Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

ISSN 0817-8542

No. 519 November 2016

Abstract | The Australian Bureau of Statistics estimates consumer fraud costs Australians $1.4b per year. Advances in technology allow fraudsters to reach an increasing number of potential victims. Age has long been considered a potential factor in the risk of victimisation; however, it remains unclear which age groups are most vulnerable.

This paper examines the relationship between age and the risk of consumer fraud, using the results of online surveys conducted by the AIC on behalf of the Australasian Consumer Fraud Taskforce in 2011 and 2012. The surveys found statistically significant relationships between age and how invitations were received; age and frauds resulting in victimisation; and age and those who sent money in response to invitations.

Targeted, age-specific awareness-raising campaigns may be an effective means of reducing the risk of consumer fraud. Initiatives that address the risks associated with lifestyle factors such as social networking, online dating and the use of both new and existing technologies may be of particular benefit.

The relationship between age and consumer fraud victimisation

Penny Jorna

Seventy-two year old Paul from rural Australia, devastated by the death of his wife, used an online dating website to find companionship and met a woman named Selina, from Ghana. They struck up a relationship. One day Paul received a phone call from a man claiming to be Selina's brother. The man told Paul that Selina had been hit by a car and had suffered a brain haemorrhage and asked Paul for $1,200 to cover the costs of the operation. The contact continued for months and the fraudsters used Paul's perceived relationship with Selina to convince him to help her village through the financing of gold refining and butter processing. Paul sent over $200,000 over several months (News.com.au 2009).

Consumer fraud, also known as personal fraud, has been defined as a type of fraud that involves communication between an individual victim and an offender, involving 'deliberate deception of the victim with the promise of goods, services or other benefits that are non-existent, unnecessary, were never intended to be provided, or were grossly misrepresented' (Titus & Gover 2001:2). As the example above demonstrates, the ramifications of fraud can be devastating both financially and emotionally.

Fraudsters use a wide range of communication methods to commit consumer fraud (Budd & Anderson 2011). While in the past fraudulent invitations were primarily sent through

postal services or made face-to-face, the digital age has seen an increase in the use of electronic devices such as computers and mobile phones to deliver consumer fraud invitations to people of all ages (Reyns 2013; Reisig & Holtfreter 2013). Fraud methods are continually adapted to advancing technologies and emerging trends in computer use, challenging authorities and fraud-prevention agencies to develop effective responses to the problem.

Keeping up with developments in online fraud activity will continue to be a key concern for authorities, given the widespread assumption that consumer fraud is likely to increase with greater advances in technology (Holtfreter, van Slyke & Blomberg 2005). Given this, it is important to fully understand the risks and protective factors that mediate an individual's likelihood of victimisation.

One such factor identified in the literature relates to the consumer fraud vulnerabilities associated with age (Fischer, Lea & Evans 2013). This paper explores the risk of consumer fraud victimisation at different ages, with the aim of identifying particular points for intervention.

The relationship between age and consumer fraud

Drawing on Cohen and Felson's (1979) routine activity theory, Pratt, Holtfreter and Reisig (2010) argue that advances in technology and the daily use of the internet for shopping, work and communication constitute a structural change in everyday routine that may bring people into more frequent contact with motivated fraud offenders. This risk is exacerbated by the absence of effective guardianship in the online world which might prevent fraud from occurring. With more daily activities like banking, shopping and socialising conducted via the internet it is important to understand how this impacts the risks of fraud victimisation associated with different ages and stages of life.

Previous research has identified two potential age-related risk factors for fraud victimisation: younger people may be at more risk of consumer fraud because they use a wide range of technologies (Titus, Heinzelmann & Boyle 1995), while some older people may be at greater risk because they are seen as attractive targets with potential access to life savings (Cohen 2006) who may suffer impaired decision-making due to ageing (Scheibe et al. 2014).

Reisig and Holtfreter (2013) note that, while a reliable demographic profile of victims has not been observed in prior studies, those aged over 60 were particularly vulnerable to consumer fraud. The authors caution that some research focuses on types of consumer fraud that typically affect older people, thereby biasing the results. Other research has found older people may be at more risk of consumer fraud victimisation because they have access to retirement savings; in addition, as older people are increasingly on fixed incomes, they may be more willing to take risks to increase their wealth (Cohen 2006; Blanton 2012). However, still other research has found that younger people may be more likely to receive fraudulent invitations and lose money to scams than older people, due to lifestyle factors related to their age (Muscat, James & Graycar 2002; Titus, Heinzelmann & Boyle 1995).

Media reports about age and consumer fraud are equally mixed. Some suggest older Australians are at greater risk of victimisation by scammers (Quist 2013), while others focus on the vulnerability of younger consumers (*Four Corners* 2013). A recent Australian Competition and Consumer Commission (ACCC) report found that, contrary to popular belief, young consumers were not over-represented in

reports of fraud to the ACCC, nor were older consumers more at risk of victimisation; and, although a great many of all scam-related reports to the ACCC were made by Australians aged 64 and over, this demographic experienced only low levels of victimisation through loss of funds (ACCC 2014). Therefore, while age has been identified as a potential risk factor for consumer-fraud victimisation, the nature of this relationship remains uncertain.

Research suggests that individuals at both extremes of the age spectrum may be made more vulnerable by how they communicate and other lifestyle factors (Titus, Heinzelmann & Boyle 1995; Pratt, Holtfreter & Reisig 2010). Economic studies of financial literacy have found sound financial decisions are less common among both younger and older people, meaning these groups may be more vulnerable to consumer fraud victimisation (Ross, Grossmann & Schryer 2014).

This paper presents findings from the 2011 and 2012 Australasian Consumer Fraud Taskforce (ACFT) surveys, with a particular focus on the relationship between age and the risk of consumer fraud victimisation, including an examination of the relationship between age groups (the independent variable for predicting victimisation) and the dependent variables of delivery method and victimisation due to consumer fraud activity. This will enhance the understanding of fraud victimisation, assist in tailoring fraud-prevention activities to particular age groups and allow more effective public education on the risks of consumer fraud.

Method

Each year the Australian Institute of Criminology (AIC) conducts a self-selected online survey on behalf of the ACFT to assess the consumer fraud experiences of participating Australians and New Zealanders. The results presented in this paper are based on surveys conducted between 1 January and 31 March in 2011 and 2012. During this period a total of 2,720 Australian and New Zealand residents responded; 25 of these, who declined to disclose their age, were excluded from the analysis, leaving a sample size of 2,695 respondents.

Respondents were asked 21 questions relating to their experience of consumer fraud in the 12 months preceding the surveys, their demographics, and their awareness of ACFT and reporting activities. As with all self-report surveys, caution should be exercised in interpreting the findings, as there is no control over who may participate and the self-selection sample bias can make generalising the findings to the wider population problematic. Other problems common to the use of surveys also apply, including the potential for respondents to misunderstand the questions and the inability to determine whether the responses accurately reflect the reported events. In addition, the survey relies on respondents being aware of their consumer fraud victimisation.

Box 1: Specific fraud types addressed by the survey

Lottery fraud: fraud involving false notification of a prize or competition win.

Advance fee fraud: fraud where fraudsters seek assistance to transfer a large amount of money overseas.

Inheritance fraud: fraud that falsely notifies the recipient of the death of a distant relative who has left the potential victim a large inheritance.

Phishing: an attempt to trick people into giving out their personal details or banking information.

Financial advice fraud: fraud involving the provision of financial advice which generally does not involve a legitimate investment or lead to increased wealth.

Work-from-home invitations: fraud involving false offers of employment. Work-from-home scams are often fronts for illegal money-laundering activities or pyramid schemes.

Computer support fraud: fraud involving contact by fraudsters who claim to be representatives of legitimate businesses, who can fix problems with the recipients' computer. Fraudsters may ask for money, personal details or passwords, or seek to sell worthless products to fix computers.

Dating/romance fraud: these schemes may demand payment for each email sent and received by the victim. Alternatively, romance scammers may 'hook' victims by asking for money for an unwell relative or to help them with financial trouble.

Other fraud: any type of fraudulent invitation that does not fit any of the previous categories.

Source: ACFT surveys 2011 and 2012

There were some minor differences between the questions asked in each year. Many respondents (n=177) to the 2011 survey, when asked about receipt of fraudulent invitations, included computer support fraud in the 'other' response category. As a result, computer support frauds were included as a specified fraud type in the 2012 survey. There was also the difficulty of the potential overlap between advance fee fraud and some other fraud types, such as lottery or inheritance fraud, which are essentially forms of advance fee fraud. To avoid this, advance fee fraud was defined for the survey as involving the transfer of large amounts of money overseas, as occurs in traditional West African 419 scams (see Smith et al. 1999; Box 1).

Further details about the survey method and analysis of the findings can be found in Jorna and Hutchings (2013).

Age of respondents

The age categories available to survey respondents were those used by the Australian Bureau of Statistics (ABS; 2012), all of which are 10-year groupings, with the exception of two: those of 17 years and under, and 65 years and over. These two categories spanned more than 10 years, as it was expected they would attract fewer respondents. Respondents were asked which age group they belonged to. The distribution of respondents by age group is shown in Table 1.

Table 1: Respondents by age category (n)

Age	n	%	% of age category who received a fraudulent invitation
17 & under	89	3	72
18–24	160	6	93
25–34	429	16	95
35–44	467	17	96
45–54	610	23	98
55–64	568	21	97
65 & over	372	14	99
Total	2,695	100	

Source: ACFT survey 2011 and 2012 [AIC computer file]

Fraud delivery method

Of the 2,695 survey respondents, 2,585 (96%) reported receiving one or more fraudulent invitations, including offers of money, goods or relationships that later turned out to be false. Those who received a fraudulent invitation were asked how it had been delivered. The results concerning age and delivery method are presented in Table 2. Only delivery by mail was not found to have a significant relationship with age (χ^2 (6, n=2,585)=8.10, p>0.05).

Invitations were most often received by email; 73 percent of respondents had received a fraudulent invitation in this way. As Table 2 shows, there was a significant association between age and the delivery of invitations by email (χ^2 (6, n= 2,585)=19.58, p<0.001). The adjusted residuals were analysed to identify which categories were influencing the statistically significant results. This analysis showed that, while respondents aged 65 or over were significantly less likely to receive a fraudulent invitation by email, those aged 18–34 were significantly more likely to receive one in this way.

The analysis also found a significant relationship between age and the receipt of invitations via mobile phone or SMS (χ^2 (6, n=2,585)=19.58, p<0.001). Respondents aged 55 or over were statistically less likely to receive frauds in this way. Those aged 17 and under, and 25–34 year olds, were significantly more likely to receive an invitation via mobile phone or SMS. A significant relationship was also found between age and the receipt of an invitation over the internet (χ^2(6, n=2,585)=180.35, p<0.001). Those aged 34 and under were statistically more likely to receive an invitation via the internet, while those aged 55 and over were less likely to receive an invitation in this way. Another statistically significant association was found between age and those who received an invitation via a landline telephone (χ^2 (6, n=2,585)=9.58, p<0.001); those aged 18–34 were significantly less likely than others to receive invitations via this method. No particular delivery method was more likely for those aged over 35 who received a fraudulent invitation.

In summary, the analysis found a relationship between age and how fraudulent invitations were delivered, with younger respondents more likely to receive fraudulent invitations via more recent technologies such as the internet and SMS.

Table 2: Receipt of unsolicited fraud invitations by age and delivery method (%; n=2,585)

Delivery method	17 & under (n=64)	18–24 (n=148)	25–34 (n=406)	35–44 (n=450)	45–54 (n=596)	55–64 (n=553)	65 and over (n=368)	Significance
Mail	22	18	21	20	19	17	14	$p>0.05$, Cramer's V 0.1
Email	73	81*	81*	73	75	69	59*	$p<0.001$, Cramer's V 0.2
Landline phone	50	36*	45*	54	49	49	53	$p<0.01$, Cramer's V 0.1
Mobile phone/ SMS	39*	22	23*	19	20	15*	11*	$p<0.001$, Cramer's V 0.1
Internet	67*	31*	25*	17	17	14*	6*	$p<0.001$, Cramer's V 0.3
Other	9	8	7	8	7	5	3*	$p<0.05$, Cramer's V 0.1

*Denotes ages that are significantly different based on an analysis of the adjusted residuals
Source: ACFT surveys 2011 and 2012 [AIC computer file]

Table 3: Fraud victimisation (dichotomised) and age (Fisher's Exact test), (n)

Fraud type	17 & under	18–24	25–34	35–44	45–54	55–64	65 & over	Total	Significance
Work-from-home fraud									
Victim	1	8*	7	3*	14	8	10	51	$p<0.05$ Cramer's V 0.08
Not a victim	63	140	399	447	582	545	358	2,534	
Dating fraud									
Victim	1	1	2*	9	22*	8	6	49	$p<0.05$ Cramer's V 0.08
Not a victim	63	147	404	441	574	545	362	2,536	
Computer support scheme									
Victim	4*	2	2*	8	8	6	19*	49	$p<0.001$ Cramer's V 0.12
Not a victim	60	146	404	442	588	547	349	2,536	

*Denotes ages that are significantly different based on an analysis of the adjusted residuals
Source: ACFT survey 2011 and 2012 [AIC computer file]

Responses to fraudulent invitations

For this study, a victim was defined as an individual who provided personal details and/or suffered a financial loss as a result of replying to an invitation (Jorna & Hutchings 2013). No significant relationship was found between age and responses to fraud victimisation by sending personal details or money. With regard to specific types of fraud, no significant relationship was found between age and victimisation by lottery fraud, advance fee fraud, inheritance fraud, phishing, financial advice fraud or other fraudulent invitations.

As shown in Table 3, a statistically significant relationship was found between age and victimisation by work-from-home frauds (χ^2 (6, n=2,585)=15.21, $p<0.05$), and between age and victimisation by a dating/romance fraud (χ^2 (6, n=2,585)=17.49, $p<0.05$). Computer support scheme victimisation was also found to be significantly related to age (χ^2 (6, n=2,585)=33.55, $p<0.001$).

Age-related differences were most apparent among those respondents who had been victims of a dating or romance fraud. Those aged 45–54 were most likely to be victimised by this type of fraud (45% of victims). However, as presented in Table 3, Cramer's V values indicate the association between these variables was weak. A weak association may indicate that variables other than age alone might affect victimisation.

Nature of responses

Sending personal details

Victims of fraud may send personal information to fraudsters, including bank account or personal details. The disclosure of such information can lead to further victimisation and ongoing financial loss through identity theft.

Table 4 shows a significant relationship between age and the sending of personal details in response to an invitation (χ^2 (6, n=459)=4.35, p=<0.05). Three hundred and fifty-seven respondents were victimised by sending personal details in the 12 months prior to completing the surveys. Respondents aged 18–24 were more likely to send personal details in response to a fraudulent invitation than those in any other age category (p<0.05), whereas those aged 65 and over were statistically less likely to send personal details as a result of a fraudulent invitation. No significant relationship was found between age and the sending both of money and personal details in response to an invitation (χ^2 (6, n= 459)=3.75, p>0.05).

Table 4: Sending personal details, passwords and/or money by age category (%)

Age	Personal details only		Money only		Both	
	N	%	N	%	N	%
17 & under (n=89)	10	11	4	4	3	3
18–24 (n=160)	30	19*	17	11	15	9
25–34 (n=429)	50	12	31	7	20	5
35–44 (n=467)	68	15	37	8*	25	5
45–54 (n=610)	87	14	70	11	40	7
55–64 (n=568)	59	10	54	10	32	6
65 & over (n=372)	53	14*	53	14*	29	8
Significance		p<0.05, Cramer's V 0.2		p<0.05, Cramer's V 0.2		p>0.05, Cramer's V 0.1
Total	357		266		164	

* Denotes ages that are significantly different based on an analysis of the adjusted residuals
Source: ACFT survey 2011 and 2012 [AIC computer file]

Financial loss

Three financial loss amounts—$200m, $16.5m and $5m—were removed from analysis as they were considered outliers (ie large loss figures believed to be a result of misunderstanding the survey questions). Outliers were similarly excluded in previous years.

Of the respondents who reported being a victim of fraud in the previous 12 months, 58 percent (n=266) had sent money in response to a fraudulent invitation. A significant association was found between age and those respondents who sent money in response to an invitation (χ^2 (6, n=2,585)=14.82, p<0.05; Table 4). Those aged 65 and over were statistically significantly more likely to send money than other age groups (14%).

Respondents aged 35–44 were statistically less likely to send money as a result of a fraudulent invitation than any other age group. Analysis was undertaken to test the relationship between the age of respondents who reported a financial loss (n=221) and the amount of money lost. As the amounts reported lost were skewed, the variable was normalised using logarithmic transformation prior to analysis.

A one-way, between-groups analysis of variance was conducted to explore the impact of age on the amount of financial loss due to fraud victimisation. No statistical difference was found between the amount of monetary loss and age ($F(6, 220)=1.99$, $p>0.05$).

Multivariate analysis

As the bivariate analyses showed an association between age and consumer fraud victimisation, logistic regression analyses were performed to account for other factors that may have contributed to fraud victimisation (Field 2013) and to model potential factors predicting consumer fraud victimisation. Respondents were asked their age; other demographic variables in the questionnaires related to gender, income level and place of residence (either New Zealand or an Australian state or territory). Regression models were developed to examine consumer fraud victimisation by holding age, gender and income levels constant to determine which variable contributed most to the prediction model.

Previous bivariate analyses have shown that dichotomising respondents into victim and non-victim categories and analysing by age does not produce a statistically significant association for all types of consumer fraud examined. Therefore, only the three types of consumer fraud—work-from-home fraud, computer support schemes and dating/romance fraud—which initially showed an association were included in the regression models. Three models were created to determine if victimisation by consumer fraud could be predicted by the demographic variables of age, income level and gender. All models sought to predict victimisation using the chosen variable while holding the other, aforementioned variables constant.

The first model sought to predict victimisation by computer support frauds; the second model predicted victimisation by dating and romance frauds; and the third model sought to predict victimisation through work-from-home fraudulent invitations. As there were few reported victims aged 17 years and under, a combined 17 years and under and 18–24 years group was created (n=249) to represent the younger respondents in the survey.

All three models achieved a receiver operating characteristic curve (area under curve or AUC) score above 0.7, indicating the models provided an acceptable level of discrimination between observed groups (Field 2013; see Tables 5–7 for relevant tables). All three models were overall statistically significant (Model 1 [$p<0.001$], Model 2 [$p<0.01$] and Model 3 [$p<0.01$]), indicating the models were better predictors of consumer fraud victimisation than no model.

Model 1: Computer support fraud

The model predicting victimisation by computer support fraud (Model 1) demonstrated that, after controlling for a range of socio-demographic factors, the only variable that made a statistically

significant contribution to the model was age. The strongest predictor of victimisation by computer support fraud was whether the respondent was aged 65 or over. Holding all other variables constant, the model found that respondents younger than 65 were less likely to fall victim to this fraud type than those aged 65 and over (p<0.01).

Model 2: Dating and romance frauds

Those aged 45–54 experienced the highest rate of victimisation by dating or romance frauds. The model (Model 2) found that respondents of all age groups (other than 35–44 years, the only age category that was not statistically significant) were less likely to be victims of a dating or romance fraud than those aged 45–54 (p<0.05).

Model 3: Work-from-home invitations

Although respondents aged 45–54 experienced higher rates of victimisation by fraudulent work-from-home invitations, they were no more likely to be a victim of this particular fraud than respondents in other age categories, holding all other variables constant (p>0.05). However, the model found the likelihood of victimisation declined as income increased—specifically, respondents who earned over $40,000 per annum were less likely to be a victim of a work-from-home fraud than those earning less than $20,000 per annum. These findings indicate that, while age was not a predictor for victimisation by work-from-home fraud, income levels may be a contributing factor to victimisation by this fraud type.

Table 5: Model 1 Logistic regression predicting victimisation by computer support fraud (n=2,585)*

	Coefficient	OR	95% CI	*p* value
<17–24 (n=249) (vs 65+ years)	-1.265	0.282	-2.531 – -0.000	0.050
25–34 (n=429) (vs 65+ years)	-2.248	0.106	-3.759 – -0.732	0.004
35–44 (n=467) (vs 65+ years)	-0.960	0.383	-1.909 – -0.011	0.047
45–54 (n=610) (vs 65+ years)	-1.300	0.273	-2.248 – -0.352	0.007
55–64 (n=568) (vs 65+ years)	-1.568	0.209	-2.611 – -0.524	0.003
Gender male (vs female)	0.257	1.293	-0.407 – 0.921	0.448
Income $20,000–<$40,000 (vs <$20,000)	-0.398	0.672	-1.371 – 0.574	0.423
Income $40,000–<$60,000 (vs <$20,000)	0.383	1.467	-0.459 – 1.226	0.373
Income $60,000–<$80,000 (vs <$20,000)	-1.929	0.145	-4.007 – 0.149	0.069
Income $80,000 and above (vs <$20,000)	-0.177	0.838	-1.180 – 0.826	0.729

*Number of respondents who received an invitation

p<0.001, AUC=0.73, R^2=0.08

Note: the reference age category 65 and over was used as respondents in that age category experienced higher levels of victimisation

Source: ACFT survey 2011 and 2012 [AIC computer file]

Table 6: Model 2 Logistic regression predicting victimisation by dating and romance frauds (n=2,585)*

	Coefficient	OR	95% CI	*p* value
<17–24 (n=249) (vs 45–54 years)	-2.296	0.101	-4.341 – -0.250	0.028
25–34 (n=429) (vs 45–54 years)	-1.949	0.142	-3.420 – -0.478	0.009
35–44 (n=467) (vs 45–54 years)	-0.467	0.627	-1.277 – -0.344	0.259
55–64 (n=568) (vs 45–54 years)	-1.009	0.365	-1.894 – -0.123	0.026
65+ (n=372) (vs 45–54 years)	-1.240	0.289	-2.274 – -0.207	0.019
Gender male (vs female)	-0.316	0.729	-0.957 –0.314	0.325
Income $20,000–<$40,000 (vs <$20,000)	-0.232	0.792	-1.114 –0 .648	0.604
Income $40,000–<$60,000 (vs <$20,000)	-0.327	0.721	-1.214 – 0.560	0.470
Income $60,000–<$80,000 (vs <$20,000)	-1.538	0.215	-2.849 – -0.227	0.022
Income >$80,000 (vs <$20,000)	-0.949	0.387	-1.890 – -0.009	0.048

* Number of respondents who received an invitation

$p<0.01$, AUC=0.70, $R^2=0.06$

Note: the reference age category of 45–54 years was used as respondents in that age category experienced higher levels of victimisation

Source: ACFT survey 2011 and 2012 [AIC computer file]

Table 7: Model 3 Logistic regression predicting victimisation by work-from-home fraudulent invitations (n=2,585)*

	Coefficient	OR	95% CI	p value
<17–4 (n=249) (vs 45–54 years)	0.319	1.375	-0.689 – 1.326	0.535
25–34 (n=429) (vs 45–54 years)	-0.228	0.796	-1.261 – 0.805	0.666
35–44 (n=467) (vs 45–54 years)	-1.347	0.260	-2.875 – 0.182	0.084
55–64 (n=568) (vs 45–54 years)	-0.539	0.583	-1.571 – 0.492	0.306
65+ (n=372) (vs 45–54 years)	0.051	1.052	-0.907 – 1.010	0.917
Gender male (vs female)	0.331	1.392	-0.342 – 1.004	0.335
Income $20,000–<$40,00 (vs <$20,000)	-0.862	0.422	-1.757 – 0.033	0.059
Income $40,000–<$60,000 (vs <$20,000)	-0.989	0.372	-1.893 – -0.086	0.035
Income $60,000 –<$80,000 (vs <$20,000)	-1.297	0.273	-2.438 – -0.156	0.026
Income >$80,000 (vs <$20,000)	-1.519	0.219	-2.674 – -0.363	0.010

*Number of respondents who received an invitation

$p<0.01$, AUC=0.71, r2=0.07

Note: the age reference category of 45–54 years was used as respondents in that age category experienced higher levels of victimisation

Source: ACFT survey 2011 and 2012 [AIC computer file]

Discussion

Prior research has found that, while age may be a risk factor for consumer fraud victimisation, it is not clear which age group is at increased risk (Ross & Smith 2011). Analysis of data from the 2011 and 2012 ACFT surveys found age-related differences both in how fraudulent invitations were delivered and in the levels of victimisation experienced.

Findings from the current study show statistically significant age-related differences in the delivery methods of fraudulent invitations. Overall, email was the most common method of delivering fraudulent invitations; however, those aged 65 and over, were least likely to receive invitations via email. This may be due, in part, to how this age group uses technology and computers. For example, those aged 65 and over may use the internet for other reasons such as online banking, paying bills or accessing government services (ABS 2014) which may not necessarily involve the use of email.

Respondents aged 35 and younger were more likely to receive fraudulent invitations via the internet than other age groups. Respondents aged 65 and over were no more likely than other age categories to receive a fraudulent invitation by a specific delivery method, although they were less likely than other age groups to receive a fraudulent invitation by SMS, the internet or email, or by 'other' means. Past research into older Australians' use of new technologies has found age to be negatively associated with the use of computers and the internet (Chesters, Ryan & Sinning 2013).

The present results show that, of all the fraud types addressed by the survey where a significant relationship between age and victimisation was found, computer support frauds accounted for the

largest differences between age groups. Further analyses show respondents aged 65 and over were more likely than those of other age groups to be victims of computer support fraud.

The findings also show a significant relationship between the provision of personal information and age. The study found younger people (those aged 18–24) sent personal details in response to fraudulent invitations at higher than expected rates. This suggests younger people are more predisposed to supplying their personal information than older respondents, and accords with research by the Australian Law Reform Commission (2008), which examined young people's attitudes to privacy and found they were more likely to provide their personal information in order to receive a discount or win a prize.

There were also age-related differences in fraud victimisation involving financial loss. Respondents aged 65 and over were significantly more likely to send money in response to a fraudulent invitation than those of other age groups, although there was no significant relationship between the amount of money sent and age. With regard to specific fraud types, respondents aged 45–55 were more likely to be victimised by dating and romance frauds. This may indicate that certain lifestyle factors such as divorce, a desire to settle down or loneliness are related to some types of victimisation. While previous research has examined phases of life to identify suitable intervention points to prevent crime (National Crime Prevention 1999), there may also be phases of life during which people are more at risk of fraud victimisation.

Demographic factors such as income levels—which may relate to lifestyle factors—were also found to be predictors of victimisation by work-from-home fraud. Those earning over $40,000 per annum were less likely to be a victim of work-from-home frauds than those earning less than $20,000.

Prevention strategies

The findings of this study may help inform potential age-targeted educational activities, as they demonstrate how respondents receive and respond to fraudulent invitations differently depending on their age. Broad-based education targeting all age groups, in addition to age-specific education, would assist in minimising online fraud risk; age-specific education could be aimed at younger people newly exposed to emerging technologies or at older people, who could benefit from broad-based education about technologies they may be encountering for the first time. However, any such educational campaigns must remain current and be relevant to different age groups. Reisig and Holtfreter (2013) note that although education campaigns are important they have their limitations—people may still engage in risky online behaviour despite being aware of the risks it entails.

Age-targeted education campaigns could also be useful in reducing victimisation arising from fraudulent invitations not received online. The current study found respondents aged 65 and older were more likely to be the victim of a computer support fraud than those of other age groups. Although the majority of such frauds are received by telephone, they exploit a lack of understanding of computers and associated technology. Education campaigns, like those run by OnGuardOnline.gov, that explain how computer protection (eg antivirus) software works could reduce misunderstanding around illegitimate virus protection and security scans.

The findings also indicate that age itself may not necessarily be a risk factor for victimisation, but rather the lifestyle factors associated with different stages of life. For example, certain age groups

were found to be at greater risk of victimisation by dating and romance fraud than others, particularly those aged 45–54. This could arguably be due to life events at different stages of life, rather than actual age-related risk factors. For example, in 2013, the median age at divorce of Australian men was 44.8, and for women it was 42.2 (ABS 2013). In this case, it is not age that creates a specific risk factor but rather life events that occur at certain stages of life for some individuals. Similarly, those aged 25–34 experienced lower than expected levels of victimisation by dating and romance scams. The median age at marriage for Australian men in 2013 was 31.5 years, and for women it was 29.5 years (ABS 2013); both these ages fall within this age group. It could be expected that married people would be less likely to be victims of dating and romance scams.

Online dating and romance services can be traced back to the beginning of the World Wide Web and the commercial internet in the mid-1990s, although the use of online dating services increased after 2005 (Rege 2009). It is possible those most at risk of online dating fraud—respondents aged between 45 and 54 years—are also those least familiar with forming online relationships. Australians lost over $25m to dating and romance frauds in 2013 (ACCC 2014); enhanced education is needed to help individuals identify fraudulent 'dates'.

Another factor associated with the risk of victimisation was income. The ACCC (2014) noted that at some stage of their life, everyone would be vulnerable to fraud. They noted that when people experience financial difficulties they may be less able to recognise and avoid fraudulent invitations. The present research found respondents who earned less than $20,000 per annum were much more likely to be victims of work-from-home frauds than those with higher incomes (see Table 7, model 3). Arguably, those actively seeking employment, or more highly paid employment, are at greater risk of victimisation by work-from-home fraud. To counter this, employment centres and legitimate employment websites could run educational campaigns about employment and work-from-home fraud. Such campaigns could provide information about what legitimate job advertisements should include, such as the type of work to be undertaken, business details and realistic earning potential (Scamwatch 2015).

This study found younger respondents, specifically those aged 18–24, provided personal details in response to fraudulent invitations more often than those in other age categories. Although the provision of personal details or passwords may not result in immediate financial loss, it can have lasting consequences. The ACFT 'Get smarter with your data' campaign for National Consumer Fraud Week 2015 (Scamwatch 2015) sought to educate people of all ages on the importance of protecting one's personal details online. The campaign drew attention to the potential consequences of providing personal information to fraudsters; for example, they may be enabled to access a victim's bank account fraudulently or steal their identity (identity theft).

Existing online safety campaigns aimed at younger people already encourage them to be 'cybersmart' and increase their awareness of the risk of both online sexual predators and consumer fraud (see www.cybersmart.gov.au). This is an important measure, given younger people spend an average of 3.5 hours per day, 6.7 days per week on the internet (ACMA 2009). As more services and products become available online, there will be a need to develop campaigns targeted at all age groups, including older people who may use technology infrequently (Chesters, Ryan & Sinning 2013) and consequently be at greater risk of some consumer frauds, such as online phishing frauds.

Ultimately, awareness and educational campaigns should be targeted at those whose risk of victimisation is higher. What groups are affected may vary depending on exposure to new technologies and lifestyle factors experienced at various stages of life. It is unlikely that broad-based

educational campaigns alone would be effective in reducing consumer fraud victimisation; campaigns targeting those whose lifestyle factors or use of specific technologies make them more vulnerable to fraud would be more suitable than either broad-based online safety campaigns or campaigns designed solely for specific age groups.

References

URLs correct at February 2016

Australian Broadcasting Corporation 2013. In Google We Trust. *Four Corners* 9 September 2013. http://www.abc.net.au/4corners/stories/2013/09/09/3842009.htm

Australian Bureau of Statistics 2014. *Household use of Information Technology, Australia 2012–13*. 8146.0 Canberra: ABS

Australian Bureau of Statistics 2013. *Marriage and divorces, Australia*. 3310.0. Canberra: ABS http://www.abs.gov.au/ausstats/abs@.nsf/mf/3310.0

Australian Bureau of Statistics 2012. *Personal fraud, 2010–2011.* 4528.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbytitle/B634CE9C7619C801CA25747400263E7E

Australian Law Reform Commission 2008. *For your information: Australian Privacy Law and Practice*. ALRC Report 108. Sydney: ALRC. http://www.alrc.gov.au/publications/report-108

Australian Communication and Media Authority 2009. *Cybersmart guide for library staff*. Melbourne: ACMA. http://apo.org.au/resource/cybersmart-materials-public-libraries

Australian Communication and Media Authority 2013. *Like, post, share: Young Australians' experience of social media*. Melbourne: ACMA. http://www.acma.gov.au/theACMA/we-like-we-post-we-share-the-online-lives-of-young-australians

Australian Competition and Consumer Commission 2014. *Targeting scams: Report of the ACCC on scam activity 2013*. Canberra: ACCC. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2013

Blanton K 2012. *The rise of financial fraud: scams never change but disguises do.* Boston, MA: Centre for Retirement Research. http://crr.bc.edu/wp-content/uploads/2012/02/IB_12-5-508.pdf

Budd C & Anderson J 2011. *Consumer fraud in Australasia: Results of the Australasian Consumer Fraud Taskforce online Australia surveys 2008 and 2009*. Technical and Background Paper no. 43. Canberra: AIC. http://aic.gov.au/publications/current%20series/tbp/41-60/tbp043.html

Chesters J, Ryan C & Sinning M 2013. *Older Australians and the take-up of new technologies*. Adelaide, SA: NCVER

Cohen C 2006. Consumer fraud and the elderly: a review of Canadian challenges and initiatives. *Journal of Gerontological Social Work* 46(3/4): 137–144

Cohen L and Felson M 1979. Social change and crime rate trends: A Routine Activity approach. *American Sociological Review* (44): 589

Field A 2013. *Discovering statistics using IBM SPSS statistics* (4th edition). SAGE Publications: London

Fischer P, Lea SEG & Evans KM 2013. Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology* 43: 2,060–2,072

Holtfreter K, van Slyke S & Blomberg TG 2005. Sociolegal change in consumer fraud: Frome victim-offender interactions to global networks. *Crime, Law and Social Change* 44: 251–275.

Jorna P & Hutchings A 2013. *Australasian Consumer Fraud Taskforce: Results of the 2012 online consumer fraud survey*. Technical and Background Paper series no. 56. Canberra: AIC. http://www.aic.gov.au/publications/current%20series/tbp/41-60/tbp056.html

Muscat G, James M & Graycar A 2002. Older people and consumer fraud. *Trends & Issues in Crime and Criminal Justice* No. 220. http://www.aic.gov.au/publications/current%20series/tandi/201-220/tandi220.html

National Crime Prevention 1999. *Pathways to prevention: Developmental and early intervention approaches to crime in Australia*. Canberra: Attorney-General's Department

News.com.au 2009. *Queensland farmers fall victim to online dating scams*. http://www.news.com.au/finance/money/queensland-farmers-fall-victim-to-online-dating-scams/story-e6frfmd9-1225787738234

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

Quist J 2013. Scams targeting seniors. *Today Tonight.* http://www.7perth.com.au/view/today-tonight-articles/today-tonight-scams-targeting-seniors

Rege A 2009. What's love got to do with it? Exploring online dating scams and identity fraud*. International Journal of Cyber Criminology*. 3(2): 494–512.

Reisig MD & Holtfreter K 2013. Shopping fraud victimization among the elderly. *Journal of Financial Crime* 20(3): 324–337.

Reyns BW 2013. Online routines and identity theft victimisation: Further expanding Routine Activity Theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency* 50(2): 216–238.

Ross M, Grossmann I & Schryer E 2014. Contrary to psychological and popular opinion there is no compelling evidence that older adults are disproportionately victimised by consumer fraud. *Perspectives on Psychological Science* 9(4): 427–442.

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

Scamwatch 2015. *2015 National Consumer Fraud Week–Get smarter with your data*. http://www.scamwatch.gov.au/content/index.phtml/itemId/693900

Scheibe S et al. 2014. Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic Applied Social Psychology*. 36(3): 272–279

Smith RG, Holmes MN & Kaufmann P 1999. Nigerian advance fee fraud. *Trends & Issues in Crime and Criminal Justice* No. 121. Canberra: AIC

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

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

Penny Jorna is a research analyst within the Transnational, Organised and Cyber Crime program at the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy Director Research, 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

©Australian Institute of Criminology 2016

GPO Box 1936
Canberra ACT 2601, Australia
Tel: 02 6243 6666

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government

aic.gov.au