseminate millions of invitations randomly in the expectation that a small number will respond and be available for victimisation, sometimes following a convoluted process of trust-building and deception (Smith, Holmes & Kaufmann 1999; Trahan, Marquat & Mullings 2005). This process entails offenders understanding the psychology of their intended victims and adapting their strategies accordingly. Victims may continue the fraudulent relationship

even after they have lost considerable sums and be unwilling to desist even in the face of clear and compelling evidence that the activity is fraudulent.

Not everyone is at risk of becoming a victim of fraud despite the wide net being cast. Rather, it is the behaviour of the consumer that is important in determining whether or not a person is taken in by a scam (Holtfreter, Reisig & Pratt 2008). Two theoretical approaches have been used to understand how people are victimised. One involves consideration of the behaviours that increase the risk of potential victimisation and the other examines the choices and decision-points of people who are exposed to fraudulent offers.

Victim behaviour

A great deal of criminal behaviour has its origins in the activities and processes of ordinary life. Cohen and Felson (1979) argued that changes in patterns of routine activity influence crime rates by creating a convergence of three crucial elements that make victimisation possible in the context of direct-contact predatory crimes. These are the presence of motivated offenders, suitable targets and the absence of capable guardians against a violation. A routine activity approach to crime prevention involves reducing the motivation of offenders, making suitable targets harder to find and/or increasing the level of guardianship.

A number of researchers have used routine activity theory to examine various forms of internet-based crime. One example concerns phishing in which internet users are tricked into disclosing personal information on fictitious websites. Hutchings and Hayes (2009) argued that the exponential rise in phishing can be explained in terms of increasing numbers of people with the technical skills needed to commit these offences (motivated offenders), the increasing use of internet banking and other online commerce (suitable targets) and the lack of awareness in the community and regulatory agencies of the threat posed by these crimes (absence of capable guardianship).

If routine activity theory was applied to advance fee scams, then it could first be assumed that a person who spent long hours on the internet would be more likely to become a target to a global pool of motivated offenders. Second, those persons who use fewer internet security measures would have a greater likelihood of victimisation because of the absence of capable guardianship to prevent the crime from occurring.

Victim psychology

Advance fee fraud is one example of a range of crime methodologies based on deception or fraud. An early analysis of the psychology of fraud argued that victims' lack of self control was central to the process of victimisation. Gottfredson and Hirschi (1990) argued that individuals with low self control tend to pursue their own self-interests without consideration of the potential long-term consequences. Such individuals prefer activities that require little skill or planning and that result in immediate gratification and as a result, it is they who are more likely to engage in risky behaviours, such as trying to make 'easy money' by responding to scam invitations. Van Wyk and Benson (1997) found that people who reported greater financial risk-taking behaviour were also more likely to report being the target of fraud, although risk-takers did not necessarily become victims of fraud. In a similar study, Holtfreter, Reisig and Pratt (2008) showed that people who scored lower on measures of low self control were more likely to report being a victim of fraud.

A more comprehensive analysis of the psychology of fraud carried out for the Office of Fair Trading (2006) argued that fraud victimisation can be explained in terms of victims' cognitive judgments ('decision errors') and motivations that scammers manipulate through the use of strategies of persuasion or deceit. They grouped various psychological strategies associated with fraud according to whether they were related to the source (the motivation and plans of the offenders), the medium (the form of the fraudulent communication), the message (the strategies used to persuade potential victims to enter into the fraud) or the recipient (the characteristics that make victims vulnerable). For this research, it was the last three factors that were of interest.

Some of the psychological strategies that scammers use include linking the scam to an apparently reputable person or business to lend legitimacy to the offer, offering a reward that is grossly disproportionate to the effort required to obtain it, personalising offers to make it appear that the victim has been personally selected and drawing victims into the scam through a series of small steps. For all of these strategies, most scammers have a further advantage because the scam is delivered via a medium such as the telephone, mail, internet site or email and victims have little capacity to confirm the validity or otherwise of the message or identity of the scammer.

The OFT research also identified a number of characteristics of scam victims that make them more vulnerable to scams. Even though victims actually spent more time analysing the content of fraudulent messages, and often had better background knowledge of the area of the scam content (eg financial market knowledge), victims appeared to be less able to regulate their emotional response to scam messages. Victims are also more likely to be socially isolated, or to keep their decisions about responding to scams private. As a result, they are less likely to receive warning messages from other people who may be more suspicious of the fraudulent message (Office of Fair Trading 2006).

Victim demographics

Prior studies have shown that there are few demographic factors that reliably distinguish fraud victims from non-victims. Victim age is the only factor that has been consistently found to be a significant predictor of fraud victimisation; however, the age group found to be most at risk varies across studies (see Lee & Soberon-Ferrer 1997; Smith & Budd 2009; Titus, Heinzelmann & Boyle 1995; Van Wyk & Benson 1997; Van Wyk & Mason 2001).

Victim lifestyle factors

Previous research has also shown that people who have experienced negative life events, such as financial or employment issues, home maintenance issues, legal issues, medical issues and neighbourhood issues, are more likely to be victims of fraud (NASD Investor Education Foundation 2006). The NASD Investor Education Foundation (2006) study, for example, showed that investment fraud victims reported a significantly greater number of negative life events than non-victims. Research by Ultrascan (2008) also demonstrated that there was a strong correlation between victims of white-collar crime and the existence of a recent or life-changing event.

Exposure to negative life events may impair people's judgment in a number of ways. Lee and Soberon-Ferrer (1997) argued that negative life events can force individuals to face consumer roles when they are least prepared to do so, making them vulnerable to fraudulent invitations. In addition, these negative events may also lead to the social isolation of an individual, which may, in turn, make them more eager to respond to fraudulent schemes as a form of social interaction.

The present study

In order to explore some of these ideas, the Australian Institute of Criminology (AIC) collaborated with Victoria Police and the School of Social and Political Sciences at the University of Melbourne in a research project that involved surveying a sample of people who had sent money to Nigeria.

The sample was identified by Victoria Police financial crime personnel using financial intelligence from the Australian Transaction Reports and Analysis Centre (AUSTRAC). It was comprised of people living in Victoria who had transferred money to Nigeria using an international funds transfer service during the 12 month period from 1 April 2007 to 31 March 2008.

A questionnaire was sent by Victoria Police to 1,410 such people in September 2008. Follow-up letters were sent a month later and 202 responses were received in all—yielding a response rate of 14.3 percent. Although this response rate is relatively low, it is similar to other surveys of this kind. Of course, some of the non-responders might also have been victims. The surveys were anonymous, although respondents were invited to participate in follow-up interviews by calling the AIC. Three such interviews were conducted, although the findings were not included in the current report owing to limitations of space. The surveys included advice about advance fee fraud and a list of contact numbers for respondents who believed they had been victimised. Victimisation was defined in accordance with the rules in Box 1.

Of the survey respondents, 54.5 percent were male, with the highest proportions aged 35–44 years (31%), having completed secondary schooling (32%) and having an income of under $20,000 (28%). Of the 202 responses to the survey, 120 (59%) were identified as victims of advance fee fraud. The remaining 41 percent were non-victims and were mainly people who said they had sent money to family or friends or had made donations to agencies in Nigeria. This high rate of victimisation is itself an interesting finding and suggests that this approach could be used to identify individuals who should receive advice about the risks involved in transferring funds to high-risk destination countries in the future.

Box 1 Identification of advance fee fraud victims

Survey respondents were identified as being a victim if they met at least two of the following criteria:

- They had sent money overseas to someone who was not a relative or as part of a normal business transaction.
- They had received repeated contacts seeking money before they sent it.
- They had sent money in response to a contact from someone they didn't know.
- They identified a known advance fee fraud victims methodology (claiming lottery winnings, assisting a foreign dignitary).
- No money had been recovered and they had not received any funds, goods or services in return.
- They had received threats of violence or intimidation in relation to the venture for which funds were sent.

Results

Respondents were asked to say to whom they had sent money, where they had sent it and the reasons why they had sent it. From their responses they were classified as being either victims or non-victims. Except where otherwise indicated, only results relating to apparent victims of advance fee fraud are presented below. Victims were further classified according to the kind of scam in which they had been involved. From Table 1, it is apparent that more than a third of victims had been exposed to 'dating' or 'relationship' scams. More than a quarter of victims had responded to invitations concerning online transactions, charitable donations and job-related scams, while the remainder were classified as having responded to 'other' types of advance fee invitations which included lottery scams.

In the following discussion, these three groups shall be referred to as follows:

- *dating scams*—including relationship scams;
- *online transaction scams*—including job offers, charity scams and other online transactions; and
- *other advance fee scams*—lottery scams and other types of advance fee scams.

Financial losses

Approximately three-quarters of victims had sent money to offenders on more than one occasion and over 40 percent had sent money five or more times. Some respondents either could not remember or were not prepared to say how much they had sent. Of those who did nominate an amount sent, the totals ranged from $100 to $120,000, with a mean of around $12,000.

Analysis of variance showed a statistically significant relationship between victim type and the amounts reported as having been sent overseas in the last 12 months ($F=4.24$, df (2, 81), $p<0.05$) and in total ($F=3.94$, df (2, 83), $p<0.05$). Post-hoc (Tukey) comparisons showed that victims of dating scams had sent more money overseas in the last 12 months and in total than victims of online transactions.

In general, victims of dating scams lost more money than those who were involved in other advance fee scams (around $17,500 compared with $11,500), while those who were victims of online transactions lost the least ($4,000 for job scams, $3,000 for charity scams and $1,000 for other online transactions).

Most of the money that victims sent came from their personal savings—80 percent of victims nominated this as the source of the money they sent—but some people took out a personal loan (13%) or borrowed money from family or friends to send (10%). A small proportion of victims (5%) had mortgaged property in order to raise funds to send to the fraudsters.

Other impacts

Many victims experienced one or more forms of trauma or hardship. In terms of the impact of the scam, the most frequently nominated response was financial hardship (54% of victims), followed by emotional trauma (43%) and loss of confidence in other people (40%). Twelve percent of victims said that they had experienced marital or relationship problems as a result of the fraud. Not surprisingly, those who reported financial hardship had lost more on average than those who did not report this impact ($14,000 versus less than $10,000).

Table 1 Victimisation by category of scam

Category of scam	Victims	
	n	%
Dating/relationship scams	42	35
Online transactions, charity and job scams	32	27
Other advance fee scam (including lottery scams)	46	38
Total	120	100

Source: AIC dataset (n=120)

Victim demographics

Age and income were found to be associated with the type of fraud that respondents experienced.

Age

A statistically significant relationship was found between victim status (victim versus non-victim) and age (Likelihood ratio=45.38, df=21, $p<0.01$). Similarly, in terms of scam type, a statistically significant relationship was found between scam type and age (Likelihood ratio=23.87, df=12, $p<0.05$). Calculation of adjusted standardised residuals for cells showed that respondents aged 65 years or older were more likely to be a victim of other advance fee scams, victims aged 45 to 54 years were more likely to be victims of dating scams and victims aged 18 to 24 years were more likely to be victims of online transaction scams. Survey respondents aged 35 to 44 years were more likely to be classified as not being a victim of any scam type.

This preponderance of older victims is consistent with the findings of other fraud research (Mathur & Moschis 1995; Office of Fair Trading 2006), but is particularly noteworthy given that the most advance fee victimisation took place via some form of internet communication (see below) and older people are the least likely to use these forms of communication (ABS 2008a).

Income

In relation to income levels, there was a statistically significant relationship between victim status (victim versus non-victim) and reported income (Likelihood ratio=43.04, df=15, $p<0.001$). Similarly, in terms of scam type and income levels, there was a statistically significant relationship between scam type and reported income (Likelihood ratio=25.33, df=10, $p<0.05$). Calculation of adjusted standardised residuals for cells showed that respondents with an income above $40,000 per annum were more likely to be classified as not a victim, respondents with incomes of under $20,000 were more likely to report being victims of other advance fee scams or online transaction scams, while respondents with incomes between $20,000 and $40,000 were more likely to report being victims of dating scams.

Education, employment and gender

There was little variation in educational levels, employment status or gender across the three forms of fraud. Overall, 53 percent of other advance fee scam victims were male while 59 percent of dating scam victims were male.

Recruitment

The most common way in which victims were recruited was through email, with two-thirds reporting that their first contact was by email. Another common form of initial contact was through web-based 'dating sites' or other social networking websites. In total, 85 percent of the victims had been recruited over the internet. A small number of victims first had contact with the offenders via mail, fax or phone, and in a very small number of cases, the victim was referred by someone they already knew.

In most cases, the approach by offenders involved a single 'message' to solicit funds. In the case of dating scams, funds were usually sought to pay for airfares, hospital bills or some other pseudo personal emergency. Other messages related to a reward available to the victim (18% of victims), money from a deceased estate (13%), or to recover money owed, obtain a well-paid job or assist in a charitable enterprise. In around 30 percent of cases, the victim was presented with more than one 'message'.

Some victims attempted to verify who they were dealing with in the course of their relationship with the scammers. Thirty percent of victims had undertaken some 'research' on the identity of the scammers and around 40 percent had been provided with some verification of the offenders' identity, including bank records, passport details and other travel documents, information held on websites and other official documentation—all invariably counterfeit.

Survey respondents were asked to indicate why they had sent money overseas. Victims of other advance fee scams said that they wanted to make extra money, obtain something they were entitled to receive, or take advantage of a unique offer. Victims of dating and charity frauds never nominated these reasons. Instead, they said they wanted to help out the person seeking their assistance or to support their relationship with the person. The presence of altruism as a motivation for responding to scam invitations is difficult to counter, as this positive quality in people is being manipulated by fraudsters for financial gain.

Contact between victims and offenders

The contact between victims and offenders was typically over an extended period and often the offenders introduced new people into the relationship. One-third of the victims were in contact with the offenders more than 20 times and nearly 30 percent of victims said they were still in contact with the offender(s) when they responded to the survey. Over half of the victims were in contact more than five times before sending money, and one in six had 20 or more contacts with the offender before sending money.

Victims of dating scams reported greater frequency of contact with the offenders than other types (around 45% had been in contact with the offender more than 20 times and there were 3 victims who had had more than 200 contacts with the offenders).

One of the strategies sometimes used by offenders who have recruited a victim is to introduce new people to authenticate their fraudulent claims (eg the victim may be introduced to a 'bank manager' or in the case of a dating fraud the fiancé's 'mother'). In around 40 percent of cases, the victim reported that new people had been introduced to them. New people were more likely to be introduced in cases of other advance fee scams. Around 50 percent of these victims reported that this had happened and identified them as purporting to be bank officials or representatives of courier companies.

Around 40 percent of victims had attempted to meet the person they had been in communication with and there were four victims who said they had travelled overseas in an attempt to meet, although in none of these cases was the attempt successful. Making attempts to meet was much more common in cases of dating scams—55 percent of these victims reported trying to meet the other person.

Reporting

An element in the criminal strategy behind advance fee fraud is that victims are often persuaded or threatened that they should not tell anyone about the details of the scam. This is usually presented to the victim with the rationale that the arrangement must be kept secret so that the victim can receive the promised benefits, although sometimes threats of violence or exposure to authorities are used. Around 20 percent of survey respondents reported that the offenders made threats of violence against either the victim or the victims' family. There was no difference between the three victim groups in terms of the likelihood that threats of violence were received.

Three-quarters of victims did not discuss the matter with anyone before they sent money overseas and 20 percent of survey respondents still had not told anyone at the time of the survey. When other people were told, this was most likely to be family or friends (46%). About one-quarter had informed their bank or credit card provider and of those who had, 30 percent had recovered some funds. Three-quarters of victims hadn't told either the federal or Victorian (state) police and only six victims had told police overseas.

The reasons victims gave for not reporting the crime was that they were embarrassed (27%), believed the police would not be able to find the offender (20%) or that there was insufficient evidence to proceed against the offender (25%). A small number of victims said they feared for their safety, or were afraid they would be prosecuted for their involvement in the fraud. Some victims hadn't made a report because they still hoped to recover some of their money. This was most often the case with victims of other advance fee scams, where one-quarter were still hopeful of recovering some funds.

Lifestyle circumstances

The questionnaire had seven questions dealing with negative life circumstances. Victims reported high levels of depression (around 40% of victims reported that they had been depressed in the last 5 years), had suffered a personal financial crisis (45%) or had a serious illness (22%). In Australia generally, only 4.1 percent of the population in 2007 reported having experienced symptoms of depression in the preceding 12 month period, or 11.6 percent over their lifetime (ABS 2008b). Clearly, the victims of the current study had a much higher incidence of self-reported depression than the general population, although it was not possible to determine if this condition was present prior to the fraud victimisation or if it arose as a result of the victimisation.

Internet usage

Over 80 percent of victimisation involved some form of internet communication, which represents the same rate of internet usage among the general Australian population (at September 2010—80.1%; Internet World Stats 2010). The Australian Bureau of Statistics reports that average internet usage by a person over 15 years is 69 minutes a day, or 8.05 hours a week (ABS 2008a). Forty-eight percent of victims in the current survey spent 10 or more hours a week on the internet, which might be indicative of increased risk of victimisation for those with above-average use of the internet.

In relation to internet security, AusCERT's (2008) *Home Users' Computer Security Survey* found that 94 percent of those surveyed had anti-virus software installed, 86 percent used a firewall and 42 percent used anti-phishing tools. The present research found similarly high levels of use of internet security measures in place, although, of course such security measures cannot provide a perfect solution to receipt of scams.

Conclusions

This research provides evidence of a number of aspects of advance fee fraud victimisation that may be important in developing prevention strategies. The first relates to the fact that it is possible to identify large numbers of victims of scams simply by examining financial transactions sent to high-risk countries. Nearly 10 percent of all those who were sent the survey provided responses that showed they were victims of some form of advance fee fraud. This is almost double the current national prevalence rate for all forms of personal fraud of five percent (ABS 2008c).

Given the substantial under-reporting of fraud (ABS 2008c), it can be assumed there was a degree of under-reporting by survey respondents and thus the 'strike rate' for identifying victims may be even higher. Fraud prevention initiatives could make use of the fact that some overseas funds transfers are more likely than others to involve scam payments. Senders could, for example, be provided with targeted information about the risks involved in proceeding with such transfers. There are some obvious limitations to this approach—clearly not all advance fee fraud offenders are based in Nigeria and not all use the international funds transfer service that was used to select the current survey respondents. Nonetheless, providing users of these services with a simple 'self assessment' for potential risks might be a useful crime prevention strategy. This kind of strategy would be enhanced by one of the features of advance fee fraud that is clearly evident from these survey results—that victims are usually in contact with offenders over an extended period and their financial losses accumulate over time. Thus, there may be opportunities to provide advice at several stages in this process that may at least limit victims' losses.

Another interesting finding was the prevalence of dating scams originating from social networking and 'dating' websites. The largest group of victims was involved in dating scams and as a group their losses were substantially higher than those of any other form of scam. Effective crime prevention needs to counter the psychological strategies used by fraudsters who seek to manipulate the altruistic tendencies of victims. For other advance fee scams, the essence of the crime prevention message may be 'if an offer seems to be too good to be true, it probably isn't true'. However, in the case of dating scams, the counter-strategy is more problematic as the fraud is based on the development of a 'romantic' or other personal relationship that may initially appear to be harmless. Emotional involvement may also make it very difficult to convince the victim of the deception involved.

Another aspect of scam victimology that has direct relevance for crime prevention is the higher vulnerability of older people. Older (55 years or more) people accounted for four in 10 victims of other advance fee scams. It is unclear whether this heightened vulnerability of older people is the result of

Dr Stuart Ross is Senior Fellow at the University of Melbourne School of Social and Political Sciences. Dr Russell G Smith is the Principal Criminologist at the AIC.

General editor, *Trends & issues in crime and criminal justice* series:
Dr Adam M Tomison, Director,
Australian Institute of Criminology

Note: *Trends & issues in crime and criminal justice* papers are peer reviewed

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

ISSN 0817-8542 (Print)
1836-2206 (Online)

GPO Box 2944
Canberra ACT 2601, Australia
Tel: 02 6260 9200
Fax: 02 6260 9299

Project no. 0151
Ethics approval no.PO-135
Dataset no. 101

greater naivety about the internet (eg placing greater trust in identity information or documents provided over the internet), lower social connectivity (so that there is less likelihood that the fraudulent relationship is exposed to others before it develops) or simply due to lack of knowledge of the true risks associated with the venture. In any case, there is clearly a need to have crime prevention strategies tailored specifically to the needs of older Australians.

Acknowledgements

The authors acknowledge the contributions to this research made by Michael Hall and Wayne Bastin from Victoria Police, Carolyn Budd, former Research Officer at the AIC and Kavisha Mann, Masters student at University of Melbourne.

References

All URLs correct at May 2011

AusCERT 2008. *Home user computer security survey*. Brisbane: AusCERT. https://www.auscert.org.au/

Australian Bureau of Statistics (ABS) 2008a. *Household use of information technology, Australia, 2007–08*. cat. no. 8146.0. Melbourne: ABS

Australian Bureau of Statistics (ABS) 2008b. *National survey of mental health and wellbeing: Summary of results*. cat. no. 4326.0. Canberra: ABS

Australian Bureau of Statistics (ABS) 2008c. *Personal fraud 2007*. cat. no. 4528.0. Melbourne: ABS

Cohen L & Felson M 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44: 588–608

Gottfredson M & Hirschi T 1990. *A general theory of crime*. Stanford: Stanford University Press

Holtfreter K, Reisig MD & Pratt TC 2008. Low self-control, routine activities, and fraud victimization. *Criminology* 46(1): 189–220

Hutchings A & Hayes H 2009. Routine activity theory and phishing victimisation: Who gets caught in the 'net'? *Current Issues in Criminal Justice* 20(3): 433–452

Internet World Stats 2010. *Internet usage and population statistics for Oceania*. http://www.internetworldstats.com/stats6.htm

Lee J & Soberon-Ferrer H 1997. Consumer vulnerability to fraud: influencing factors. *Journal of Consumer Affairs* 31: 70–89

Mathur A & Moschis GP 1995. Older consumers' vulnerability to bait-and-switch. *Advances in Consumer Research* 22: 674–679

NASD Investor Education Foundation 2006. Investor fraud study final report. Washington DC: Consumer Fraud Research Group. http://www.finrafoundation.org/web/groups/foundation/@foundation/documents/foundation/p118422.pdf

Office of Fair Trading 2006. *Research on impact of mass marketed scams*. London: OFT. http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft883.pdf

Rollings K 2008. *Counting the costs of crime in Australia: A 2005 update*. Research and public policy series no. 91. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/81-99/rpp91.aspx

Smith RG & Budd C 2009. Consumer fraud in Australia: Costs, rates and awareness of the risks in 2008. *Trends & Issues in Crime and Criminal Justice* no. 382. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi382.aspx

Smith RG, Holmes MN & Kaufmann P 1999. Nigerian advance fee fraud. *Trends & Issues in Crime and Criminal Justice* no. 121. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/121-140/tandi121.aspx

Titus RM, Heinzelmann F & Boyle JM 1995. Victimisation of persons by fraud. *Crime and Delinquency* 41(1): 54–72

Titus RM & Gover AR 2001. Personal fraud: The victims and the scams. *Crime Prevention Studies* 12: 133–151

Trahan A, Marquart JW & Mullings J 2005. Fraud and the American dream: Toward an understanding of fraud victimisation. *Deviant Behaviour* 26: 601–620

Ultrascan 2008. *419 advance fee fraud: The world's most successful scam*. http://www.ultrascan.nl/assets/applets/2007_Stats_on_419_AFF_feb_19_2008_version_1.7.pdf

Van Wyk J & Benson ML 1997. Fraud victimisation: Risky business or just bad luck? *American Journal of Criminal Justice* 21(2):163–179

Van Wyk J & Mason KA 2001. Investigating vulnerability and reporting behaviour for consumer fraud victimisation: Opportunity as a social aspect of age. *Journal of Contemporary Criminal Justice* 17: 328–345

Online resources

International

http://www.aic.gov.au/crime_community/victims/victimsorganisations.aspx

http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html

http://www.attorneygeneral.gov.uk/nfa/Pages/default.aspx

Government

http://www.ag.gov.au/agd/WWW/ncphome.nsf/Page/Financial_Crime

http://www.voc.sa.gov.au/

Non-government

http://www.victimsupport.org.au/

http://www.vocal.org.au/

Private sector

http://www.antiphishing.org/consumer_recs2.html