Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

ISSN 1836-2206 (Online) | ISBN 978 1 925304 01 5 (Online)

No. 577 April 2019

Abstract | The pervasiveness of the internet and society's reliance on it for personal and business use has brought with it many benefits. However, for those who seek to defraud others, it has also provided new ways of identifying and targeting potential victims.

Online consumer fraud can take a variety of forms and can target anyone. It comes with substantial costs. The Australian Competition and Consumer Commission (ACCC) estimates that more than $90m was lost as a result of fraudulent activity in 2017 (ACCC 2018).

This report presents the findings of a study conducted by the Australian Institute of Criminology (AIC) with the support and cooperation of the ACCC's Scamwatch staff. The study sought to determine and quantify the factors that make individuals vulnerable to consumer fraud and that lead to their victimisation.

Predicting online fraud victimisation in Australia

Catherine Emami, Russell G Smith and Penny Jorna

The internet and the internet connectivity of our everyday lives have changed the way we perform a variety of everyday tasks, such as obtaining access to government services, shopping for goods and services, communicating with family and friends and how we obtain our entertainment (Stay Smart Online 2018). The development of wireless technology, smartphones, tablet PCs and other mobile devices has made it easier for people to access the internet for a range of activities from virtually anywhere and at any time (Holt & Bossler 2014). This has led to an increase in crime taking place online and has provided a larger pool of potential victims for criminals to target. Although it is difficult to know who will become a victim of online fraud, this report examines the differences between victims of online fraud and those who shop or socialise online but are not victimised. The objective was to isolate those critical personal and behavioural indicators that make some individuals more vulnerable to online fraud than others.

CRG CRIMINOLOGY RESEARCH GRANT

Online fraud takes place when an individual responds via the internet to 'a dishonest invitation, request, notification or offer by providing personal information or money that leads to a financial or non-financial loss or impact of some kind' (Cross, Smith & Richards 2014: 1). Examples of online fraud include dating or romance fraud, deceptive sales of products and services, dishonest investment schemes, lottery or inheritance schemes, working from home schemes (often a form of money laundering), or lottery fraud involving false prize draws or sweepstakes (Button et al. 2014; Button, Lewis & Tapley 2009; Chang 2008; Cross, Smith & Richards 2014). Syntactic methods of fraud that make use of malware, phishing, vishing or skimming often accompany fraudulent invitations and may mislead users into disclosing personal information, transferring funds, or having their personal information obtained electronically without their knowledge (Button et al. 2014; Chang 2008; Cross, Smith & Richards 2014).

Online fraud is a costly phenomenon not just in terms of its financial impact on business and government, but also because of the detrimental impact that it has on many of its victims. The total value of losses attributed to online consumer fraud in reports to the Australian Competition and Consumer Commission's (ACCC's) Scamwatch website, reports made to the Australian Cybercrime Online Reporting Network (ACORN) and those detected through scam disruption programs was more than $340m in 2017, an increase of $40m over 2016 losses (ACCC 2018).

It is possible for anyone to become a victim of online fraud. A number of researchers have observed that sociodemographic factors are not reliable predictors of fraud victimisation because the perpetrators of fraud target people from any background (Pratt, Holtfreter & Reisig 2010).

Previous research into characteristics of online fraud victims

In their study of individuals who had transferred money to Nigeria between April 2007 and March 2008, Ross and Smith (2011) noted that across studies, age was the only demographic variable that has consistently been found to have some impact on fraud victimisation, although the age group at highest risk differs between studies. For instance, Ross and Smith (2011) found that in their study, respondents aged 65 years or over were more likely to be a victim of advance fee invitations (such as lottery frauds), with victims between the ages of 45 and 54 years most likely to be victims of dating fraud. Victims aged between 18 and 24 years were more likely to be victims of online transaction fraud, while people aged between 35 and 44 years were least likely to be victims (Ross & Smith 2011).

Lee and Soberon-Ferrer (1997) also examined whether certain characteristics of victims increased their vulnerability to consumer fraud. They found that sociodemographic factors such as age, education and marital status influenced a person's vulnerability to consumer fraud, but that race and gender were not significant factors.

Jorna (2016) found that vulnerability was related to the type of fraud invitation, with significant relationships found between age and romance frauds (those aged 45–54 years were more likely to be victims) and income and work-from-home fraud (people earning less than $20,000 a year were more likely to be victims). The research also found that respondents aged 65 years and over were more likely to send money in response to a fraudulent invitation than other age groups.

Ross and Smith (2011) also found a statistically significant relationship between the type of fraud victimisation that individuals experienced and income levels. Victims who earned less than $20,000 were more likely to have been victims of advance fee fraud or online transaction fraud, while individuals earning between $20,000 and $40,000 were more likely to have been victims of dating fraud. Individuals who earned more than $40,000 were less likely to be fraud victims than those in other income level categories.

Negative life events

Certain negative life events have, however, been found to have an impact on the likelihood of individuals becoming victims of crime. This is particularly pertinent to consumer fraud victimisation, due to the impact that negative life events can have on an individual's cognitive judgment and their ability to subsequently process information and make sound decisions (Lee & Soberon-Ferrer 1997). Negative life events, such as those involving a loss of some kind, can place considerable psychological stress on individuals. Such stress may adversely affect an individual's risk-taking behaviour and impede their ability to manage consumer tasks if they are forced to make a decision during such a period of vulnerability (Chang & Chong 2010; Lee & Soberon-Ferrer 1997; Ross & Smith 2011).

It has been suggested that perpetrators of fraud actually make the most of the impact that negative life events can have on people's lives by relying on 'cognitive biases or errors in the mental process to initiate and execute their attacks and produce automatic emotional responses in their victims' (Atkins &Huang 2013: 24). Cross (2015) has made a similar observation, noting that fraudsters frequently rely on identifying a victim's weaknesses, which they then exploit to gain the desired benefit or reward.

While ageing can contribute to impairments in cognitive functioning, psychological, sociocultural and environmental factors have also been identified as playing a role (Lee & Soberon-Ferrer 1997). Indeed, this would appear to be supported by the findings of a study by Shadel, Pak and Sauer (2014) which found victims of fraud were more likely to report experiencing negative life events such as a negative change in financial status, divorce, or a serious illness or injury to themselves compared to non-victims. Ross and Smith (2011) have also suggested that unfortunate life events can have a negative impact on the ability of individuals to make sound judgements, which in turn can increase their chances of falling victim to fraud, including online fraud.

Other studies have also found a link between fraud victimisation and recent experiences of negative life events. For instance, Anderson (2013) found that individuals who had experienced a serious negative life event such as a divorce, the death of a family member or close friend, a serious injury or illness in their family, or the loss of a job, were more than two-and-a-half times as likely to have experienced fraud compared with those who had not suffered these types of negative events. Those who had experienced a serious negative life event were also almost four times more likely to have fallen victim to debt-related fraud (ie advance fee loans, mortgage and credit relief schemes). They were three times as likely to have been a victim of a fraudulent prize promotion compared with those individuals who had not experienced these negative life events (Anderson 2013).

Similarly, Ross and Smith (2011) found that 45 percent of online fraud victims in their study had suffered a personal financial crisis, with approximately 40 percent experiencing depression at some point in the previous five years, and 22 percent suffering a serious illness. While it is unclear whether the serious life events experienced by a number of the online fraud victims in Ross and Smith's 2011 survey occurred prior to, or after, they fell victim to fraud, it is possible that the victims' vulnerability to online fraud victimisation may have been influenced by such events.

Psychological factors in online fraud

It is difficult to identify precisely the factors that may contribute to a person's susceptibility to falling victim to online fraud. As noted by Cross (2015), victims of online fraud are often viewed in a negative way, with the victims' perceived ignorance or greed being to blame for their victimisation. However, Atkins and Huang (2013) have suggested that contrary to the belief that people fall victim to fraudulent invitations due to ignorance or greed, a person's vulnerability to online fraud is actually linked to the ability of fraudsters to skilfully manipulate human weaknesses to achieve their desired objectives. This use of manipulative and deceptive techniques to persuade people to perform particular actions has been described as 'social engineering' (Atkins & Huang 2013; Nhan, Kinkade & Burns 2009).

Fraudsters use many forms of social engineering to achieve their objectives, including impersonation, attraction, invoking sympathy or pity, assertion of authority, mimicking, persuasion, creating urgency, implying scarcity, and bribery (Atkins & Huang 2013; Chang 2008). The UK Office of Fair Trading (2009) while examining the psychology of scams found two main reasons for the success of some scams—appeals to trust and authority and visceral triggers. Button et al. (2014) also found some scams used authority and legitimacy to convince people to engage, such as the use of professional looking websites, and referencing well-known companies.

Methodology

The present study aimed to identify the characteristics of those who respond to online invitations that could increase their risk of fraud victimisation. The methodology used in this study replicated a similar study that was conducted by Ross and Smith (2011).

Questions were asked about:

- consumer activities including payments made overseas in response to requests from people online;
- any consequences experienced as a result of sending money overseas;
- whether the respondents reported what happened, and to whom;
- background information about respondents including their age, gender, residence, income, language at home, Indigenous background, education, computer usage and computer security measures used, and certain psychological and behavioural characteristics; and
- recent life experiences including major life events during the preceding five years such as bankruptcy, death of a close family member or friend, experience of depression, loss of job, relationship break-up, serious illness, accident or criminal victimisation.

Results from two independent, exactly-matched samples were considered—those who were victims of online fraud, and those who were not. This paper focuses on the extent to which the personal and lifestyle factors examined were associated with fraud victimisation. Other findings are reported in Emami, Smith and Jorna (forthcoming).

Sampling framework

Two sampling frameworks were used to ensure good representation in both the victim cohort and the non-victim cohort. This would allow the differences between the two groups to be analysed.

The ACCC identified the victim sample based on individuals who had lost at least $300 and made a report on the ACCC's Scamwatch website after 1 January 2013. This date was chosen in the hope that victims would be better able to remember their victimisation and its subsequent impact if it took place within the last two years. Also, contact details for participants needed to be as current as possible.

Between May and August 2015 the ACCC sent 5,308 emails inviting individuals to complete the AIC's questionnaire. A total of 566 completed questionnaires were received—a completion rate of 10.7 percent. Although this rate appears quite low, it is consistent with other similar studies (Ross & Smith 2011).

The same questionnaire used with the victim sample obtained from the ACCC was given to a separate independent sample of 1,271 individuals who had subscribed to an online research panel provided by i-Link Research Solutions, a commercial market research provider. The final non-victim sample size was 321.

To form part of the control group sample, respondents needed to meet the following criteria:

- they have not made a report to the ACCC about goods or services that they had attempted to buy online from overseas since 1 January 2013;
- they are a resident in Australia; and
- they have sent money overseas and been completely satisfied with the goods or services received in exchange for that money.

Matched data analysis

To determine whether there were differences between victims and non-victims that might result in some respondents becoming victims of online fraud, a comparison group of sufficient size and comparability was selected. This was a matched group from existing samples of victims and non-victims. This type of study was adapted from case-control studies used in epidemiology research, where an outcome (usually a disease) is already known and researchers work backwards to determine how that outcome was reached (Pearce 2016).

The comparison group of non-victims was then matched with victims on:

- gender (exact match);
- age (exact match); and
- highest level of education attained (exact match).

These factors were included as they had been shown to have an impact on victimisation (Ross & Smith 2011; Titus & Gover 2001; Whitty 2017). This left a sample of 352 respondents, 176 victims of online fraud and 176 non-victims of this kind of fraud.

Findings

This study identified a small number of statistically significant findings that may be useful in guiding the future development of targeted awareness-raising and online fraud prevention programs.

What makes a victim of online fraud?

Respondents were identified as victims from the survey data if they had sent money overseas in the two years prior to completing the survey and they were dissatisfied with what they received in return.

The research initially examined the differences between victims and non-victims and their activities online. As all participants must have transferred money overseas in the two years prior to completing the survey, part of the research was to determine what non-victims did differently to victims to explain why some people were more likely to become victims of online fraud compared with others.

Victims were more likely to send money overseas in response to contact they received from a stranger to them, ($\chi^2(2,352)=31.50$, $p<0.001$). This is a fundamental difference between victims and non-victims (Table 1).

Table 1: Money sent in response to contact from a stranger (via internet), victims and non-victims

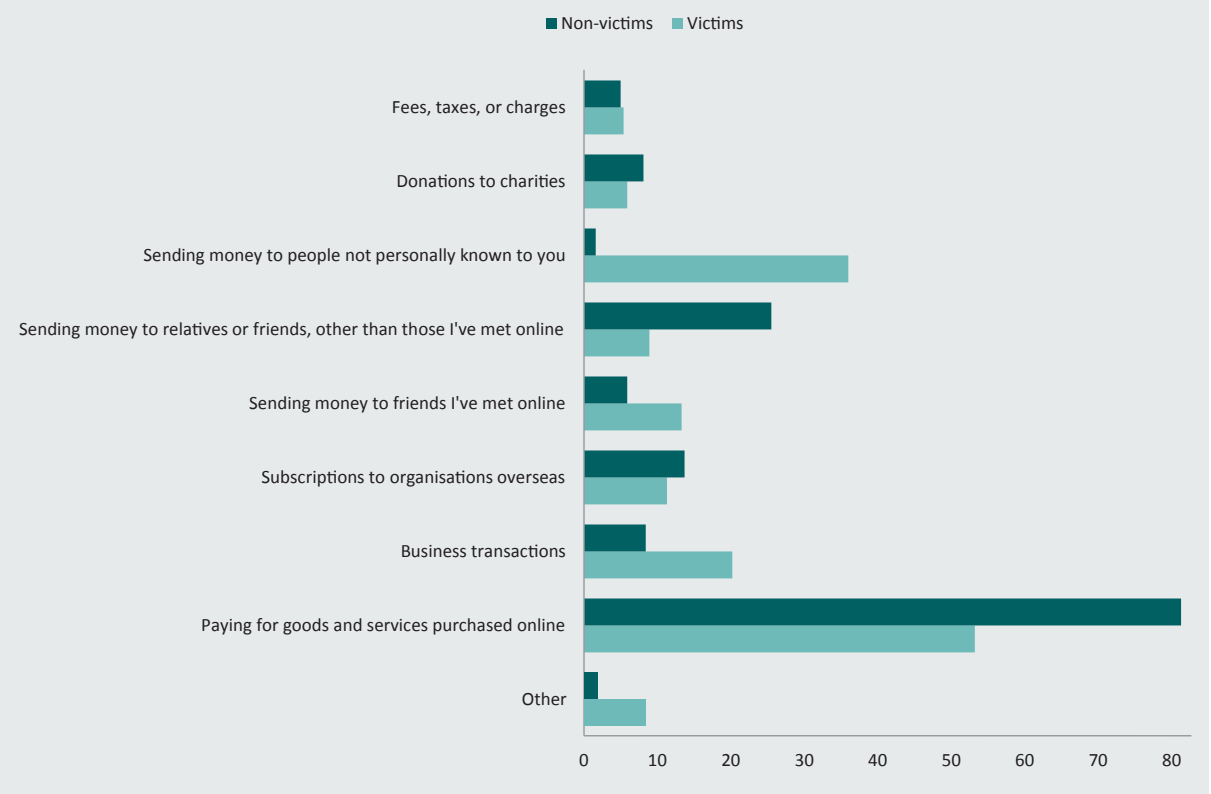
	Money sent to stranger			Total
	Yes	No	Nil response	
Victims	131*	44	1	176
Non-victims	81	95	0	176
Total	212	139	1	352

*Chi-square statistically significant at the $p<0.001$ level

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Victims and non-victims differed as to why they sent money overseas. Figure 1 indicates that victims were more likely to send money to people not personally known to them or to friends they had made online than were non-victims. However, victims more frequently cited reasons like paying for goods and services purchased online or sending money to relatives or friends (other than those met online).

Figure 1: Purpose of sending money overseas, victims and non-victims (%)



Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

The observed differences in Figure 1 were analysed to see if the differences between the victims and non-victims were statistically significant. Four purposes showed statistically significant differences between the victim and non-victim samples. The first was that non-victims were more likely to send money overseas as payment for goods and services they had purchased online than were victims ($\chi^2(1,352)=28.04$. $p<0.001$, Cramér's V=0.2823). Non-victims were also more likely to send money to relatives or friends (those they had not met online) than victims ($\chi^2(1,352)=19.26$, $p<0.001$, Cramér's V=0.2327). Victims were also more likely to have sent money overseas for a business opportunity ($\chi^2(1,352)=7.10$, $p<0.01$, Cramér's V=0.1420) or to someone they had met online ($\chi^2(1,352)=9.93$, $p<0.01$, Cramér's V=0.1680) than non-victims.

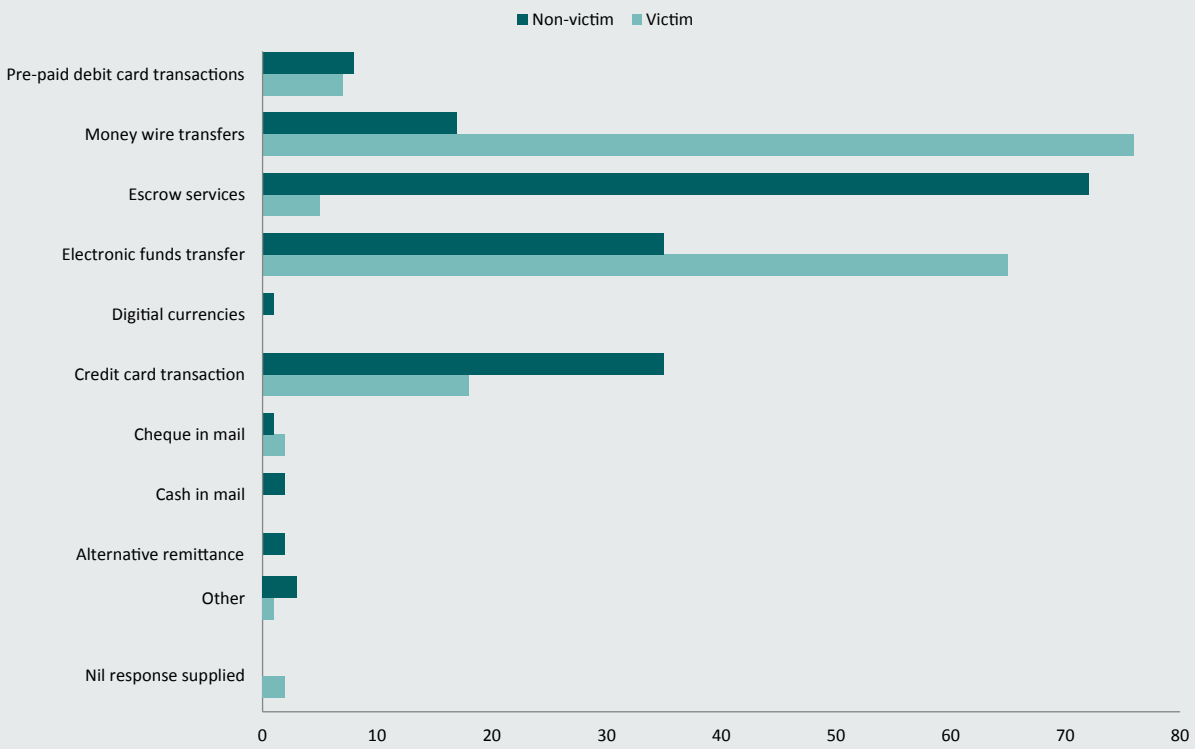
Table 2: Chi-square results for victimisation and purpose of sending money overseas

Purpose	Victim	Non-victim	DF	*p*-value
Paying for goods and services purchased online	52.8%	79.6%	1	<0.001
Business transactions	18.2%	8.5%	1	<0.01
Sending money to friends I've met online	12.5%	3.4%	1	<0.01
Sending money to relatives or friends (not met online)	8.5%	26.1%	1	<0.001

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Respondents were asked which funds transfer method they used for the largest funds transfer overseas in the last two years (Figure 2).

Figure 2: Method of sending the largest amount transferred overseas in the past two years, victims and non-victims (n)



Source: AIC Preventing Consumer Fraud in Australia Survey 2015 [AIC dataset]

Victims were more likely to use electronic funds transfers, or direct credit, than non-victims (37% compared with 20% of non-victims); or use money wire transfers provided by companies such as Western Union or Travelex, than non-victims (43% compared with 10% of non-victims). Conversely, non-victims were more likely to use credit card transactions (20% of non-victims compared with 10% of victims), or escrow services such as PayPal, than were victims (41% of non-victims compared with 3% of non-victims) ($\chi^2(10, n=352)=118.58$, $p<0.001$).

Table 3 presents the differences in the amounts of money sent overseas by victims and non-victims.

Table 3: Total amount of money sent overseas during the last two years, victims and non-victims				
Amount sent	Victims		Non-victims	
	n	%	n	%
$0–$5,000	130	64.0	303	94.4
$5001–$10,000	19	9.4	9	2.8
$10,001–$20,000	21	10.3	4	1.2
$20,001–$40,000	13	6.4	3	0.9
$40,001–$80,000	6	3.0	1	0.3
$80,001–$160,000	8	3.9	1	0.3
$160,001–$320,000	2	1.0	0	0.0
> $320,001	4	2.0	0	0.0

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Victims appeared to have sent more money overseas during the last two years than non-victims, with 10.3 percent of victims sending between $10,001 and $20,000, 9.4 percent sending between $5,001 and $10,000, and 6.4 percent sending between $20,001 and $40,000. By contrast, only 2.8 percent of non-victims sent between $5,001 and $10,000 and 1.2 percent sent between $10,001 and $20,000. Less than two percent of non-victims sent between $20,001 and $160,000. The data were not normally distributed, with more respondents sending lower amounts of money than higher amounts.

As the data were exactly matched, it was not appropriate to transform the data as this may have caused some of the matches to be dropped or changed. Using the Mann-Whitney U test was the best equivalent of the t-test under these circumstances. The test found that non-victims sent significantly less money overseas than victims of online fraud ($z=-9.582$, $p<0.01$, $n=352$). Looking at the differences between victims and non-victims and the total amount sent in the past two years, the Mann-Whitney U test found non-victims sent overseas significantly less money in total than victims ($z=-7.392$, $p<0.001$, $n=352$).

Life events

Participants were asked questions about life events they had experienced within the last five years. As was the case discussed above, one of the limitations of the survey instrument used in this research was the fact that it did not ask participants whether these events took place prior to, or after, the participants sent money overseas.

Table 4: Victim and non-victim experiences with life events (n)						
Life event	**Victims**			**Non-victims**		
	Yes	**No**	**I'd rather not say**	**Yes**	**No**	**I'd rather not say**
Ever declared bankrupt	18	156	2	15	159	2
In the last five years a close family member or friend died	97	73	6	84	88	4
In the last five years suffered depression	64	101	5	56	115	5
In the last five years lost job	42	127	7	32	140	4
In the last five years being diagnosed with a serious illness	28	142	6	28	140	8
In the last five years being a victim of a serious accident	7	167	2	2	170	4
In the last five years marriage or other close personal relationship breakdown*	36	135	5	19	153	4
In the last five years victim of a serious crime (eg theft, burglary, assault or sexual assault)	18	156	2	15	159	2

*statistically significant chi-square test at the 0.05 level

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

A series of chi-square tests was performed to determine if there was an association between certain life events and victimisation. Only one statistically significant relationship was found between victimisation and any of the variables examined. Table 4 shows the number of respondents who had experienced those events, those who had not, and the small number who would prefer not to say. A significant association was found between victimisation and those respondents who had experienced the break-up of either their marriage or another close personal relationship in the last five years (Fischer's Exact $p<0.05$).

Personal characteristics of victims compared with non-victims

The questionnaire contained seven questions asking participants about their personality traits. Participants were asked to rate their likelihood of behaving in certain ways on a scale ranging from 'very unlikely' to 'very likely'. The characteristics of victims and non-victims were explored in more detail. The personality characteristics are not from a particular psychological scale but are traits that have been linked to psychological factors that may make some people more vulnerable to fraudulent schemes.

The survey did not ask respondents how they rated themselves in relation to certain personal characteristics before, compared with after, victimisation. Therefore, it was not possible to analyse whether there had been a change in the personal characteristics that certain individuals displayed as a result of victimisation. Victim and non-victim responses to the questions are displayed in Table 5. The two groups differed in some ways. A number of statistically significant findings were identified regarding the relationship between certain characteristics of respondents and whether they were victims or non-victims. The only non-statistically significant relationship was between victimisation and the ratings of how likely people were to deal with adverse circumstances.

Table 5: Personal characteristics of victims and non-victims					
Characteristic	**Very unlikely**	**Unlikely**	**Neutral**	**Likely**	**Very likely**
Trust strangers					
Victims	79 (44.9%)**	47 (26.7%)	33 (18.8%)	15 (8.5%)	2 (1.1%)
Non-victims	42 (23.9%)	48 (27.3%)	66 (37.5%)	17 (9.7%)	3 (1.7%)
Help those in need					
Victims	24 (13.6%)*	26 (14.8%)	44 (25.0%)	64 (36.4%)	18 (10.2%)
Non-victims	7 (4.0%)	12 (6.8%)	56 (31.8%)	71 (40.3%)	30 (17.0%)
Seek opportunities					
Victims	30 (17.0%)	42 (23.9%)**	47 (26.7%)	48 (27.3%)	9 (5.1%)
Non-victims	11 (6.3%)	16 (9.1%)	77 (43.8%)	61 (34.7%)	11 (6.3%)
Make impulsive decisions					
Victims	59 (33.5%)**	63 (35.8%)	31 (17.6%)	20 (11.4%)	3 (1.7%)
Non-victims	27 (15.3%)	60 (34.1%)	54 (30.7%)	32 (18.2%)	3 (1.7%)
Make intuitive decisions					
Victims	30 (17.0%)	34 (19.3%)	59 (33.5%)	43 (24.4%)	10 (5.9%)
Non-victims	9 (5.1%)	10 (5.9%)	56 (31.8%)	89 (50.6%)**	12 (6.8%)
Wait for something due to me					
Victims	36 (20.5%)**	37 (21.0%)	71 (40.3%)	29 (16.5%)	3 (1.7%)
Non-victims	8 (4.5%)	16 (9.1%)	80 (45.5%)	65 (36.9%)	7 (4.0%)
Deal with adverse circumstances					
Victims	21 (11.9%)	12 (6.8%)	65 (36.9%)	58 (33.0%)	20 (11.4%)
Non-victims	9 (5.1%)	8 (4.5%)	61 (34.7%)	76 (43.2%)	22 (12.5%)

Note: Chi-square tests significant at $^{**}p<0.001$, $^{*}p<0.01$

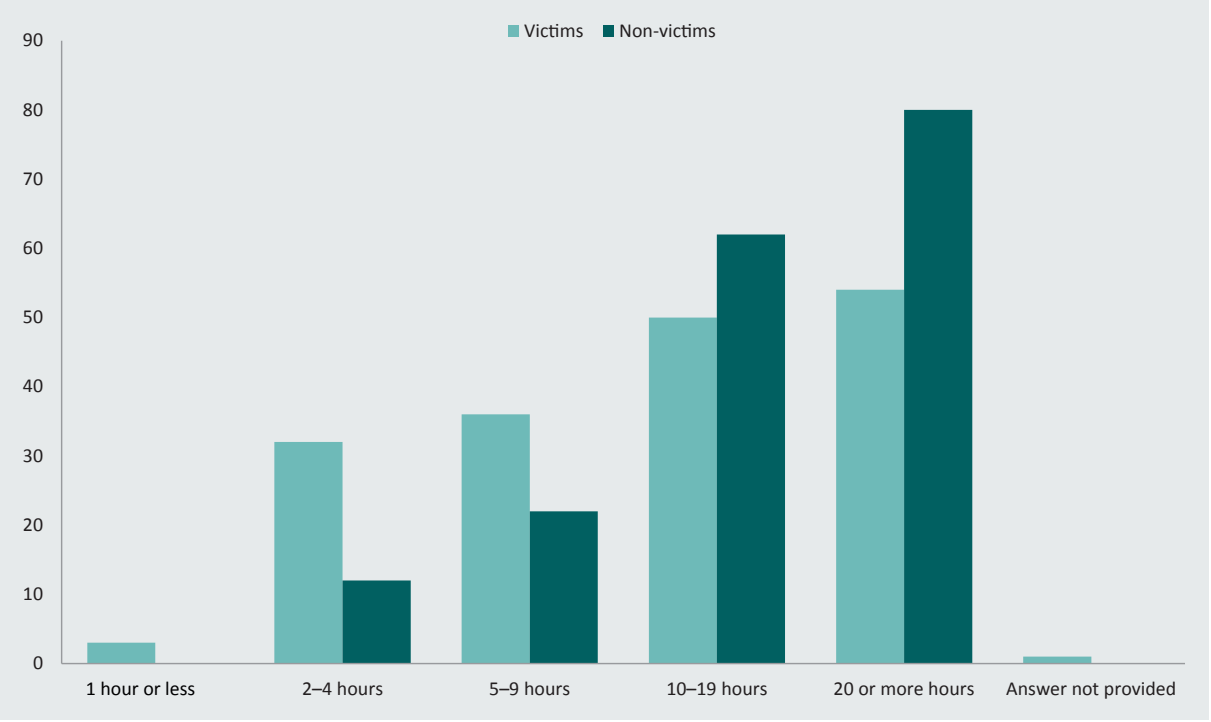
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

With all other personal characteristics there were significant differences in the ways that victims and non-victims perceived how likely they were to engage in the behaviours indicated. Victims were much less likely to trust strangers than non-victims, ($\chi^2(4,352)=22.65$, $p<0.001$, Cramér's V=0.2537), and were also much less likely to help those in need than non-victims ($\chi^2(4,352)=19.28$, $p<0.01$, Cramér's V=0.2341). Victims and non-victims differed in decision-making, with victims being very unlikely to make impulsive decisions ($\chi^2(4,352)=20.97$, $p<0.001$, Cramér's V=0.2441), and non-victims more likely to make intuitive decisions than non-victims ($\chi^2(4,352)=40.39$, $p<0.001$, Cramér's V=0.3400). Victims were also less likely to seek opportunities ($\chi^2(4,352)=29.47$, $p<0.001$, Cramér's V=0.2893), and were very unlikely to wait for something due to them ($\chi^2(4,352)=42.06$, $p<0.001$, Cramér's V=0.3457).

Capability online

Respondents were asked how many hours each week they spent using the internet for work and personal use, including email. Differences were identified in the number of hours spent by victims and non-victims, with non-victims spending more time each week accessing the internet than victims (Figure 3).

Figure 3: Hours spent on the internet each week, matched sample of victims and non-victims (n)



Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Given that frequency of online behaviour may have an impact on victimisation, further analysis was conducted. Internet use was dichotomised to either more or less than 10 hours a week. A chi-square test was then performed to determine if the frequencies observed were obtained by chance or there were significant differences in internet usage between victims and non-victims. A statistically significant relationship was found to exist between the amount of time spent using the internet, and victimisation. A higher proportion of non-victims spent 10 hours or more each week using the internet than victims, with 81 percent of non-victims spending this amount of time online each week compared with 59 percent of victims, ($\chi^2(1,352)=19.49$, $p<0.001$). The strength of the association, using Cramér's V, was only moderate.

Three types of computer and information and communications technology (ICT) security were found to be statistically related to victimisation (Table 6). Non-victims were more likely than victims to use anti-spyware software ($\chi^2(1,352)=6.769$, $p<0.01$, V=0.1387); anti-phishing software ($\chi^2(1,352)=7.425$, $p<0.01$, V=0.1449), and content and imaging filtering ($\chi^2(1,352)=7.214$, $p<0.01$, V=0.1423). None of the effect sizes was very large, indicating a weak association between the specific type of computer security and victimisation.

Table 6: Contingency table for method of computer security and matched victim/non-victim sample						
Type of computer security	Victim (n)		Non-victim (n)		χ^2	Significance
	Selected	Not selected	Selected	Not selected		
Anti-spyware software	92	84	116	60	6.76	<0.01
Anti-phishing software	58	118	83	93	7.43	<0.01
Content and image filtering	25	151	45	131	7.13	<0.01

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Multivariate analysis

Based on the prior research about vulnerability to fraud victimisation already discussed, further analyses were undertaken to determine if victimisation through online fraud could be predicted in terms of hours spent using the internet each week, the number of computer security measures used, and personality traits of trusting strangers, helping those in need, making impulsive decisions, relationship status, and the method used to send money overseas. The variables around the type of computer security measures used were collapsed into an 'advanced computer security' variable that included: data encryption, anti-spam filters, anti-virus software, anti-spy software, anti-phishing software, and internet content/imaging filtering or monitoring. Unlike passwords or firewalls, these categories of computer security are not standard with most computers and internet service providers, and involved a level of technical understanding exceeding simply purchasing a computer or wireless device and going online. A dummy dichotomous variable was created for 'how money was sent overseas' as victims were found to be more likely to use electronic funds transfer methods of payment than were non-victims. The variable recorded transfers using electronic funds transfer or money wire transfer, or not using these methods. There were few significant associations with life events. However, it was found that victims were more likely to have suffered a relationship breakdown than non-victims and so relationship breakdown was included in the model.

The analysis involved logistic regression where the predictor variable was a binary outcome of either victim or non-victim. The primary hypothesis was that greater levels of computer security would decrease the likelihood of online fraud victimisation. It was also hypothesised that the more time a person spent using the internet, the less likely it would be that they would become a victim of online fraud, since familiarity with the internet and searching websites would act as a preventive factor. The variables age, gender and education were not included in the model as they were exactly matched in the victim and non-victim groups.

The overall model (see Table 7) was statistically significant in predicting factors that would increase online fraud victimisation ($\chi^2(12,352)=131.25$, $p<0.001$). The model predicted factors that determined online fraud victimisation better than no model at all, with an Area Under the Receiver Operator Curve (ROC) of 0.83. An acceptable range and the variance explained by the model was: Nagelkerke=0.419. Importantly, the main hypothesis—that respondents who employed greater levels of computer security would be less likely to be victims of online fraud than those without—was not supported. However, the hypothesis that greater familiarity with online activities would result in a reduced likelihood of victimisation was supported. The only life event that was found to have a significant association with victimisation was relationship brakedown.

However, when included in the model this variable was not a statistically significant predictor of victimisation. The model also showed victims were more likely to use money wire transfers and electronic funds transfers to send money in response to scam invitations than other forms of payment.

Table 7: Logistic regression: Predictors of online fraud victimisation versus not being a victim

Variable	Odds ratio	SE	Wald (z statistic)	*p*-value
Advanced computer security	0.891	0.063	-1.64	0.102
Greater than 10 hours on internet	0.356	0.093	-3.94	0.000
Trust strangers 1—unlikely	0.679	0.212	-1.24	0.216
Trust strangers 2—neutral	0.385	0.131	-2.82	0.005
Trust strangers 3—likely	0.662	0.303	-0.90	0.367
Trust strangers 4—very likely	0.612	0.608	-0.47	0.622
Make impulsive decisions—1 unlikely	0.705	0.235	-1.05	0.295
Make impulsive decisions—2 neutral	0.458	0.174	-2.06	0.039
Make impulsive decisions—3 likely	0.409	0.174	-2.11	0.035
Make impulsive decisions—4 very likely	0.657	0.583	-2.11	0.636
Relationship breakdown had occurred	1.510	0.383	1.08	0.282
Money transferred via electronic funds transfer or money wire transfer	8.870	0.273	7.99	0.000
Constant	6.859	2.468	5.35	0.000

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Discussion

At the end of December of 2017, there were 14.2m internet subscribers in Australia, an increase of 3.4 percent from the end of June that year (Australian Bureau of Statistics 2016). The way that people use the internet for recreation or for buying goods and services raises a number of important questions relevant to their risk of being victimised, including why some people experience more problems than others as a result of their online interactions.

Online fraud has become one of the most prevalent international crimes. The Australian Bureau of Statistics (ABS) estimated for 2014–15, 1.6 million Australians (8.5% of the population 15 years and over) experienced personal fraud, with losses for all personal fraud (including scams, credit card fraud and identity crime) reaching $3b (ABS 2016). In 2017, the Australian Competition and Consumer Commission, the Australian Cybercrime Online Reporting Network and other government organisations such as the Australian Taxation Office received more than 200,000 scam reports with reported losses exceeding $340m—an increase of $40m from the previous year. The ACCC alone received more than 161,500 scam reports with $90.9m in financial losses, representing an eight percent increase in reported losses over 2016 (ACCC 2018). Online fraud in Australia is a costly and potentially devastating crime.

This study sought to determine and to quantify the factors that make an individual vulnerable to online fraud and lead to victimisation. Using a methodology similar to that for case–control samples in epidemiology studies, two independent samples were collected, one of victims and another of non-victims, all of whom had sent money overseas in the past two years. A number of factors were examined to determine how the two groups differed and why some people became victims while others did not. These included: online behaviour, demographic factors, and the effects of important life events. A small number of statistically significant findings were identified which may be useful in guiding the future development of targeted awareness-raising and online fraud prevention programs. Many of the findings did not demonstrate statistically significant relationships between variables that were expected to indicate vulnerability to consumer fraud.

A statistically significant relationship was found between victimisation and the amount of money sent overseas, with victims sending more money overseas during the last two years compared with non-victims. In particular, the regression model demonstrated the importance financial institutions and money transfer businesses have when it comes to reducing victimisation by scammers. Victims were more likely than non-victims to use methods such as money wire transfers and other forms of electronic funds transfers—a fast way of sending money that can then be instantly transferred elsewhere. This finding reinforces the need for programs such as the ACCC's Scams Disruption Project (ACCC 2018), South Australia Police's Operation Disrepair (Nankervis 2014) and Project Sunbird (WA Department of Commerce 2014)—all no longer operating. Given the large amounts of money lost to online fraud in Australia every year, it may be useful to reintroduce and extend these proactive disruption initiatives to all Australian states and territories. Relying on the financial intelligence collected by the Australian Transaction Reports and Analysis Centre (AUSTRAC) will also be important. Efforts may be needed to share this with a larger pool of private sector entities.

The differences in time spent on the internet by victims and non-victims each week may be attributed to concern by victims that they may again become victims of online fraud. Indeed, Reisig, Pratt and Holtfreter (2009) found that individuals who perceived themselves to be at greater risk of online theft victimisation modified their online behaviours to reduce the likelihood that they would be victimised. This included spending less time on the internet. However, with everyday activities becoming increasingly based online, spending less time on the internet is not an achievable method of preventing online fraud. Rather it may mean consumers do not have enough experience online to effectively make use of various protective measures when they do go online. Bossler and Holt (2009) examined the time spent online using a Routine Activity Theory perspective, noting that internet experience had the potential to be an effective capable guardian while online. The research found that engaging in everyday online activities, such as internet banking or online shopping, was not associated with online fraud victimisation. However, people who engaged in online piracy did increase their risk of victimisation (Bossler & Holt 2009).

The use of computer and IT security had mixed results in the present research. Initial findings indicated that using more advanced forms of IT security might protect against online fraud victimisation. Respondents identified as non-victims were more likely to use security measures such as anti-phishing software, anti-spyware and to use content and imaging filtering while online compared with respondents identified as victims. This indicates that a greater level of use and understanding about computer security may help to prevent online fraud. However, when a 'computer security' variable was recoded to factor in the types of advanced security measures used by respondents, there was no statistically significant relationship between victims and non-victims in terms of use of a few or more forms of security. Whitty (2017), in a study looking at the psychological characteristics of romance scam victims, asked respondents (victims and non-victims) to self-rate their level of understanding about cybersecurity, on the basis that those who reported they did not know a lot about cybersecurity were more likely to be victims of romance scams. Consistent with the current research, Whitty (2017) found the hypothesis about knowledge of cybersecurity was not statistically supported.

Personal characteristics and negative life events

Contrary to prior similar research undertaken by Ross and Smith (2011), victims of online fraud, in the current research, were no more likely to have suffered from negative life events than non-victims of online fraud. Members of the victim sample were statistically more likely to have suffered a relationship breakdown during the last five years than respondents in the non-victim sample. This finding may be relevant for dating and romance scam victims. However, the present research was unable to determine the extent of dating and romance scam victimisation as the survey looked at generic online fraud and not specific fraud types.

Research into the psychological factors associated with dating and romance scams has found that victims are more likely to score high on scales of impulsivity and lack of self-control (Whitty 2017). While the present research looked at online fraud in general, there were some similarities between the current research findings and those of prior research. For example, the current research found victims of online fraud reported they were 'very unlikely' to wait for something due to them at greater levels than were non-victims. Although psychological assessment scales were not used in the current research, the inability to wait for something may indicate victims are more impulsive than non-victims or may indicate impulsivity as found in prior research (Holtfreter, Reisig & Pratt 2008).

While other significant differences in personality traits were found between victims and non-victims there were some limitations in the number of conclusions that could be drawn from these findings. The survey instrument did not ask respondents how they rated themselves in relation to certain personal characteristics before and after victimisation. Also, the questions were not presented as part of a personality inventory of psychological items, meaning the phrasing of the questions could not assess psychological traits such as 'kindness' or 'impulsivity' to any true extent. As a result, it was difficult to ascertain if victims answered the questions from the perspective of how they would have behaved prior to being victimised, or whether they answered the questions based on how they would behave now that the victimisation had occurred, and whether or not the questions indicated psychological traits. These aspects could be pursued further in future research.

Policy implications

The present study identified several differences between the online behaviour of victims and non-victims of online fraud. These may provide opportunities for policymakers, police and consumer affairs organisations to improve the targeting of online consumer fraud prevention and awareness-raising initiatives in the future.

It was found that non-victims tended to shop online using sites known to them or send money overseas to people who were personally known to them, such as friends (not made online) or family. Victims, however, were more likely to send money to people they did not know and people with whom they had recently established online relationships. These findings present opportunities for those involved in cyber-safety and fraud prevention to alert individuals engaged in online shopping to be vigilant in determining the identity and legitimacy of individuals with whom they are proposing to conduct transactions online. Advice could be provided as to how to verify the identity of online contacts, and the red flags that could indicate high-risk activities.

Another notable difference between victims and non-victims was that non-victims were more likely to have spent more time using the internet. This finding proved to be an important protective factor for users, reinforcing the need for those engaging in online shopping to spend more time online to learn safe shopping and entertainment behaviours. They should also be encouraged to maintain safe hardware and software and be aware of the latest risks of consumer fraud online, and how to avoid them.

Victims also sent more money overseas than non-victims, and used different methods of transferring money. The fact that the current study identified victims as being more likely to send money overseas via money wire transfers compared with non-victims also highlights the continuing need for consumer protection campaigns and programs to educate and remind individuals of the risks associated with using money wire transfers when making overseas payments. Awareness campaigns of this nature are currently being undertaken by some of the largest corporate remitters, but industry campaigns should also make users aware of the benefits of using payment methods that have high levels of security and the mechanisms for reimbursing funds where losses occur through no fault of those conducting transactions online.

This study provides new data to support the development of targeted online fraud awareness-raising campaigns. These could effectively focus on areas of online behaviour most likely to lead to victimisation. Further research could be conducted to verify whether the factors that were found to be statistically significant predictors of victimisation in the present study remain so when account is taken of their presence before and after victimisation.

References

URLs correct as at February 2019

Anderson K 2013. *Consumer fraud in the United States, 2011: The third FTC survey*. https://www.ftc.gov/reports/consumer-fraud-united-states-2011-third-ftc-survey

Australian Bureau of Statistics 2016. *Personal Fraud, 2014-2015*. *ABS cat. no. 4528.0.* Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0/

Australian Competition and Consumer Commission 2018. *Targeting Scams. Report of the ACCC on scams activity in 2017*. Canberra: ACCC

Atkins B & Huang W 2013. A study of social engineering in online frauds. *Open Journal of Social Sciences* 1(3): 23–32

Bossler AM & Holt TJ 2009. On-line activities, guardianship and malware infection: An examination of Routine Activities Theory. *International Journal of Cyber Criminology* 3(1): 400–420

Button M, McNaughton Nicholls C, Kerr J & Owen R 2014. Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology* 47(3): 391–408

Button M, Lewis C & Tapley J 2009. *Fraud typologies and victims of fraud: Literature review*. London: National Fraud Authority

Chang J 2008. An analysis of advance fee fraud on the internet. *Journal of Financial Crime* 15(1): 71–81

Chang J & Chong M 2010. Psychological influences in e-mail fraud, *Journal of Financial Crime* 17(3): 337–350

Cross C 2015. No laughing matter: Blaming the victim of online fraud. *International Review of Victimology* 21(2): 187–204

Cross C, Smith RG & Richards K 2014. Challenges of responding to online fraud victimisation in Australia. *Trends & issues in crime and criminal justice* no. 474. https://aic.gov.au/publications/tandi/tandi474

Emami C, Smith RG & Jorna P forthcoming. *Individual differences in online fraud victimisation in Australia*. *Research Report*. Canberra: Australian Institute of Criminology

Holt TJ & Bossler AM 2014. An assessment of the current state of cybercrime scholarship. *Deviant Behavior* 35: 20–40

Holtfreter K, Reisig M & Pratt T 2008. Low self-control, routine activities, and fraud victimization. *Criminology* 46: 189–220

Jorna 2016. The relationship between age and consumer fraud victimisation. *Trends & issues in crime and criminal justice* no. 519. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi519

Lee J & Soberon-Ferrer H 1997. Consumer vulnerability to fraud: influencing factors. *Journal of Consumer Affairs* 31(1): 70–89

Nankervis D 2014. Operation Disrepair finds South Australians lost more than $2 million in 4261 transactions to foreign scams. *The Advertiser*, 3 Mar. https://www.adelaidenow.com.au/operation-disrepair-finds-south-australians-lost-more-than-2-million-in-4261-transactions-to-foreign-scams/news-story/519962b331e753cf9c21a9e2db8d6c8a

Nhan J, Kinkade P & Burns R 2009. Finding a pot of gold at the end of an internet rainbow: Further examination of fraudulent email solicitation. *International Journal of Cyber Criminology* 3(1): 452–475

Office of Fair Trading (OFT) 2009. *The psychology of scams: Provoking and committing errors of judgement*. London: OFT

Pearce N 2016. Analysis of matched case-control studies. *The BMJ*: 2016 352:i969. http://www.bmj.com/content/352/bmj.i969

Pratt T, Holtfreter K & Reisig M 2010. Routine online activity and internet fraud targeting: Extending the generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency* 47(3): 267–296

Reisig MD, Pratt TC & Holtfreter K 2009. Perceived risk of internet theft victimisation: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior* 36: 369–384

Ross S & Smith RG 2011. Risk factors for advance fee fraud victimisation. *Trends & issues in crime and criminal justice* no. 420. Canberra: AIC. https://aic.gov.au/publications/tandi/tandi420

Shadel D, Pak K & Sauer J 2014. *Caught in the scammer's net: Risk factors that may lead to becoming an internet fraud victim.* https://doi.org/10.26419/res.00076.004

Stay Smart Online 2018. *Why this matters to you*. Canberra: Commonwealth of Australia. https://www.staysmartonline.gov.au/protect-yourself/why-matters-you

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

Western Australia Department of Commerce 2014. *Project Sunbird*. http://www.scamnet.wa.gov.au/scamnet/Scam_Types-Advanced_fee_frauds-OperationProject_Sunbird.htm

Whitty M 2017. Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior and Social Networking* 21(2): 105–109

Acknowledgments

This study was conducted with the cooperation and support of the Australian Competition and Consumer Commission (ACCC). The considerable expertise and assistance of the ACCC's Scamwatch staff are gratefully acknowledged.

Data collection for the sample of non-victims was undertaken professionally and efficiently by i-Link Research Solutions and funding for this was provided by the Criminology Research Fund. Anthony Morgan, Research Manager at the Australian Institute of Criminology, kindly assisted with matched data analyses. The time and willingness of those who completed the survey are also gratefully acknowledged.

The opinions expressed in this publication are those of the authors alone and do not necessarily reflect the views or policies of the Australian Government or its entities.

Catherine Emami is a former Research Officer at the Australian Institute of Criminology.

Dr Russell G Smith is Principal Criminologist at the Australian Institute of Criminology and a Professor in the College of Business, Government and Law at Flinders University.

Penny Jorna is a Research Analyst at the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy 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 1836-2206 (Online)
ISBN 978 1 925304 01 5 (Online)

GPO Box 1936
Canberra ACT 2601, Australia
Tel: 02 6268 7166

aic.gov.au