Trends & issues
in crime and criminal justice

No. 474 May 2014

Australian Government
Australian Institute of Criminology

Challenges of responding to online fraud victimisation in Australia

Cassandra Cross, Russell G Smith & Kelly Richards

Foreword | *Online fraud occurs when an individual or a business responds in some manner to an unsolicited invitation received via the internet and suffers financial or other detrimental effects as a result. In 2010–11, the Australian Bureau of Statistics (2012) found that over 1.2 million Australians (6.7% of the population aged 15 years and over) had been a victim of personal fraud, losing approximately $1.4b in the preceding 12 months. More than half of these victims (55.7%) were contacted via the internet or email (online victimisation). In addition to monetary losses, victims of online fraud suffer serious psychological, emotional, social and even physical problems as a consequence of their victimisation. This paper explores the challenges of responding to online fraud victimisation in Australia and describes some of the specific support services that have recently emerged to support victims of this crime.*

Adam Tomison Director

The Australian Bureau of Statistics (2012: np) categorises personal fraud as being either identity fraud or a consumer scam. A *consumer scam* is a fraudulent invitation, request, notification or offer, designed to obtain someone's personal information or money, or otherwise obtain a financial benefit by deceptive means. *Identity fraud* involves the theft of an individual's personal details without their consent and includes both identity theft and credit or bank card fraud (ABS 2012: np). For the purposes of this paper, *online fraud* is defined as *the experience of an individual who has responded via the internet to a dishonest invitation, request, notification or offer by providing personal information or money that has led to a financial or non-financial loss or impact of some kind*. To fall within this definition, an individual must have received an unsolicited invitation via the internet and responded in some way that has led to a loss or other negative impact. While the loss need not necessarily be monetary in nature, cases in which individuals reply to fraudulent requests merely to solicit more information but without incurring a loss or other negative impact, are excluded from the current discussion.

There are many different types of online fraud, although almost all involve so-called 'advance fee' schemes entailing unsolicited invitations, which offer some benefit or reward that will be provided in return for assistance and the payment of a fee in advance of receiving the benefit or reward. Sometimes the promised reward is considerable, with invitations mentioning millions of dollars that will be provided in return for a small advance payment of a few hundred dollars. These include the infamous West African frauds in which assistance is sought to move stolen funds from Africa to a safe country in return for a proportion of the capital sum.

Lottery fraud, inheritance schemes and romance fraud all feature the common element of a requirement to transfer funds to the offender in return for receipt of lottery winnings, an inheritance, or a promised romantic relationship, respectively (Ross & Smith 2011). Other types of online fraud seek personal information (often bank account details and evidence of identity information) that are then used to withdraw funds from the victim's bank account

without permission (Cross 2012). Still other types of fraud simply employ the internet as a medium to perpetrate traditional frauds such as investment fraud, market manipulation, or Ponzi scheme, which offer impossibly high returns on funds invested with dividends paid out of capital received for investment from other victim investors.

A range of technological devices and procedures are used in connection with online fraud—as described by the UK Sentencing Council (Kerr et al. 2013)—including:

- *Phishing*—when consumers are tricked into transmitting financial information to a fraudulent website where the information is later housed for use in fraudulent activities;
- *Pharming*—in which victims' computer systems are compromised via hacking or malware, or where software redirects victims to fake websites where they are asked to enter their details;
- *Skimming*—where personal information is 'skimmed' from plastic cards by devices covertly attached to card readers; and
- *Malware*—when malicious software such as viruses are used or installed on computers in order to alter functions within programs and files (Kerr et al. 2013: 22).

There are also a number of new and emerging techniques:

- *SMiShing*—personal information obtained via SMS;
- *Vishing*—personal information obtained via phone;
- *Malware*—used to collect personal information via Smartphones;
- *Spear-phishing*—highly targeted spam;
- *Koobface on social media*—where victims are sent messages via their social media site with a virus;
- *Social phishing*—whereby the perpetrator gains the trust of an individual and accesses their friend list or as a phisher gains unauthorised access to a user's account and starts sending spam to the user's direct contacts;
- *Keylogging viruses*—these viruses capture login details or passwords for bank accounts, for example, which can then be used or sold;
- *Fraud* in virtual platforms such as 'Second Life'; and
- *Online rental scams*—whereby fake rental flats are advertised online and victims send personal information and/or deposit payments to prove they can pay the rent (Kerr et al. 2013: 23).

While the types of approaches that offenders use are numerous, all are directed at obtaining personal information that can be used to extract funds or other value from their targets.

Prevalence of victimisation

A number of surveys have been conducted in Australia to quantify the nature and extent of online fraud and internet-enabled consumer fraud. In the victimology literature, there is some debate concerning the appropriateness, or otherwise, of describing those who have experienced fraud as 'victims' as this tends to connote a state of vulnerability or helplessness that some who have experienced fraud might not possess (Goodey 2005). The present paper will, nonetheless, use this terminology as it is conventionally adopted in the consumer fraud literature.

Large-scale national surveys of householders conducted by the Australian Bureau of Statistics (2012, 2008) have found that the proportion of persons aged 15 years and over who have experienced personal fraud over the preceding year increased from five percent of the population in 2007 to 6.7 percent in 2010–11. This represents an increase of 382,100 victims who reported an increase in losses from $977m in 2007 to $1.4b in 2010–11. Three in five victims of personal fraud (60% or 713,600 persons) lost money; an average of $2,000 per victim who incurred a financial loss. The median loss for personal fraud was $300.

Each year since 2007, the Australian Institute of Criminology (AIC) has collected information on consumer fraud by conducting a self-selected, online survey of Australians who have received scam invitations during the preceding 12 months. In 2012, a high proportion of the 1,576 survey respondents reported receiving a scam invitation (95%). Almost a quarter of those who had received an invitation (23.5%) responded in some way, with eight percent of those who had received an invitation losing money—approximately $8,000 per person or $846,170 in total. The most prevalent scam type involved fraudulent lotteries and email was the most common scam delivery method, with 72 percent of respondents reporting having received a scam this way (Jorna & Hutchings 2013).

Of the 231 victims who had lost personal details or suffered a financial loss as the result of the scam, 142 (61.5%) identified themselves as female, 85 (36.8%) identified themselves as male and four (1.7%) declined to reveal their gender. Therefore, of the respondents who disclosed their gender, 16.5 percent of the 861 female respondents experienced victimisation, compared with 12.4 percent of the 685 males. Respondents in the age categories '35 to 44 years' and 'over 65 years' reported the highest proportion of victimisation (16.5% of total respondents within those age categories). In 2012, respondents in the income category $20,000 to less than $40,000 reported the highest proportion of victimisation (20% of total respondents within that income category; Jorna & Hutchings 2013).

In 2012, 69 percent of the total sample reported their experience to at least one person or organisation, most often family and friends (43% of the total sample). The most common reasons for not reporting scams were 'unsure of which agency to contact' (40% of the total sample), 'I didn't think anything would be done' (32%) and 'not worth the effort' (29%; Jorna & Hutchings 2013).

Other recent research by the Australian Crime Commission (2012), undertaken in collaboration with the AIC, examined serious and organised investment fraud in Australia, or the solicitation of investment in non-existent or essentially worthless shares and other securities. It was found that between January 2007 and April 2012, more than 2,600 Australian were victimised with losses in excess of $113m.

In 2012, the Australian Competition and Consumer Commission received 83,803 scam-related contacts with consumers and businesses who had suffered just over $93.4m in financial losses. Online shopping scam reports have increased by 65 percent since 2011 to over 8,000 contacts and more than $4m in reported losses (ACCC 2013).

Finally, in 2013 the Office of the Australian Information Commissioner (2013) conducted a survey of community attitudes to privacy that sought to measure Australians' changing awareness and opinions about privacy, as well as their expectations in relation to the handling of their personal information. In respect of personal information, Australians believed that the biggest privacy risks concerned online services—including social media sites. Almost a quarter of respondents (23%) felt that the risk of identity fraud and theft was the biggest, followed by data security (16%) and the risks to financial data in general (11%).

The Office of the Australian Information Commissioner asked adult Australians if they had ever been the victim of identity fraud or theft or whether they know someone who has. One in eight (13%) said that they had been a victim themselves (up from 9% in 2007) and one in five (21%) said it had happened to someone they knew (up from 17% in 2007). In the 2013 survey, a third (33%) of the population had either been the victim of identity fraud or theft or knew someone who had been victimised in this way (OAIC 2013: 46).

The impact of victimisation

It is difficult to assess the impact of fraud on a group of victims who may not realise that they have been victimised or who may not feel confident enough to make a report to the police. Consequently, little is known about the impact that fraud has on victims and their associated needs. Nonetheless, a small number of studies has been conducted overseas and this research is uniform in finding that fraud victims 'share many of the same devastating outcomes as their counterparts who have suffered serious violent crime' (Marsh 2004: 127; see also Button, Lewis & Tapley 2009a; Deem 2000; Deem, Nerenberg & Titus 2013). These studies indicate that the harm suffered by fraud victims extends far beyond any financial loss to physical harm, emotional/psychological trauma, a sense of betrayal and relationship breakdown (ASIC 2002a, 2002b; Button, Lewis & Tapley 2009a, 2009b; Cross 2012; Deem 2000; Ganzini, McFarland & Bloom 1990; Titus, Heinzelmann & Boyle 1995). In extreme cases, victims of online fraud have even resorted to self-harm or suicide (see Box 1).

In the United Kingdom, one study involved interviews with over 750 victims of fraud to ascertain the impact of the crime on their wellbeing (Button, Lewis & Tapley 2009a). The findings indicated that:

- 68 percent reported strong feelings of anger;
- 45 percent claimed the financial loss had a high effect on their emotional wellbeing;
- 44 percent recorded feelings of stress;
- 37 percent recorded a profound psychological/emotional impact; and
- a smaller proportion of victims reported problems in their relationships, mental or physical health issues or feelings of suicide (Button, Lewis & Tapley 2009a).

In Australia, there is limited research specifically examining the nature of victimisation as it relates to victims of personal fraud. The Australian Securities and Investment Commission (2002a; 2002b) conducted a study of telemarketing fraud victims and found that the loss for 'investors' (or victims) 'was not just a financial betrayal but also emotional betrayal. Thus investors described feelings of anger, stupidity, betrayal, confusion and shock' (ASIC 2002a: 63).

In relation to online fraud, the Queensland Police Service has documented the impact of fraud on seniors (n=85) who had received fraudulent email requests. It was found that victims experienced a deterioration of physical health and wellbeing, including depression (Cross 2012). Ross and Smith's (2011) study of 202 victims of advance fee frauds in Victoria found that the most frequently reported impact on victims was financial hardship (54% of victims), followed by emotional trauma (43%), loss of confidence in other people (40%) and marital or relationship problems (12%).

Re-victimisation also poses a significant problem for victims of online fraud. Once a person has responded positively to a fraudulent request for personal details or money, their details may be included on what is known as a 'sucker's list' (NFA 2008: 44). This list is then sold by one offender to other offenders, who attempt to defraud the victim through another scheme or engage in 'recovery fraud' (in which the offender offers to recoup the original amount of money lost by the victim, for a fee and in turn defrauds the victim again; NFA 2008). This can lead to a group of chronic victims, who are financially devastated by multiple offenders on multiple occasions.

Numerous cases have also been identified in which victims of online fraud have been deceived into travelling abroad—usually to meet those whom they believe to be potential business or romantic partners—and have been abducted by perpetrators in an attempt to exact further money from the victim's family (see Benin: US 'internet scam victim' freed by police. *BBC News* 1 June 2012. http://www.bbc.co.uk/news/world-africa-18293883; American kidnapped in Benin victim of Internet scam. *Vanguard* 30 May 2012. http://www.vanguardngr.com/2012/05/american-kidnapped-in-benin-victim-of-internet-scam/; Smith 2012). In some cases, victims have been robbed and killed. For example, 67 year old Perth woman Jette Jacobs was found dead in South Africa on 9 February 2013 after she travelled there to meet a man she had commenced a long-distance relationship with via an online dating site (Powell 2013). Ms Jacobs had already sent over $100,000 to the man she had met online including $20,000 to assist him with travelling to meet her in South Africa. Police are treating her death as suspicious and believe that she was a victim of an overseas fraud (Powell 2013). As recent AIC research has shown, fraudulent online behaviour has even led to instances of women being trafficked into domestic servitude (Lyneham & Richards 2013).

Box 1 Suicide and self-harm following online fraud victimisation

Nigerian fraud

A 23 year old Chinese student committed suicide after she lost more than £6,000 in an online lottery fraud after arriving in England to study at the University of Nottingham. The Nottingham Coroner, Dr Nigel Chapman, reported a suicide verdict and stated that '[the victim] has taken her own life because of a scam from Nigeria' (Web scam drove student to suicide. *BBC News* 2 May 2008. http://news.bbc.co.uk/2/hi/uk_news/england/nottinghamshire/7380093.stm).

Lottery fraud

In 2009, a 48 year old man committed suicide by pouring petrol over himself and setting himself on fire following an online lottery fraud. He had been in debt and had been relying on the winnings from the lottery to ease this financial pressure. The Deputy Coroner, Dr Colin Lattimore, recorded a verdict of suicide and stated that he had 'killed himself while suffering from depression, caused by what would have been good news but turned out to be very bad news' (Corbin 2010).

Romance fraud

In 2009, a 58 year old UK man committed suicide by lying on train tracks after losing £82,000 in an online romance fraud. The twice-divorced man had been deceived into paying for numerous medical bills for a woman he believed he had come to know over the internet (Brooke 2010).

Ponzi investment fraud

In Sri Lanka, over 9,000 investors in the Golden Key Credit Card Company lost Rs26b (US$260m) in the largest financial Ponzi scam to affect the country. Although the Central Bank of Sri Lanka has appointed a Task Force to recover a proportion of the funds invested, many lost their life savings leading to five suicides (Shauketaly 2013).

Phishing fraud

An Australian woman recently attempted suicide on two occasions after she lost $300,000 due to a 'phishing' fraud (Mandel 2013).

The most serious consequence of online fraud on victims is self-harm, on occasions leading to suicide. Internationally, a number of incidents of online fraud have led to victims taking their own lives following loss of life savings or important relationships. Some examples are shown in Box 1.

Online fraud victims' rights in Australia

While historically, crime victims have tended to be marginalised in the criminal justice system and viewed primarily as witnesses or complainants (Burgess, Regehr & Roberts 2013; Erez & Roberts 2013), there have been recent moves towards recognising victims' rights and addressing their needs in Western criminal justice systems (Burgess, Regehr & Roberts 2013).

Internationally, the United Nations General Assembly (1985) Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power ('the Declaration') was a pivotal step in recognising victims of crime and their needs. While the Declaration is non-binding, it has influenced the development of victims' rights' policies in Australia, where victims' rights are now provided for under the *National Framework of Rights and Services for Victims of Crime 2013–2016* (SCLJ 2013) and in each jurisdiction's victim legislation. However, assistance and services that are available are targeted at victims of violent crime, leaving victims of crimes such as online fraud with few avenues of counselling or compensation.

In Victoria in 2004, the Parliamentary Drugs and Crime Prevention Committee observed that:

> the services provided by victim support agencies, which have traditionally focused on the victims of violent crime, need to be extended to the victims of economic and white-collar crime as well. One submission received by the Committee found traditional victim support agencies of no help whatsoever in dealing with the victims of white-collar crimes (Parliament of Victoria 2004: 298–299).

Further, while victims of online fraud theoretically have certain rights that apply to all victims, their unique characteristics often mean that these rights have little impact in practice. For example, in most jurisdictions, victims have a right to be informed about the investigation, arrest, bail, trial and sentencing of 'their' offender. Victims also usually have the right to present a Victim Impact Statement during the sentencing of 'their' offender. In the case of online fraud however, the majority of victims are defrauded by an overseas-based offender. When a victim residing in Australia is defrauded by an overseas-based offender, state and federal police agencies can offer only limited assistance. They may take details of a complaint from the victim and forward it to the relevant policing authority overseas; however, it is then at the discretion of that police agency whether or not action will be taken. As a consequence, the majority of online fraud victims do not have their cases investigated by police and therefore are not in a position to make use of the services and procedures available to complainants of other types of crime. This can lead to immense frustration on the part of victims, who feel powerless at the seemingly arbitrary nature of criminal justice agencies to deal with their complaint (see Finklea 2013).

Finally, while all crime victims have the right to be treated with courtesy, compassion and respect, for many online fraud victims, this can be problematic. As Cross's (2013) examination of 85 seniors in Queensland found, victims of online fraud are often characterised as being greedy and gullible individuals who are responsible for their own victimisation. Similarly, Button, Lewis and Tapley's (2009b) UK research found that many online fraud victims face a lack of empathy and understanding when they recount their victimisation to officials in the criminal justice system and meet with negative and derogatory responses.

In summary, while victims of online fraud are recognised as victims in international and national frameworks and domestic legislation, they are often unable to participate in the criminal justice system and receive support in a way that other victims are.

Box 2 Support services for victims of online fraud

Fraud victim support groups

In 2010, the Queensland Police Service established a face-to-face support group dedicated to victims of fraud. This was the first of its kind within Australia. The group, which meets on a bi-monthly basis in Brisbane, provides a safe space in which victims of fraud, including online fraud, are able to share their experiences with other victims. The purpose of the support group is to:

- encourage victims to speak up and give them back their voice;
- help victims recover their self-esteem;
- educate the community about fraud and its effects;
- provide skills to community members to help prepare them against online predators;
- provide an environment in which victims will not be judged; and
- turn 'victims' into 'survivors' through self-empowerment (QPS 2012).

In late 2013, South Australia also established a support group, the result of a partnership between the South Australian Police and Victim Support Services (VSS). This support group is being led by VSS and is in its infancy (personal communication, VSS).

ActionFraud/Victim Support (United Kingdom)

All victims of crime in the United Kingdom can access support through Victim Support, a national charity largely staffed by volunteers. Within the United Kingdom, there is a central reporting agency for all fraud complaints, called ActionFraud. When reporting to ActionFraud, victims of online fraud are asked about the severity of the impact of their crime and whether they would like to be referred to Victim Support for further assistance. If an individual agrees, a referral is made to Victim Support. Contact by Victim Support is initiated with the victim via a telephone call, with the offer of emotional support or practical help. If required, face-to-face support can be offered through a network of agencies across the United Kingdom (Cross 2012).

Senior busters (Canada)

The Canadian Anti-Fraud Centre is the central fraud reporting authority in Canada and includes 'SeniorBusters', a support program operating specifically for older persons who have been a victim of fraud or who are seen to be at risk of fraud victimisation. Like the UK's ActionFraud service, SeniorBusters is staffed by approximately 50 volunteers (who are seniors themselves) who help to increase the awareness of fraud among seniors, as well as offering support to victims and others vulnerable to fraud (usually as a result of their lodging of a complaint to the Canadian Anti-Fraud Centre; Cross 2012).

TransUnion (United States)

TransUnion's Fraud Victims Assistance Department in the United States is the credit industry's first department dedicated to help victims of credit fraud. The Department works with consumers, credit grantors, law enforcement officials and other credit reporting companies to help investigate and prevent credit fraud. The Department helps victims identify fraudulent accounts, advises them of the creditors that need to be informed of the fraud and works to remove fraudulent accounts from credit files (TransUnion 2013). In Australia, similar services are provided for a fee by *Secure Sentinel, part of Veda (2013), formerly the Credit Reference Association*

Support services for victims of online fraud

Recently, however, some support services have been established in a number of jurisdictions that seek to assist victims of fraud in general and online fraud in particular. The services provided include, inter alia, the *provision of:*

- individual case workers;
- up-to-date information concerning the progress of the case;
- service providers who adopt a more sympathetic approach;
- staff trained in how to deal with victims;
- better and clearer information;
- assistance with restitution and compensation; and
- services that aim not to re-victimise individuals (see Button, Lewis & Tapley 2009b).

Examples of services available in Australia, the United Kingdom, Canada and the United States that have been specifically designed to assist victims of fraud are set out in Box 2.

Conclusion

Victims of online fraud are often unable to obtain assistance from criminal justice agencies as suspects are often located overseas, making investigation and prosecution difficult or impossible. In addition, victim support services are often focused on those who have experienced violent crimes as opposed to financial losses. Such lack of support can often exacerbate the impact that being a victim of online fraud entails. In particular, failure to recognise their status as legitimate victims of crime can lead to isolation and alienation of such victims, many of whom require the same support services that other victims can secure.

While victims of online fraud experience levels of harm similar to other victims of crime, they are often not seen as being legitimate victims. For most online fraud victims, this stems from the unique characteristics of the crime perpetrated against them that makes conventional criminal justice responses difficult or impossible.

While the need to provide support services for victims of online fraud is clear, the very few dedicated services that are available show that further attention to the problem is needed, both by government agencies as well as by non-governmental bodies. The provision of coordinated and centralised reporting, such as that proposed in the Australian Cybercrime Online Reporting Network, could assist victims of online fraud when the Network becomes operational. Further research into specifics around the needs of online fraud victims is currently being undertaken by the authors to address the issues identified in this paper and further to inform the evidence base on this important topic.

References

All URLs are correct at February 2014

Australian Bureau of Statistics (ABS) 2012. *Personal fraud 2010–2011*. ABS cat. no. 4528.0. Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4528.0Main+Features12010-2011?OpenDocument

Australian Bureau of Statistics (ABS) 2008. *Personal fraud, 2007*. Canberra: ABS. http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/866E0EF22EFC4608CA2574740015D234/$File/45280_2007.pdf

Australian Competition and Consumer Commission (ACCC) 2013. *Targeting scams: Report of the ACCC on scam activity 2012*. Canberra: ACCC

Dr Cassandra Cross and Dr Kelly Richards are Lecturers in the School of Justice, Queensland University of Technology.

Dr Russell G Smith is Principal Criminologist at the AIC.

SUPPORT AND ADVICE FOR VICTIMS OF ONLINE FRAUD ARE AVAILABLE FROM Lifeline (Ph: 13 11 14), SANE Helpline (Ph: 1800 187 263) and Grief Line (Ph: 03 9596 7799).

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: 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

Australian Crime Commission (ACC) 2012. *Serious and organised investment fraud in Australia*. Canberra: ACC

Australian Securities and Investment Commission (ASIC) 2002a. *Hook, line and sinker: Who takes the bait in cold calling scams?* Canberra: ASIC

Australian Securities and Investment Commission (ASIC) 2002b. *International cold calling investment scams*. Canberra: ASIC

Brooke C 2010. Lonely divorcee kills himself after falling for £82,000 internet dating con. *Daily Mail* 2 February. http://www.dailymail.co.uk/news/article-1247774/Divorcees-train-suicide-82-000-internet-date.html

Burgess A, Regehr C & Roberts A 2013. *Victimology: Theories and applications*, 2nd ed. Burlington, MA: Jones and Bartlett Learning

Button M, Lewis C & Tapley J 2009a. *A better deal for fraud victims*. London: Centre for Counter Fraud Studies

Button M, Lewis C & Tapley J 2009b. *Fraud typologies and victims of fraud: Literature review*. London: Centre for Counter Fraud Studies

Corbin J 2010. A mysterious email and a split-second mistake: That's all it took for internet gangsters to hijack my life... *Daily Mail* 15 January. http://www.dailymail.co.uk/news/article-1243634/A-mysterious-email-split-second-mistake-Thats-took-internet-gangsters-hijack-life-.html

Cross C 2013. Nobody's holding a gun to your head: Examining current discourses surrounding victims of online fraud, in Richards, K & Tauri J (eds), *Crime, justice and social democracy: Proceedings of the 2nd international conference*. Brisbane: Queensland University of Technology: 25–32

Cross C 2012. *The Donald Mackay Churchill Fellowship to study methods of preventing and supporting victims on online fraud*. Available http://eprints.qut.edu.au/view/person/Cross,_Cassandra.html

Deem D 2000. Notes from the field: Observations in working with the forgotten victims of personal financial crimes. *Journal of Elder Abuse and Neglect* 12(2): 33–48

Deem D, Nerenberg L & Titus R 2013. Victims of financial crime, in Davis R, Lurigio A & Herman S (eds), *Victims of crime*, 4th ed. London: Sage: 185–210

Erez E & Roberts J 2013. Victim participation in the criminal justice system, in Davis R, Lurigio A & Herman S (eds), *Victims of crime*, 4th ed. London: Sage: 251–270

Finklea K 2013. *The interplay of borders, turf, cyberspace and jurisdiction: Issues confronting U.S. law enforcement*. Congressional Research Service. http://www.fas.org/sgp/crs/misc/R41927.pdf

Ganzini L, McFarland B & Bloom J 1990. Victims of fraud: Comparing victims of white collar crime and violent crime. *Bulletin of the American Academy of Psychiatry and Law* 18(1): 55–63

Goodey J 2005. *Victims and victimology: Research, policy and practice*. London: Pearson Longman

Jorna P & Hutchings A 2013. Australasian Consumer Fraud Taskforce: Results of the 2012 online consumer fraud survey. *Technical and background paper* no. 56. Canberra: Australian Institute of Criminology

Kerr J, Owen R, McNaughton Nicholls C & Button M 2013. *Research on sentencing online fraud offences*. London: Sentencing Council. http://sentencingcouncil.judiciary.gov.uk/docs/Research_on_sentencing_online_fraud_offences.pdf

Lyneham S & Richards K 2013. Human trafficking involving marriage and partner migration. *Research and public policy series* no. 128. Canberra: Australian Institute of Criminology

Mandel H 2013. Nigerian phishing scam victim attempted suicide twice. *Examiner* 26 May: http://www.examiner.com/article/nigerian-phising-scam-victim-attempted-suicide-twice

Marsh I 2004. *Criminal justice: An introduction to philosophies, theories and practice*. London: Routledge

National Fraud Authority (NFA) 2008. *The National fraud strategy: A new approach to combating fraud*. London: National Fraud Authority

Office of the Australian Information Commissioner (OAIC) 2013. *Community attitudes to privacy survey*. Canberra: Wallis Strategic Market & Social Research for OAIC

Parliament of Victoria. Drugs and Crime Prevention Committee 2004. *Inquiry into fraud and electronic commerce, final report*. Melbourne: Government Printer for the State of Victoria

Powell G 2013. Woman believed victim of online scam found dead. *ABC News* 5 March. http://www.abc.net.au/news/2013-03-04/woman-believed-victim-of-online-scam-found-dead/4551050

Queensland Police Service (QPS) 2012. *Police support victims of fraud*. 25 July: http://mypolice.qld.gov.au/blog/2012/05/29/police-support-victims-of-fraud/

Ross S & Smith RG 2011. Risk factors for advance fee fraud victimisation. *Trends & Issues in Crime and Criminal Justice* no. 420. Canberra: Australian Institute of Criminology. http://aic.gov.au/publications/current%20series/tandi/401-420/tandi420.html

Shauketaly F 2013. Ceylinco: Further payment to Golden Key depositors. *Sunday Leader* 4 November. http://www.thesundayleader.lk/2013/08/11/ceylinco-further-payment-to-golden-key-depositors/

Smith D 2012. South African police rescue Asian pair kidnapped in 419 scam. *The Guardian* 14 June: http://www.guardian.co.uk/world/2012/jan/13/south-african-police-419-scam

Standing Council on Law and Justice (SCLJ) 2013. *Annual report 2012–13*. http://www.sclj.gov.au/agdbasev7wr/sclj/sclj_annual_report.pdf

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

TransUnion 2013. *TransUnion fraud victim assistance department*. http://www.transunion.com/personal-credit/credit-disputes/fraud-victim-resources/fraud-victim-assistance.page

United Nations General Assembly (UNGA) 1985. *Declaration of basic principles of justice for victims of crime and abuse of power*. G.A. res. 40/34, annex, 40 U.N. GAOR Supp. (No. 53) at 214, U.N. Doc. A/40/53 (1985). http://www.unodc.org/pdf/compendium/compendium_2006_part_03_02.pdf

Veda 2013. *Secure sentinel*. http://www.veda.com.au/personal/secure-sentinel