Australian Government
Australian Institute of Criminology

Australasian Consumer Fraud Taskforce: Results of the 2013 online consumer fraud survey

Penny Jorna

AIC Reports
Technical and Background Paper 58

Australasian Consumer Fraud Taskforce: Results of the 2013 online consumer fraud survey

Penny Jorna

AIC Reports
Technical and
Background Paper
58

aic.gov.au

ISSN 1836-2052
ISBN 978 1 922009 93 7

Published by the Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601
Tel: (02) 6260 9200
Fax: (02) 6260 9299
Email: front.desk@aic.gov.au
Website: aic.gov.au

Please note: minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

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

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **aic.gov.au**

Contents

Figures

Tables

Foreword

Each year since 2007, the Australian Institute of Criminology (AIC) has collected information on consumer scams by conducting an online survey of Australians who have received scam invitations during the preceding 12 months. The research is conducted on behalf of the Australasian Consumer Fraud Taskforce (ACFT), which comprises 22 government regulatory agencies and departments in Australia and New Zealand who work alongside private sector, community and non-government partners to prevent fraud of this nature. The annual survey seeks to obtain a snapshot of the public's exposure to consumer scams, to assess the range of ways in which scams can affect victims and their families, to determine how victims respond and to identify emerging typologies, and look at issues that could be used to inform fraud prevention initiatives. Survey respondents are not representative of the whole Australian population, as the sample is made up of only those individuals who choose to opt in; although in 2013, over 1,000 people completed the survey with good levels of representation from all states and territories, and other demographic categories.

This report presents the results of the 2013 survey conducted in conjunction with the 2013 National Consumer Fraud Week campaign, 'Outsmart the scammers', which was aimed at promoting consumer awareness of scams related to shopping online. Australians are increasingly buying goods and services online, taking advantage of the speed, convenience and the often greater choice that the internet can offer. Scammers have taken advantage of this trend to target consumers for involvement in scams. Online shopping awareness campaigns target both buyers and sellers to educate the public on reducing the risks of being scammed (ScamWATCH 2013).

As in previous years, a high proportion of respondents to the survey had received a scam invitation (97%), with just over a third of the respondents responding to the scam invitation in some way. Last year, four percent of respondents reported having lost money to a scam, with the median amount of money reported as being lost per incident was $2,150—just over $1,110,000 lost in total. Fraudulent lottery and prizes wins were the most prevalent scam type experienced by respondents in 2013. While email remained the most commonly used method by which scams were delivered, consistent with previous years, scams delivered via landline and mobile telephones continued to increase.

This report also includes some additional information on relationship scams; that is, romance or dating scam invitations received by scammers. Relationship scams are the subject of the 2014 consumer fraud awareness week held in June 2014. The AIC scam survey has found in previous years that scams involving dating or romance-type scenarios are not as widely received by respondents as other scam types, although they are generally the type of scam that causes the largest financial losses to victims.

Acknowledgements

This paper makes use of information provided by members of the Australasian Consumer Fraud Taskforce. The views expressed are those of the authors alone and do not necessarily represent the views or policies of the government agencies represented on the Taskforce or its partners.

This paper would not have been possible without those who gave up their time to participate in the online survey. Particular thanks go to those participants who have responded to previous Australasian Consumer Fraud Taskforce surveys. The author would like to thank Dr Alice Hutchings for her advice and guidance with the restructure of the survey.

Acronyms

ABS	Australian Bureau of Statistics
ACCC	Australian Competition & Consumer Commission
ACFT	Australasian Consumer Fraud Taskforce
AIC	Australian Institute of Criminology
SMS	Short message service

Executive summary

The Australasian Consumer Fraud Taskforce (ACFT) includes 22 government regulatory agencies and departments in Australia and New Zealand that work alongside private sector, community and non-government partners to prevent fraud. The ACFT has conducted a range of fraud prevention and awareness-raising activities since 2006. One key activity of the ACFT is to hold an annual consumer fraud survey to obtain a snapshot of the public's exposure to consumer fraud/scams, to assess their impact, to determine how victims respond and to identify emerging typologies and issues. The Australian Institute of Criminology (AIC) as a member of the ACFT and chair of the research subgroup hosts the survey on behalf of the ACFT. It should be noted that as the survey participants were not randomly sampled, the survey findings are therefore not representative of the general population.

This report presents the results of the 2013 survey, which ran for six months commencing from 1 January. This period encompassed the National Fraud Prevention week, which coincides with global awareness-raising activities. The theme of the 2013 campaign was 'Outsmart the scammers', which aimed to raise awareness about consumer fraud risks while shopping online. The survey explored consumer fraud where respondents were contacted by phone, SMS, email, letter, via the internet and/or in person by someone who they did not know in relation to:

- having won a lottery or some other prize (lottery scams);
- a request for assistance to transfer money out of another country (such as Nigeria) (advance fee frauds);
- a notification of an inheritance (inheritance scams);
- a request by a business to confirm your personal details or passwords (phishing scams);
- a request to supply you with financial advice (financial advice scams);
- a request to buy, sell or retain securities or other investments (boiler-room scams);
- an opportunity to work from home (a front for money laundering) (work from home scams);
- pursuing a personal relationship that turned out to be false (dating scams);
- a person representing themselves as someone from a computer support centre (computer support scams); and
- other fraud types.

The survey was made available for completion on the AIC's website. Participants who did not reside in Australia or New Zealand were excluded from the survey, as were invalid responses. In 2013, 1,059 participants completed the survey. Outliers, typically very large loss figures from respondents who appeared to have misunderstood the question, were removed for the analysis, which left 1,034 responses for analysis.

The 2013 survey suffered from a number of constraints, which meant that comparisons with previous years were not possible. These constraints included a change in the reporting time period and structural changes in the survey. There are also additional limitations with the survey that make it difficult to generalise its findings to the greater Australasian population, particularly the self-selection bias of the survey design. As the sample was not randomly selected, those who participated in the survey may differ from the general population in terms of their experience of scams.

Delivery of scams

The 2013 survey asked respondents about the types of scams they had received, as well as how the scam invitations had been delivered to them. Results indicated that:

- Ninety-seven percent of respondents reported having received at least one scam invitation in the 12 months preceding the survey.
- The most common type of scams reported to have been received were lottery scams (received by 69% of the total sample), computer support centre scams (58%) and phishing scams (52%).
- The least common type of scams received were boiler-room scams, reported by 11 percent of the total sample.
- Email was the most common scam delivery method, with 78 percent of the sample reporting having received a scam this way.

Responding to scam invitations

Responding to scam invitations included requesting further information, providing personal details or suffering a financial loss. Key findings included:

- Thirty-four percent of the respondents responded in some way to a scam invitation in the 12 months preceding the survey.
- Six percent in sent their personal details.
- Four percent of respondents reported a financial loss.
- Seven percent reported both sending their personal details and having experienced a financial loss.
- The median amount reported lost to scams was $2,150. With outliers removed, a total financial loss of $1,110,106 was reported.
- The top two reasons given for not responding to scam invitations were that the respondent had received similar offers before and thought they were scams (54.2% of the total sample) and 'had seen/heard this was a type of scam in the media or from a public source' (50.6% of the total sample).

Victim demographics

Victims were defined as respondents who had provided their personal details and/or suffered a financial loss as the result of replying to a scam invitation. Analysis of the demographic variables of scam victims indicated that:

- Of the survey respondents who disclosed their gender (98%), 16.1 percent of respondents experiencing victimisation in 2013 were females and 12.9 percent were male.
- In 2013, the age category that reported the highest percentage of victimisation was 'over 65' years (22% of total respondents within that age category).
- In 2013, the income category that reported the highest percentage of victimisation was $20,000 to less than $40,000 (26% of total respondents within that income category).

Reporting consumer fraud

Respondents were asked whether they had reported consumer fraud incidents to another person or organisation. Key findings included:

- In 2013, 74 percent of the total sample reported a scam to at least one person or organisation.
- Family and friends were the most common recipients of scam complaints, with 43 percent of the total sample reporting to this category in 2013.
- The most common reasons provided for not reporting scams were 'unsure of which agency to contact' (40% of the total sample), 'I didn't think anything would be done' (32%) and 'not worth the effort' (29%).
- The most common reasons for reporting scams were 'wanted to prevent others from being scammed' (39% of the total sample), 'knew it was the right thing to do' (28%) and 'to assist in the investigation of an offence' (26%).

Perceptions of consumer fraud

Respondents were asked whether they considered each scam type to be *a crime*, *wrong but not a*

crime, or *just something that happens*. The results indicated that:

- In 2013, the top three scam types to be considered a crime by respondents were advance fee fraud (85%), phishing (85%) and computer support scams (80%).

Recommendations for future campaigns

The report findings were used to develop recommendations for future education and awareness campaigns. It was suggested that future campaigns should focus on:

- developing a greater understanding of the consequences of consumer fraud, not just the financial impact, but the psycho-social aspects and the lasting effects that falling victim to a scam may have;
- changing the perception that scams (a type of consumer fraud) are not victimless crimes and victims are not necessarily gullible, greedy or doing something illegal;
- educating the public on what to do if they have been the victim of a scam or if they are receiving a large amount of scam invitations. The survey has continually found that respondents are unaware of to whom they should report consumer fraud.

Introduction

The purpose of this paper is to report the findings from the ACFT 2013 survey in order to provide an overall picture of the nature of consumer fraud in Australasia.

Australasian Consumer Fraud Taskforce

The ACFT, chaired by the Australian Competition & Consumer Commission (ACCC), was formed in March 2005 and is comprised of 22 Australian and New Zealand governmental regulatory agencies and departments that have responsibility for consumer protection regarding frauds and scams, including consumer protection and policing agencies at the state and federal levels. The ACFT also has a range of partners from the community, non-government and private sector that have an interest in increasing the level of scam awareness in the community. The aim of the ACFT is to apply a coordinated approach to reduce the number of incidents and the impact of consumer frauds and scams. In order to meet this aim, the ACFT coordinates a week-long information campaign each year, timed to coincide with global consumer fraud prevention activities.

Since 2006, the AIC has conducted an annual survey to assess consumer fraud experiences. See Smith (2007) for the results of the pilot study conducted in 2006, Smith and Akman (2008) for the 2007 survey results, Budd and Anderson (2011) for the results of the 2008 and 2009 surveys, Hutchings and Lindley (2012) for the 2010 and 2011 survey results, and Jorna and Hutchings (2013) for the 2012 survey results. The survey reported in this paper ran for six months between January and June 2013, which included the annual Fraud Week conducted by the Taskforce.

Defining consumer fraud and scams

According to the Australian Bureau of Statistics (ABS), scams are defined as

> a fraudulent invitation, request, notification or offer, designed to obtain someone's personal information or money or otherwise to obtain a financial benefit by deceptive means (ABS 2012: np).

While the terms 'fraud' and 'scam' are often used interchangeably, scams are generally considered to be a subcategory of fraud, with 'fraud' referring to matters involving dishonesty and deception. There are a range of consumer fraud activities that may be classified as scams. Nine common types of consumer frauds were explored in the 2013 ACFT survey namely:

- advance fee fraud (money transfer scams);
- dating scams;
- financial advice scams;
- boiler-room scams;
- inheritance scams;
- lottery scams;
- phishing;
- work from home scams; and
- computer support scams.

An additional 'other' category was offered to respondents for scam types that did not fall into the supplied categories. 'Boiler-room scams' was a new scam type for the 2013 survey. Its inclusion was as a result of consultation among the ACFT members after the release of the Australian Crime Commission (ACC & AIC 2012) factsheet *Organised Investment Fraud*. Definitions for each scam type is provided in Table 1.

Table 1 Common scams and their definitions

Advance fee fraud/Nigerian 419 scams	Advance fee frauds or Nigerian 419 scams have existed throughout history and have adapted to advances in technology. Generally, these scams are communicated by email or letter seeking assistance to transfer a large amount of money overseas. These are the most commonly complained about scams in Australia according to the ACCC
Dating/social networking scams	Dating and social networking scams may be conducted through illegitimate and legitimate dating or social networking websites and often take the form of requiring a payment for each email sent and received by a potential match. Alternatively, scammers may hook victims by posing as a potential partner and then claiming to have an ill relative or severe financial problems and seek financial assistance from the 'love interest' they met on the site. Due to the trust already established, victims may be more easily duped and in disbelief when scammers cease communication after money has been sent
Financial advice scams	Financial advice scams are undertaken by scammers cold calling from overseas offering advice on shares, mortgage or real estate 'investments', 'high-return' schemes, option trading or foreign currency trading. The advice generally does not lead to increased wealth
Boiler-room scams	Requests to buy, sell or retain securities or other investments (including superannuation investments). Usually offered through cold calling by scammers who seek to sell worthless shares or investments to recipients
Inheritance scams	Inheritance scams are usually sent by a fake lawyer or bank purporting to act for a deceased estate and may falsely claim that a distant relative has died and through some means has left the target a large inheritance
Lottery scams	A lottery scam may be delivered by email, text message or pop-up screen falsely claiming the target has won a prize or competition
Phishing	Phishing refers to emails that deceive people into giving out their personal details and banking information. They are increasingly being sent by SMS
Work from home scams	Work from home scams are often promoted through spam emails or advertisements on noticeboards; however, are usually not advertising real jobs. Work from home scams may be fronts for illegal money-laundering activities or pyramid schemes
A person representing themselves as someone from a computer support centre	Computer support centre scams occur when recipients receive (mainly) telephone calls from scammers claiming they are from well-known computer manufacturers or businesses that can fix problems with the recipients' computers. Scammers may ask for money, personal details or passwords or seek to sell worthless products to fix computers

Source: AIC ACFT Survey 2013; ACCC 2013, 2011

Method

The ACFT online surveys have been designed to examine the types of consumer fraud that respondents were exposed to during the previous 12 months. The surveys sought to measure:

- the extent of consumer scams;
- the types of frauds or scams that attracted the most victims;
- the factors relevant to victimisation; and
- what affects reporting of scams.

Each year, between 1 January and 31 March, an anonymous online survey hosted by the AIC has been used to collect data on scams. However, for the 2013 survey, the timeframe was extended to include the period from 1 January to 30 June 2013. This survey timeframe was chosen to correspond with the ACFT fraud awareness campaign, which ran from 17 to 23 June in 2013, as well as collect data before and after the campaign period to assess the impact of the campaign on participation rates.

The online survey method is considered the most cost-effective way to gather information on consumer fraud in Australia and New Zealand as it is accessible by a large public audience and does not involve any administration costs such as postage or interview expenses. It also allows respondents to remain anonymous, which was considered advantageous as the survey asked questions about personal experience and possible victimisation.

The online survey was advertised in a variety of forums, including as a hyperlink via the SCAMwatch website, through government agency websites, via posters and pamphlets, and through the media. ACFT members were asked to publicise the survey internally and SCAMwatch employees allowed callers to the SCAMwatch hotline to complete the survey over the phone.

Survey questions

The survey contained a mixture of closed responses and open-ended, qualitative questions about the respondent's exposure to, and victimisation from, consumer scams (see *Appendix 1*). These questions were developed in consultation with the ACFT committee members. Information was sought on the following consumer scams:

- lottery scams;
- advance fee fraud;
- inheritance scams;
- phishing;
- financial advice scams;

- boiler-room scams;
- work from home scams;
- dating scams; and
- computer support scams.

An 'other' response category was also included to capture additional scams. Questions related to respondents' experiences of consumer fraud in the 12 months prior to the survey, as well as their personal demographics and awareness of ACFT activities. As such, the survey period could incorporate up to 18 months in the survey period.

There were substantial changes to the 2013 survey compared with previous years. The first change was the inclusion of boiler-room scams as a scam category. The other major change was a restructure of the survey. Rather than asking questions for all potential scam invitations, the survey was structured so that respondents were only asked additional questions pertaining to contact with scammers and potential victimisation if they had received an invitation to that particular scam.

Media coverage

A search of media databases for the periods 1 January 2013 to 30 June 2013 found 10 newspaper articles inviting readers to participate in the survey. These were:

- The Australian Institute of Criminology has called on Canning residents to have their say in the 2012 scam survey. *The Canning Times* 22 January, 2013.
- Help fight scammers. *The Melville Times* 5 February, 2013.
- Survey a vital weapon in war on scammers. *Cockburn Gazette* 15 January, 2013.
- The Australian Institute of Criminology in partnership with the Australasian Consumer Fraud Taskforce, is conducting its annual survey to better understand the trends and impacts of online fraud. *Cockburn Gazette* 22 January, 2013.
- Survey to track scams. *Stirling Times* 15 January, 2013.
- Survey helps stop scammers. *Eastern Reporter* 22 January, 2013.
- Survey to help stop scammers. *Southern Gazette* 29 January, 2013.
- School news. *Cranbourne Leader* 30 January, 2013.
- Scam survey. *Mordialloc-Chelsea Leader* 16 January, 2013.
- Crime survey aimed at victims of scams. *The Whitehorse Leader* 16 January, 2013.

Radio interviews conducted with AIC staff in 2013 also promoted the survey and sought respondents. These included an interview on Mix 104.9 Darwin, Northern Territory, an interview on National Radio News on 9 January and an interview with Leon Delaney on Radio 2SM Sydney on 10 January.

In addition to the partner agencies of the ACFT including links to the survey and details about consumer fraud on their websites, the survey was advertised on the Neighbourhood Watch website and included in their newsletter distributed to households.

Additional media reports during the week-long campaigns that did not mention the survey may have nevertheless generated visits to the websites where links to the survey were provided. A search of media databases identified 36 additional newspaper articles published between 17 and 23 June 2013 that discussed consumer fraud (refer to *Appendix 2*).

Limitations of the survey

The 2013 AIC survey experienced the same methodological constraints as those identified in previous years (see Budd & Anderson 2011; Hutchings & Lindley 2012; Jorna & Hutchings 2013; Smith & Akman 2008). Limitations associated with the relatively small sample sizes and the self-selection bias of the samples make generalising the findings to the wider population problematic, particularly as those who have received a scam invitation and/or fallen victim may be more likely to complete the survey than those who have not. Directly completing the survey was also limited to those who had computer access; however, this was not considered overly restrictive, as SCAMwatch employees were able to complete a survey over the phone with respondents.

It can also be difficult to measure fraud incidents within a given timeframe as it is not always easy to determine when fraud occurs due to the time lapse between when scams are received or carried out, identified by the victim and then reported (if indeed they are). The reference period for the 2013 AIC online survey was the previous 12 months and respondents were asked about whether they had received and responded to scams in this time. As the 2013 survey period encompassed January to June 2013, this could potentially include 18 months within the survey period. It is possible that some incidents may have been forgotten by respondents, or respondents incorrectly recalled dates and events. In addition, there are general problems common with the use of surveys that are also relevant to the ACFT survey, such as the potential for respondents to not understand the questions being asked. There is also the difficulty that there is no way to determine whether the responses given are accurate reflections of the events reported. As a result, the survey results cannot provide a robust measurement of consumer fraud victimisation rates in Australasia, nor of the success of the 2013 Fraud Awareness week. The results are also unable to identify whether the campaign increased people's awareness of consumer frauds or scams.

Due to the limitations of the data as outlined above, descriptive statistics were predominantly used to report the results, particularly frequency distributions and percentages. As the survey was designed to capture information relating to respondents residing in Australia or New Zealand, respondents who indicated they resided elsewhere were excluded from the sample. Outliers—typically very large loss figures from respondents who appeared to have misunderstood the question—were removed for the analysis.

The following sections present the key results from the 2013 ACFT survey.

The 2013 consumer fraud survey results

Sample characteristics

Between 1 January and 30 June 2013, 1,059 people responded to the survey hosted on the AIC's website, www.aic.gov.au. Twenty-five respondents were removed as they did not reside in Australia or New Zealand, leaving 1,034 responses that formed the sample subject to analysis.

Seventy percent of respondents (n=727) reported that they completed the survey in their capacity as a working member of the public, (not part of an ACFT partner agency) while a further 17 percent (n=174) of respondents characterised themselves as retirees. Six respondents (0.6%) were members of the police, 24 respondents (2.3%) were employed by an ACFT government agency, four respondents (0.4%) were employed by an ACFT private sector partner and 80 respondents (7.7%) were employed by another government agency.

Websites were the most popular way respondents were directed to the survey, with the SCAMwatch site referring 358 respondents (35%) and other government websites referring 268 respondents (26%). The media generated 110 responses (11%), posters and pamphlets directed eight respondents (0.8%) and 58 respondents (6%) were referred to the survey by another agency. A further 57 respondents (6%) found out about the survey through word of mouth. Two hundred and fifty-eight respondents advised that they had found out about the survey through other means, such as from their schools, Neighbourhood Watch pamphlet and from respondents' own banks.

Twenty percent (n=207) were aware of the ACFT's campaign and 14 percent (n=142) were aware of campaigns that had been run in previous years. Forty-three respondents (4%) had completed the 2012 survey, 25 respondents (2%) had completed the 2011 survey, 12 (1%) had completed the 2010 survey, seven (0.7%) had completed the 2009 survey and 930 respondents (90%) had not previously completed the survey.

There was an average of 39 responses a week in the 24 weeks prior to the 2013 campaign (n=938); 77 participants completed the survey during the week-long campaign, while the remaining 19 participants completed the survey in the week following the campaign.

Respondents were asked why they chose to complete the survey (multiple responses were allowed). Most respondents (n=765, 74%) wanted to 'assist in

research to combat scammers'. A further 447 participants (43%) completed the survey because 'they had received scams, but not been scammed'; 235 respondents (23%) 'wanted to learn more about scams' and 193 respondents (18.7%) had 'recently been scammed', although it should be noted that this was a larger number of respondents than the number in the survey who advised they were victims.

Demographics

Females comprised 59 percent of the sample (n=610), while males comprised 38.2 percent of the sample (n=395). Twenty-nine respondents (2.8%) did not disclose their gender. Table 2 shows the breakdown of respondents by their age group.

As shown in Figure 1, most respondents resided in New South Wales (27.6%, n=286), Western Australia (20.1%, n=207), Victoria (18.8%, n=194) and Queensland (14.9%, n=159). Eleven respondents (1.1%) resided in New Zealand. South Australia (4.9%, n=51), Tasmania (1.5%, n=15) and the Northern Territory (1.4%, n=14) were the least represented states and territories in Australia.

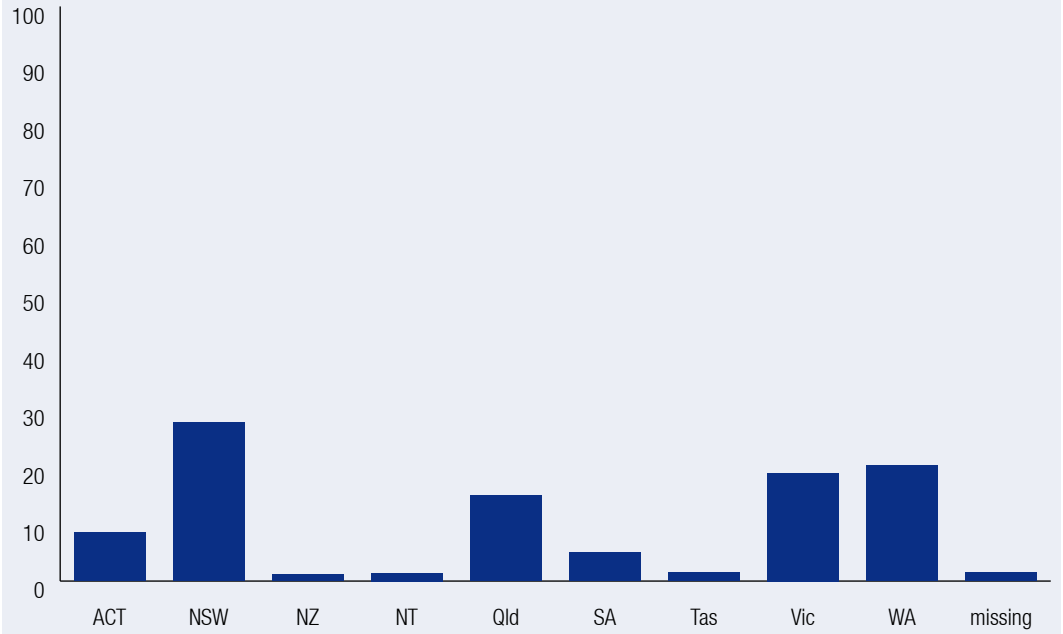
When asked about income, over one-quarter of respondents (n=293, 28.3%) preferred not to disclose their income level and a further three percent (n=39) did not respond to the question. Slightly less than 40 percent of the respondents, 375 (36.3%) earned an income somewhere in the middle categories provided ($20,000 to $80,000), while 15.1 percent (n=156) earned less than $20,000 and 16.5 percent (n=171) earned in excess of $80,000 per annum (see Figure 2).

Table 2 Respondents by age

Age category (years)	n	%
17 and under	33	3.2
18–24	51	4.9
25–34	135	13.1
35–44	179	17.3
45–54	226	21.9
55–64	221	21.4
Over 65	173	16.7
Missing	16	1.6
Total	1,034	100

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

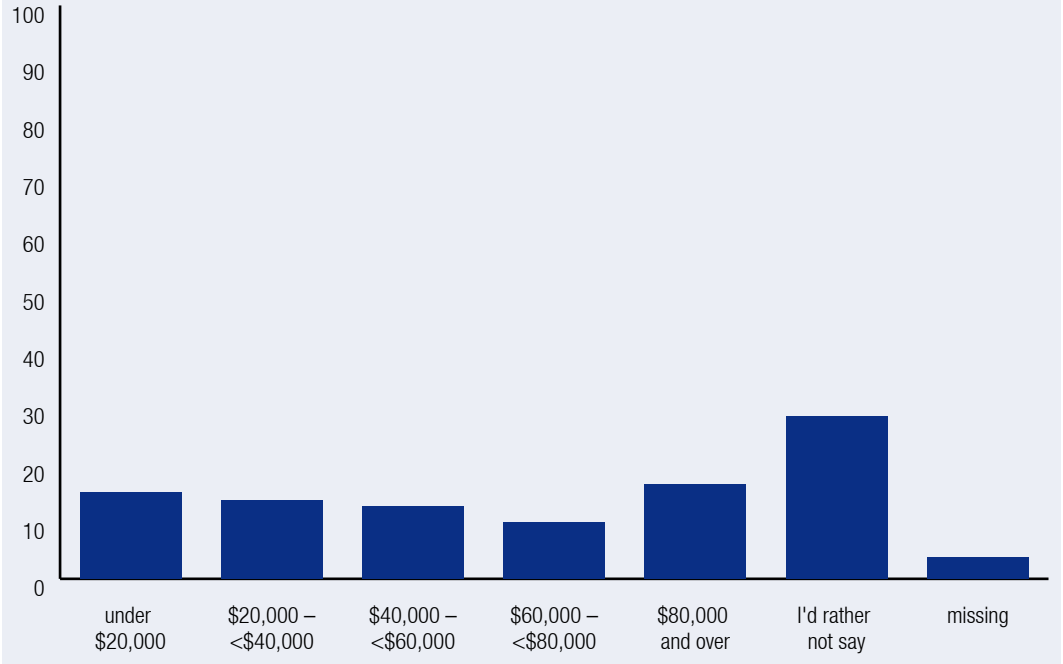
Figure 1 Respondents by region (% of respondents)



Note: Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Figure 2 Respondents by annual income (% of respondents)



Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Receiving scams

Of the 1,034 survey participants in 2013, 1,003 (97%) had received at least one scam invitation. The number and percentage of respondents who had received at least one scam invitation by scam type is provided in Table 3. Respondents may have received invitations for more than one scam type. Lottery scams were the most common type of scam received, reported by 692 (66.9%) of the survey participants. This was followed by computer support centre scams (received by 56.3% of survey participants and 58.0% of those who had received a scam invitation). The least likely type of scam invitation reported to have been received were boiler-room scams, received by 115 of the survey respondents, representing 11.5 percent of the sample who had received a scam invitation and 11.1 percent of the total sample.

Details of the types of delivery methods by which respondents reported receiving scams are provided in Table 4. It is noted that participants could have received more than one scam invitation; therefore, multiple responses are recorded. Email was the most popular delivery method, with 78.1 percent of respondents who had received a scam invitation receiving at least one invite this way. Consistent with previous years, telephone was also a common delivery method for scam invitations with 689 (68.7% of those who had received a scam invitation) respondents receiving scam invitations via that method.

Respondents were asked how many times over the previous 12 months they had received scams by each delivery method (see Figure 3). The results indicate that email is not only the most common scam delivery method, but also that participants received multiple scams in this way.

Table 3 Scam invitations received by scam type

Scam type	Received scam invitation (n)	Received a scam invitation (%) (n=1,003)	Total sample (%) (n=1,034)
Lottery scams	692	69.0	66.9
Advance fee fraud	482	48.1	42.8
Inheritance scams	364	36.3	36.6
Phishing	522	52.0	45.0
Financial advice scams	186	18.5	22.8
Boiler-room scams	115	11.5	11.1
Work from home scams	366	36.5	39.3
Dating scams	234	23.3	13.1
Computer support scams	582	58.0	56.3
Other	312	31.1	30.2

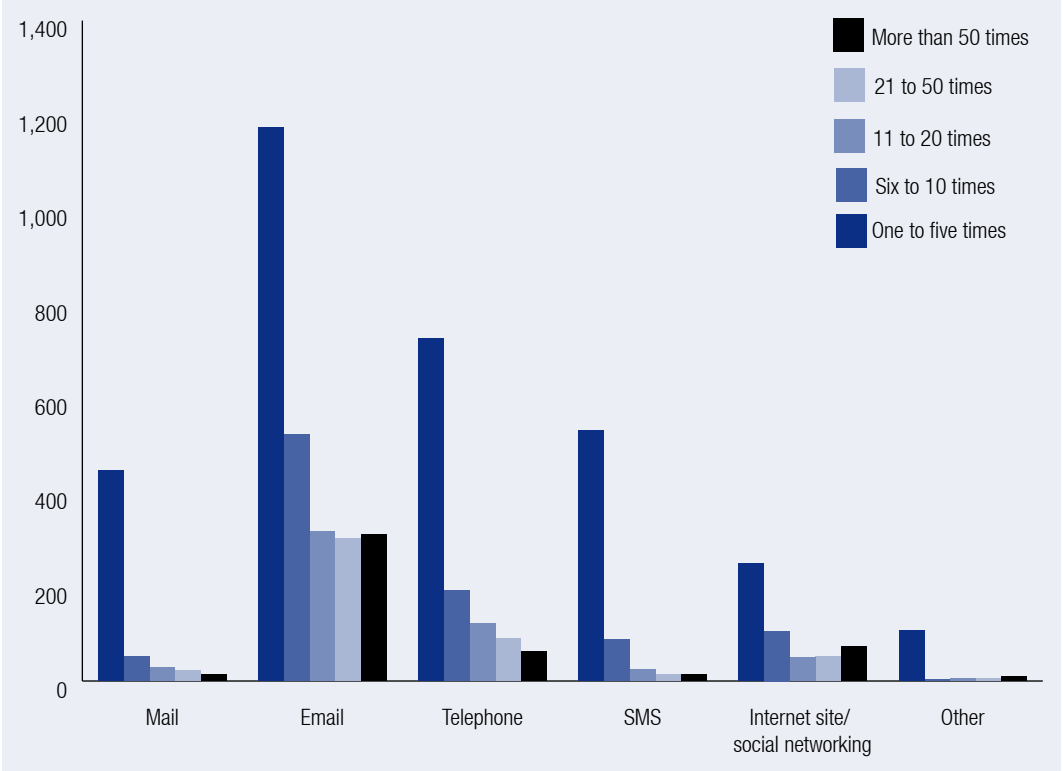
Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Table 4 Scams by delivery method

Method of delivery	Received a scam invitation (n)	Received a scam invitation (%) (n=1,003)	Total sample (%) (n=1,034)
Mail	337	33.6	32.6
Email	783	78.1	75.7
Telephone	689	68.7	66.6
SMS	447	44.6	43.2
Internet site/social networking	281	28.0	27.2
Other	83	8.3	8.0

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Figure 3 Number of scams received by delivery method (n)



Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Responding to scams

During the 12 months prior to the survey, 338 (33%) survey participants responded to a scam invitation by way of requesting further information, providing personal details or suffering a financial loss. This represented 34 percent of those who had received a scam invitation during the 12 month period.

Fifteen percent of the sample who had received an invitation sent their personal details, suffered either a financial loss or both in response to at least one a scam (n=153, 14.8% of the total sample). Sixty-four participants (6.4% of the sample who received a scam invitation and 6.2% of the total sample) sent their personal details only, 37 participants (3.7% of the sample who received a scam invitation and 3.6% of the total sample) suffered a financial loss only and 65 participants (6.5% of the sample who received a scam invitation and 6.3% of the total sample) lost money as well as sent their personal details.

The number of respondents who provided personal details or lost money to each type of scam, as well as the percentage of the total sample, the percentage of the sample who received any type of scam and the percentage of the sample who received that particular type of scam invitation is provided in Tables 5 and 6. Some respondents provided personal details and/or lost money as the result of multiple scams.

In the 2013 survey, none of the respondents indicated that they had lost money to a financial advice scam. Work from home scams and inheritance scams were the scam invitations least likely to result in the reported loss of personal details. The scam types with the highest conversion rates; that is, the scam types that led to more respondents sending money were advance fee frauds (1.7% of victims who had received a scam invitation of that nature) and dating or social networking scams (1.7% of victims who sent money who had received a scam invitation of that type). Dating and social networking scams continued to be among the most likely to lead to a financial loss despite not being as prevalent as other scams, with two percent of the sample who received a dating and social networking scam invitation reporting the loss of personal details, which resulted in losses of $536,779.76. These are the largest losses of any scam type.

Of the 153 victims who reported having suffered a financial loss, 94 (76%) disclosed the amount. This reportedly ranged from $5 to $2,000,000. With outliers removed ($2,000,000 reportedly lost due to a lottery scam), the reported financial loss totalled $1,110,106.66, ranging from $5 to $110,000 (mean=$11,810, median=$2,150).

Participants were able to select multiple responses when asked why they did not respond to scam invitations (see Table 7). The most common reasons for not responding to scams included ‘had received similar offers and thought they were scams’ (reported by 54.2% of the total sample), ‘had seen/heard this was a type of scam in the media or public source’ (50.6% of the total sample), or ‘something was not quite right with the offer or invitation’ (45.4% of the total sample).

Table 5 Loss of personal details by scam type

Scam type	Provided personal details (n)	Received a scam invitation (%) (n=1,003)	Total sample (%) (n=1,034)	Received an invitation to that type of scam (%)
Lottery scams	8	0.8	0.8	1.2
Advance fee fraud	8	0.8	0.8	1.7
Inheritance scams	4	0.4	0.4	1.1
Phishing	22	2.2	2.2	4.2
Financial advice scams	4	0.4	0.4	2.2
Boiler-room scams	2	0.2	0.2	1.7
Work from home scams	4	0.4	0.4	1.1
Dating or social networking scams	7	0.7	0.7	3.0
Computer support scams	13	1.3	1.3	2.2
Other	11	1.1	1.1	3.5

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Table 6 Loss of money by scam type

Scam type	Suffered a financial loss (n)	Received a scam invitation (%) (n=1,003)	Total sample (%) (n=1,034)	Received an invitation to that type of scam (%)
Lottery scams	5	0.5	0.5	0.7
Advance fee fraud	8	0.8	0.8	1.7
Inheritance scams	1	0.1	0.1	0.3
Phishing	1	0.1	0.1	0.2
Financial advice scams	0	0	0	0
Boiler-room scams	0	0	0	0
Work from home scams	2	0.2	0.2	0.5
Dating or social networking scams	4	0.4	0.4	1.7
Computer support scams	9	0.9	0.9	1.5
Other	13	1.3	1.3	4.2

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Table 7 Reasons for not responding to scams received			
Reason for not responding	n	Received an scam invitation (%) (n=1,003)	Total sample (%) (n= 1,034)
Seemed too good to be true	442	44.1	42.7
Had received similar offers and thought they were scams	560	55.8	54.2
Had seen or heard this was a scam in the media or from a public source	523	52.1	50.6
Was told it was a scam by someone I knew	180	17.9	17.4
Someone I know was a victim of a scam	82	8.2	7.9
I wanted to respond but I could not afford to participate	10	1	1
Something was not quite right with the offer or invitation	469	46.8	45.4
Offer was identified as spam/unsafe by internet filter	254	25.3	24.6
Other	137	13.7	13.2

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Victim demographics

For the purpose of this report, scam victims were defined as those who had provided scammers with their personal details and/or suffered a financial loss as the result of a scam. Of the 153 victims who had lost personal details or suffered a financial loss as the result of the scam, 98 (64.1%) identified themselves as female, 51 (33.3%) identified themselves as male and four (2.6%) declined to reveal their gender. Therefore, of the respondents who disclosed their gender, 16.1 percent of the 610 female respondents experienced victimisation, compared with 12.9 percent of the 395 males.

The age of victims, including the percentage of total respondents within that age category who reported being a victim, is shown in Table 8.

Table 9 shows victims' annual income levels, as well as the percentage of total respondents within that income category who reported victimisation.

Table 10 shows victims by the region in which they resided, as well as the percentage of total respondents within that region who reported victimisation. Most victims resided in New South Wales (n=41, 26.8% of the sample who reported victimisation), Western Australia (n=32, 20.9% of the sample who reported victimisation) and Queensland (n=27, 17.6% of the sample who reported victimisation). Four of the respondents residing in New Zealand reported victimisation and as there were 11 respondents from New Zealand, this resulted in a 36 percent victimisation rate of respondents from within that region.

Table 8 Victims by age

Age category (years)	n	%	Respondents within that age category (%)
17 and under	0	0	0
18–24	8	5.2	15.7
25–34	17	11.1	12.6
35–44	24	15.7	13.4
45–54	31	20.3	13.7
55–64	33	21.6	14.9
Over 65	38	24.8	22.0
Missing	2	1.3	12.5

Note: Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Table 9 Victims by annual income

Annual income	n	%	Respondents within that income category (%)
Less than $20,000	31	20.3	19.9
$20,000–<$40,000	40	26.1	28.2
$40,000–<$60,000	21	13.7	16.0
$60,000–<$80,000	10	6.5	9.8
Over $80,000	11	7.2	6.4
I'd rather not say	33	21.6	11.3
Missing	7	4.6	17.9

Note: Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Table 10 Victims by region

Region	n	Percentage of victims	Percentage of victims within that region
Australian Capital Territory	13	8.5	14.9
New South Wales	41	26.8	14.3
New Zealand	4	2.6	36.4
Northern Territory	1	0.7	7.1
Queensland	27	17.6	17.5
South Australia	7	4.6	13.7
Tasmania	1	0.7	6.7
Victoria	26	17.0	13.4
Western Australia	32	20.9	15.5
Missing	1	0.7	6.7

Note: Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Reporting scams

Eighty-one percent of respondents who had received a scam invitation reported it to at least one other person or organisation (n=812, 78.7% of the total sample). There were 222 respondents (21% of the total sample) who did not report the scam to anyone. Friends and family were the most common person(s) respondents reported scam attempts to (n=542, 52.4% of the total sample; see Table 11); however, if they are excluded from the analysis, the reporting rate dropped to 55.6 percent of the sample who had received a scam invitation (n=558, 54.0% of the total sample). Computer support centre scam invitations were the most common scam reported to police.

Of the 153 respondents who reported falling victim to a scam, 136 (88.9%) reported scams to at least one other person or organisations. When friends and family were excluded, the reporting rate dropped to 75.8 percent (n=116) of the victim respondents who had reported to an external agency. Table 12 shows those organisations or persons victimisation was reported to, with respondents permitted to select more than one option.

Respondents were asked if they had reported scams they had received to a formal agency, what their reasons for doing so were. Participants could select more than one reason for reporting scams. The most common reasons for reporting a scam included 'wanting to prevent others from being scammed' (41.7% of sample who received a scam invitation), and 'knew it was the right thing to do' (30.6% of the sample who received a scam invitation; see Table 13). Respondents were given the opportunity to express their own reasons for reporting a scam if the provided responses did not fit their circumstances. Some respondents indicated that it was part of their work responsibilities to report scams. Other reasons for reporting scams ranged from 'to confirm it was a scam' to 'I wanted to try and get my money back'. There were also numerous responses that indicated that respondents were hoping that by reporting the scam invitation it would lead to the scammer ceasing contact. One respondent reported that they decided to report the scam when 'the caller was verbally abusive'.

Reasons for not reporting scam invitations are outlined in Table 14. The most commonly provided reasons included 'unsure of which agency to contact' (41.0% of the sample who had received a scam invitation) and 'didn't think anything would be done' (32.4% of the sample who had received a scam invitation). It is noted that participants may have reported some scams but not others and may have had multiple reasons for not reporting. Respondents were given the option to supply their own reason for not reporting a scam. A reoccurring reason for those who received a scam invitation and did not report it was that respondents 'assumed it was well known', with over 30 respondents indicating similar responses. The survey asked whether respondents had reported scams on behalf of anyone else. Seventy-eight respondents (7.5%) indicated that they had. Participants were allowed to select all options that applied to them (see Table 15).

Table 11 Reporting of scams by agency

Organisation or person reported to	n	Received a scam invitation (%) (n=1,003)	Total sample (%) (n=1,034)
Not reported to anyone	222	22.0	21.0
Family/friends	542	54.0	52.4
Police	102	10.2	9.9
SCAMwatch website (www.SCAMwatch.gov.au)	232	23.1	22.4
Australian Competition and Consumer Commission	86	8.6	8.3
The business represented (eg bank, eBay etc)	228	22.7	22.1
Internet Service Provider	92	9.2	8.9
Legal aid, a lawyer or a community legal services clinic	11	1.1	1.1
Unable to recall	28	2.8	2.7
Other	165	16.5	16.0

Note: Respondents were allowed to select more than one option, therefore percentages may not total 100

Source: ACFT Consumer Fraud Survey 2013 [AIC computer file]

Table 12 Reporting of victimisation by agency

Organisation or person reported to	n	Reported victimisation (%) (n=153)
Not reported to anyone	17	11.0
Family/friends	78	51.0
Police	42	27.5
SCAMwatch website (www.SCAMwatch.gov.au)	63	41.2
Australian Competition and Consumer Commission	26	17.0
The business represented (eg bank, eBay etc)	57	37.4
Internet Service Provider	18	11.8
Legal aid, a lawyer, or a community legal services clinic	6	3.9
Unable to recall	3	2.0
Other	28	18.3

Source: ACFT Consumer Fraud Survey 2013 [AIC computer file]

Table 13 Reasons for reporting scams received

Reason for reporting scam invitation	n	Received a scam invitation (%) (n=1,003)	Total sample (%) (n=1,034)
Desired the apprehension of offender(s)	218	21.7	21.1
Wanted to prevent others from being scammed	418	41.7	40.4
Knew it was the right thing to do	307	30.6	29.7
To assist in the investigation of an offence	299	29.8	28.9
To support your insurance claim	5	0.5	0.5
Other	76	7.6	7.4

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Table 14 Reasons for not reporting scams received

Reason for not reporting	n	Received a scam invitation (%) (n=1,003)	Total sample (%) (n=1,034)
Not worth the effort	278	27.7	26.9
Didn't think it was illegal	42	4.2	4.1
Unsure of which agency to contact	411	41.0	39.7
Feared I would get into trouble	21	2.1	2.0
Didn't think anything would be done	325	32.4	31.4
Receive too many to report	269	26.8	26.0
Other	141	14.1	13.6

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Table 15 Scams reported on behalf of someone else

Scam reported on behalf of	n	Total sample (%) (n=1,034)
Child (son or daughter)	9	0.9
Older relative (brother/sister, parent, grandparent, aunt/uncle)	36	3.5
Younger relative (niece/nephew, brother/sister)	7	0.7
A friend	23	2.2
A colleague	10	1.0
A student (if you are a teacher or in some similar capacity)	1	0.1
Other	17	1.6

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Perceptions of scams

Respondents were asked how they perceived each scam type. They were asked to indicate whether they considered each scam type as *a crime*, *wrong, but not a crime*, or *just something that happens*. Respondents were permitted to select more than one response (see Table 16). Advance fee fraud and phishing were most likely to be considered a crime (by 84.9% and 85.0% of the sample respectively). Respondents were given the opportunity to provide details of some of the other scams they had received; some included fake charities and scams that involved *ransomware* (*ransomware* is a type of malicious software that scammers threaten to activate on recipients' computers unless a fee is paid). Most responses indicated that all scams are a crime; however, some considered them deceptive, but not necessarily a crime or just something that happens.

The perception of scams by respondents who reported victimisation was also explored according to scam type. Again, it is noted that participants could select more than one response (see Table 17). Advance fee fraud was most likely to be considered a crime by victims of this scam, whereas inheritance scams were more likely not to be considered a crime, but rather something that just happens. It should be noted that some respondents chose to not respond to the questions.

Table 16 Perceptions of scams by scam type

Scam type	A crime		Wrong but not a crime		Just something that happens	
	n	%	n	%	n	%
Lottery scams	694	67.1	230	22.2	58	5.6
Advance fee fraud	878	84.9	75	7.3	24	2.3
Inheritance scams	723	69.9	207	20.0	39	3.8
Phishing	879	85.0	80	7.7	20	1.9
Financial advice scams	520	50.3	352	34.0	98	9.5
Boiler-room scams	653	63.2	241	23.3	66	6.4
Work from home scams	742	71.8	167	16.2	61	5.9
Dating scams	564	54.5	329	31.8	63	6.1
Computer support scams	827	80.0	130	12.6	26	2.5
Other	822	50.5	130	12.6	89	8.6

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Table 17 Perceptions of scams by respondents who reported victimisation by scam type

Scam type	A crime		Wrong but not a crime		Just something that happens	
	n	%	n	%	n	%
Lottery scams (n=23)	15	65.2	4	17.4	3	13.0
Advance fee fraud (n=26)	21	80.8	3	11.5	1	3.8
Inheritance scams (n=6)	4	66.7	0	0	2	33.3
Phishing (n=26)	20	76.9	3	11.5	1	3.8
Financial advice scams (n=5)	1	20.0	4	80.0	0	0
Boiler-room scams (5)	1	20.0	2	40.0	1	20.0
Work from home scams (n=8)	5	62.5	3	37.5	0	0
Dating scams (n=31)	24	77.4	6	19.4	1	3.2
Computer support scams (n=40)	37	92.5	2	5.0	0	0
Other (n=38)	23	60.5	6	15.8	2	5.4

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

Specific scams types

A major change to the 2013 survey was the restructure of the survey instrument. Respondents were asked details about the types of scam invitations they may have received so that the responses could be linked to the specific scam types.

As noted previously, 1,003 respondents received at least one scam invitation in the 12 months prior to completing the survey. Of those, 858 received more than one scam invitation, with eight respondents advising they had received all 10 types of scam invitation (including the 'other' category). There were 145 respondents who received only one scam invitation in the 12 months prior to the survey. The most commonly received invitation by those respondents was the computer support centre scam.

There were 338 respondents (32.7% of the total sample) who responded to a scam invitation in some way, either by requesting further information, sending personal details or money or alternatively sending both personal details and money as a result of a scam invitation. Lottery scams or false notification of prizes resulted in the most people seeking further information from scammers, with 208 respondents (20.7% of participants who had received a scam invitation) seeking further information about the scam or sending money and/or personal information as a result of the invitation. Invitations for boiler-room scams were the least likely to elicit a response from survey participants, with only 44 respondents (4.4% of respondents who received a scam invitation) seeking further information or sending money and/or personal information to scammers.

When examining specific scam types in detail, there were some notable differences in the type of victimisation they produced. Computer support centre scams resulted in the highest number of people sending money alone (22.5% of participants who reported being a victim of that particular scam). The 'other' scam type, comprising a range of diverse scam types, also had a larger number of respondents sending money to scammers when compared with the categorised scam types (13 respondents, 1.3% of those who had received an invitation who indicated they had sent money only to an 'other' scam). Phishing scams resulted in the most people sending personal details or passwords, with 22 respondents (2.2% of those who had received a scam invitation) advising they had disclosed their personal details in response to a scam of that nature. Scams that involved financial advice and boiler-room scams were the least likely to result in personal details being sent to scammers.

The scam type that resulted in the most respondents sending both money and personal details or

passwords to a scammer was dating and social networking scams. Twenty respondents from the 234 respondents (8.5% of those who received a dating or romance scam invitation) advised that they had sent both money and personal details in response to a scam invitation of that nature. More details about dating and social networking scams can be found in the next section.

After dating and social networking scams, money transfer scams caused the next highest losses for respondents. There were 18 respondents who reported losing $217,136 to scams of that nature.

The range of financial loss experienced was from $28 to up to $70,000 experienced by one victim of a money transfer scam. It is worth noting that the 'other' scam type (comprising less prevalent scams) had 25 respondents who experienced a combined total loss of $231,675. Examples of some of the scam types involved where respondents advised they had lost money included paying money for invalid or counterfeit tickets, fake psychic hotlines and online gambling programs. The range of the losses experienced by 'other' scam types was from $40 to $54,000. The median amount lost was $2,600.

Relationship consumer fraud: Dating and social networking scams

The theme of the 2014 National Consumer Fraud Week is relationship scams and knowing who you are dealing with online, to help reduce the risk of victimisation from scams. Accordingly, 2013 findings relating to relationship scams are discussed in greater detail in this section. A relationship scam (classified as *dating or social networking scams* in the 2013 ACFT survey) is defined as a scam that may be conducted through legitimate or illegitimate dating or social networking websites and often takes the form of requiring a payment for each email sent and received by a potential match. Alternatively, scammers may deceive victims by posing as a potential partner and then claiming to have an ill relative or severe financial problems and seek financial assistance from the 'love interest' they met on the site, or alternatively they may ask for money for flights to meet up with the victim.

In previous years, it has been found in the ACFT survey that dating scams have resulted in the greatest levels of reported victimisation, even though they were the least prevalent scam type received by participants. These findings were consistent with scam complaints made to the ACCC in 2012 (ACCC 2013). Cross, Smith and Richards (2014) stressed the difficulty in assessing the impact of consumer fraud on victims, as some people may not realise they have been the victims of fraud or may feel embarrassed or upset and not wish to make a formal report. The paper also highlighted instances where victims of romance scams had taken their own lives when discovering the fraud, or where the victims had been robbed and killed by scammers.

Due to the extent of victimisation being reported to the ACCC in 2012, the ACCC issued voluntary best practice guidelines for dating websites to prevent the proliferation of romance scams. Some of the guidelines included displaying warning messages in appropriate locations on the website, implementing a vetting and checking system to identify scam sites or false advertisements on legitimate sites and providing a mechanism whereby uses can easily report scams (ACCC 2012). In 2012, Project Sunbird was launched as a joint operation between the Western Australian Police Major Fraud Squad and the Western Australian Consumer Protection department (WA Scamnet 2013). The project found that since August 2012, Western Australians have sent over $6m to West African countries as a result of relationship frauds (WA Scamnet 2013).

There were 234 participants who had received a relationship scam invitation in the 12 months prior to them completing the 2013 ACFT survey. The most common methods of receiving a dating or romance scam was through email (18.1%) or via the internet (9.5%; see Table 18). Participants reported receiving romance or dating scam invitations from multiple sources and by contrast with other scam types, they were contacted frequently by scammers.

Table 18 Mode of delivery of romance or dating scam invitations										
	Mail	%	Email	%	Phone	%	SMS	%	Internet	%
No contact	1,009	97.6	847	81.9	1,006	97.3	1,011	97.8	936	90.5
1–5 times	13	1.3	59	5.4	11	1.1	11	1.1	46	4.4
6–10 times	4	0.4	34	3.3	3	0.3	2	0.2	14	1.4
11–20 times	4	0.4	31	3.0	5	0.5	4	0.4	12	1.2
21–50 times	1	0.1	22	2.1	5	0.5	3	0.3	10	1.0
More than 50 times	3	0.3	41	4.0	4	0.4	3	0.3	16	1.5
Total	1,034		1,034		1,034		1,034		1,034	

Source: ACFT Consumer Fraud Survey 2013 [AIC data file]

The states and territories where participants reported receiving the most dating or social networking scam invitations (per total respondents) were the Australian Capital Territory (n=29, 33.3%) and South Australia (n=15, 29.4%), followed equally by Queensland and Victoria (24.7%). There were no participants from New Zealand who reported receiving a dating or social networking scam invitation in the 12 months prior to completing the survey.

Of the 234 respondents who had received a dating or romance scam invitation in the 12 months prior to completing the survey, those aged 17 years and under (18.2%) and those aged 65 years and over (15.6%) were the least likely age groups to receive an invitation of that nature. Respondents in the age categories 18–24 years, (33.3%), 25–34 years (30.4%) and 45–54 years (27.0%) received the highest amount of dating scam invitations. There was one participant who failed to disclose their age.

Victimisation through romance, dating scams or social networking scams

A *victim* for the purposes of the survey was defined as someone who had sent money or personal details or both money and personal details to a scammer as a result of a scam invitation.

Thirty-one participants (3% of the total sample; 13% of respondents who had received a romance or dating scam) reported in the survey that they had been the victim of a dating, romance or social networking scam in the 12 months prior to completing the survey. An additional 18 participants stated they had requested further information in response to a dating or romance scam invitation, but had not become a victim of the scam.

Losses

Seven participants sent personal details only and four participants sent money only to a scammer in response to a dating, romance or social networking scam. Another 20 participants sent both money and personal details. Of the 24 participants who sent money and personal details, 18 specified a loss amount. The money sent by respondents ranged from a minimum amount of $5 to a maximum of $128,000. The total amount sent as a result of a dating or social networking scam was $536,779.76 with the median amount being $9,500.

Victim demographics

The highest percentage of people who were the victims of dating or social networking scams resided in the Australian Capital Territory (n=5, 6% of those participants who had received a scam invitation of that nature). Twenty-nine percent of victims were aged between 45 and 54 years, 26 percent of victims were aged 55–64 years. There were no victims aged 17 years and under.

Respondents aged between 45–54 years sent the highest amount of money in response to dating or romance scams. Four respondents in that age category sent a total of $276,800. Although, respondents aged between 55–64 years sent money more frequently, six respondents in that age category sent a total of $27,777. There were no respondents aged 17 years and under who sent money in response to a dating, romance or social networking scam invitation.

Of the participants who identified themselves as victims of a dating or social networking scam nine (29% of victims) were male and 22 (71% of victims of that scam type) were female. The majority of victims (10 respondents) said their yearly income was between $20,000 and $40,000, with four respondents saying their yearly income was over $80,000 and another seven who specified they would rather not disclose those details.

Responding to victimisation

Participants were asked if they had reported the scam to anyone. Options they could choose from were family and friends, police, SCAMwatch, the ACCC or another regulatory agency, the business represented in the scam, an Internet Service Provider or a lawyer or Legal Aid representative. Twenty-six (84%) victims of a dating, romance or social networking scams advised in the survey that they had reported the scam to someone from the options list. Five victims of a dating or social networking scam advised they did not report or tell anyone about the scam. When family and/or friends were removed as a reporting option, the number of victims who reported the scam dropped to 18 (58%).

Conclusion and policy implications

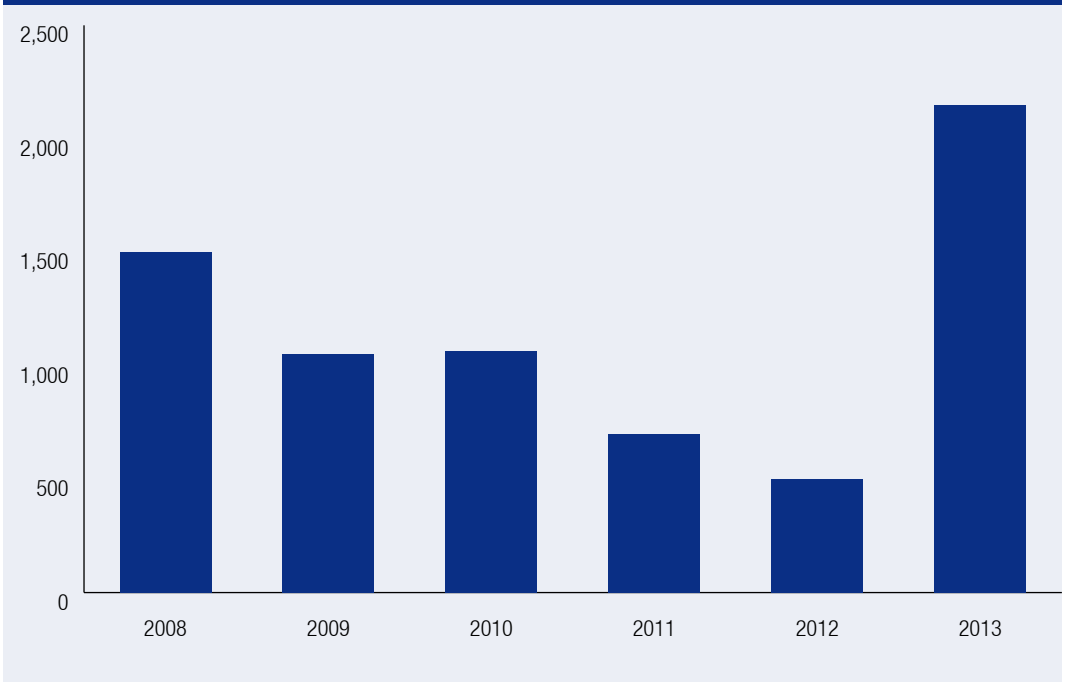
Findings and discussion

As in previous years, scams were received by a large proportion of the survey respondents, with 97 percent of participants receiving a scam invitation in the 12 months prior to the survey. The most commonly received scam invitations were lottery scams, computer support centre scams and phishing scams. Despite some changes to the 2013 survey methodology, the most common scam invitation types were consistent with findings from previous surveys.

Thirty-four percent of respondents disclosed that they had responded to a scam invitation in the 12 months prior to the survey. Responding could involve sending money or personal details or seeking further information. Six percent stated that they sent personal information as a result of a scam invitation and four percent sent money, with seven percent of the sample disclosing they had sent personal details and experienced a financial loss. The proportion of respondents experiencing both a financial loss *and* sending personal details has increased since the 2012 survey findings (Jorna & Hutchings 2013).

Of those scams reported to the ACCC in 2012, more people advised that they had received an unsolicited telephone call as the scam delivery method (ACCC 2013) than in previous years. While email remained the most common method by which scams were reported to be delivered in the ACFT survey, the 2013 findings continue to show high levels of scams delivered by telephone and SMS.

Figure 4 Median reported financial loss by year ($)



Source: ACFT Consumer Fraud Surveys 2013, 2012, 2011, 2010, 2009, 2008 [AIC data files]

As shown in Figure 4, the median financial loss reported each year had been steadily declining since 2010; however, the median financial loss of $2,150 reported in 2013 is the highest reported figure in the AIC's annual consumer fraud survey thus far and is three times higher than the median loss amount from the amount reported in 2012 survey.

It has previously been noted that the rate of reporting of scams to law enforcement and regulatory agencies is generally quite low (Hutchings & Lindley 2012). This continued to be evident in the 2013 findings, with only 27 percent of victims reporting the scam to police and 17 percent reporting the scam to the ACCC. It was concerning to note that the most common reason for not reporting a scam invitation was that respondents were unsure of which agency to contact regarding the scam. This could indicate that further publicity about the role of SCAMwatch is necessary. There are important reasons for people to report scam attempts or victimisation. For example, a low reporting rate affects resources that may be allocated to combat scams. Non-reporting of scams can also impact the overall knowledge and understanding that agencies hold when developing awareness and education campaigns around scam victimisation.

It has been demonstrated consistently by this survey's results over the years that it is not the most commonly received scams, such as lottery scams, that cause the most frequent victimisation—it is scams that are new to the public, such as the computer support centre scams or those that have changed or adapted from previous years, such as dating or social networking scams. While reporting rates remain low, when respondents did report a scam invitation, the most frequent reasons for doing so were to prevent others from becoming a victim of the scam and because they knew it was the right thing to do. Those reasons may demonstrate an understanding that education is a key requirement to lessen the impact of scams.

Included in the 2013 survey was the new scam category of 'boiler-room scams'. A boiler-room scam was defined as a 'request to buy, sell or retain securities or other investments (including superannuation investments) that are usually offered through cold-calling by scammers who seek to sell worthless shares or investments to recipients'. This category was included in the 2013 survey after the release of the joint Australian Crime Commission and AIC publication *Serious and Organised Investment*

Fraud in Australia. It was believed that the existing category of 'investment scam' might not be capturing the types of fraud outlined in the publication. In the 2013 survey findings, 'boiler-room scams' were the scam invitation category that was received the least by participants, with only 115 participants receiving a scam invitation of that nature. Of the 115 participants who had received an invitation of that nature, five participants identified as victims of a boiler room scam and three victims advised they had lost a total of $23,750.

Dating and social networking consumer frauds

Consistent with previous ACFT survey findings (Hutchings & Lindley 2012; Jorna & Hutchings 2013), dating scams resulted in the highest amount of money sent of all scam types. Victims of dating scams reported losses exceeding $520,000. This finding remains consistent with scam complaints made to the ACCC (2013) and findings from other Australian investigations. For example, Project Sunbird found that since August 2012, Western Australians sent over $6m to West African countries as a result of relationship frauds (WA Scamnet 2013).

When responding to dating or social networking scams, participants reported sending a combination of money and personal details at higher rates than money or personal details alone. Dating and social networking scams also had the most successful conversion rate, with 13.2 percent of scam invitations of that nature resulting in victimisation. Respondents who identified themselves as victims of a dating or social networking scam and were aged 45 to 54 years old sent the highest amount of money to scammers in response to an invitation of that nature. Although it was respondents aged 55–64 years who sent money the most frequently (33% of those who had sent money as a result of a dating scam).

Suggestions for future campaigns

Suggested themes for future education and awareness campaigns include a focus on:

- Developing a greater understanding of the consequences of scams; not just the financial impact, but the psychological and social aspects associated with victimisation, and the lasting effects that falling victim to a scam may have. Research about victims of scams has found that it is not just the individual victims who are affected by scams, but rather their entire family may be impacted as a result of the scam (see Button, Lewis & Tapley 2014).
- Changing public perceptions of victims of consumer fraud. Survey findings indicate that respondents may hold negative views about people who fall victim to scams. These beliefs may be heightened by media portrayals. Future campaigns could seek to educate the public about the harms of scams beyond the financial impact by highlighting the sophistication of some scams and the damage they cause, including the emotional impacts on victims and their families. Two respondents in the survey advised that they felt shame due to their victimisation and had not wanted to report the scam due to those feelings. Public perceptions and the way consumer fraud incidents are referred to as 'scams' may trivialise their significance; however, this is a theory that needs to be explored further.
- Educating the public on what to do if they have been the victim of consumer fraud or if they are receiving a large amount of scam invitations. The survey has continually found that respondents are unaware of where they should report scams and if scams are even illegal. A campaign that seeks to clarify who to report scams to and to give greater understanding of what outcomes those reporting scams may expect would be beneficial for those respondents who received a lot of scam invitations and for those who fell victim to a scam.

References

URLs correct as at September 2014

Australian Bureau of Statistics (ABS) 2012. *Personal fraud 2010–11*. cat. no. 4528.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0

Australian Competition & Consumer Commission (ACCC) 2013. *Targeting scams: Report of the ACCC on scam activity 2012*. Canberra: ACCC. http://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2012

Australian Competition & Consumer Commission (ACCC) 2012. *Best practice guidelines for dating websites*. Canberra: ACCC. http://www.accc.gov.au/publications/best-practice-guidelines-for-dating-websites

Australian Competition & Consumer Commission (ACCC) 2011. *The little black book of scams: Your guide to scams, swindles, rorts and rip-offs*. Canberra: ACCC

Australian Crime Commission (ACC) & Australian Institute of Criminology (AIC) 2012. *Serious and organised investment fraud in Australia*. Canberra: ACC. https://www.crimecommission.gov.au/sites/default/files/SOIFA_Report_030812.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 series* no. 43. Canberra: AIC. http://www.aic.gov.au/publications/current%20series/tbp/41-60/tbp043.aspx

Button M, Lewis C & Tapley J 2014. Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal* 27: 36–54. http://www.palgrave-journals.com/sj/journal/v27/n1/pdf/sj201211a.pdf

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. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/461-480/tandi474.html

Hutchings A & Lindley J 2012. Australasian Consumer Fraud Taskforce: Results of the 2010 and 2011 online consumer fraud surveys. *Technical and background paper series* no. 50. Canberra: AIC. http://aic.gov.au/publications/current%20series/tbp/41-60/tbp050.html

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

SCAMwatch 2013. *National consumer fraud week 2013*. http://www.scamwatch.gov.au/content/index.phtml/itemId/1042580

Smith RG 2007. Consumer scams in Australia: An overview. *Trends & Issues in Crime and Criminal Justice* no. 331. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/321-340/tandi331.html

Smith RG & Akman T 2008. Raising public awareness of consumer fraud in Australia. *Trends & Issues in Crime and Criminal Justice* no. 349. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/341-360/tandi349.html

WA ScamNet 2014. *Project Sunbird*. Government of Western Australia Department of Commerce Consumer Protection. http://www.scamnet.wa.gov.au/scamnet/Fight_Back-Project_Sunbird.htm

Appendices

Appendix 1: 2013 consumer fraud survey

Australasian Consumer Fraud Taskforce 2013

The following questions ask about various scam invitations that you might have received during the last 12 months and how you received them. Nine types of scams are included in addition to a general category of 'other scams'. The scams are:

1. Lottery scams – Dishonest notifications from someone the recipient doesn't personally know in relation to having won a lottery or some other prize or competition.

2. Money transfer scams – Requests for assistance to transfer large sums of money out of another country (such as Nigeria) to the recipient›s bank account in return for a percentage of the amount transferred. Advance fee payments are sought before the large sums are sent and the scammer then defaults on the agreement sending no money at all.

3. Inheritance scams – Invitations usually sent by scammers posing as a lawyer or bank employee purporting to act on behalf of a deceased estate falsely claiming that a distant relative has died and has left the recipient a large inheritance which can be recovered in return for a payment.

4. Phishing scams – Requests by businesses to confirm the recipient's personal details or passwords or to supply other personal information – these types of scams seek to trick people into providing their personal details and banking information and sometimes make use of malicious software downloaded to computers.

5. Financial advice scams – Financial advice scams consist of illegitimate advice offering high financial returns on investments that invariably lead to overall loss of money by the recipient.

6. Boiler-room scams – Requests to buy, sell or retain securities or other investments (including superannuation investments) that are usually offered through cold-calling by scammers who seek to sell worthless shares or investments to recipients.

7. Work from home scams – Work from home scams are often promoted through spam emails or advertisements on noticeboards in which attractive job offers are made but which do not relate to legitimate employment and often involve illegal money laundering.

8. Computer support centre scams – Computer support centre scams occur when recipients receive mainly telephone calls from scammers claiming they are from well known computer manufacturers or businesses that can fix problems with the recipients' computers. Scammers may ask for money, personal details or passwords or seek to sell worthless products to fix computers.

9. Dating and social networking scams – These may use illegitimate or legitimate dating or social networking websites and may require payment for each email sent and received by a potential match. Alternatively, scammers may initiate relationships in order to trick people into paying money for dishonest reasons.

10. Other scams – A variety of other dishonest invitations from someone the recipient don't personally know involving a type of scam not referred to above.

1. Lottery scams

Over the last 12 months, have you been dishonestly contacted in any way (including by phone, SMS, email, letter, or on the internet and/or in person) by someone you don't personally know in relation to winning a lottery or some other prize?

☐ Yes
☐ No

How were you contacted in relation to receiving a scam relating to winning a lottery or some other prize, and how many times were you contacted? (Select all that apply).

	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail	☐	☐	☐	☐	☐
Email	☐	☐	☐	☐	☐
Telephone (including landline and mobile phones)	☐	☐	☐	☐	☐
SMS	☐	☐	☐	☐	☐
Internet site/social networking site	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

If 'other' please provide details for the most frequent type of other contact:

Over the last 12 months, have you responded in any way to a notification of having won a lottery or some other prize?

Responding includes contacting the person(s) in any way to request further information, providing your personal details, or sending money etc.

Do not include contact you have had with the person(s) if you were attempting to cease communication or engage in 'scam baiting' (pretending to respond to a scam invitation to annoy the scammer without any intention of providing money etc.).

- ☐ No
- ☐ Yes, I requested further information only
- ☐ Yes, I sent personal details or passwords
- ☐ Yes I sent money
- ☐ Yes I sent personal details and money

If you sent money as a result of a notification of winning a lottery or some other prize, what is your best estimate of the total amount of money you have sent in the last 12 months?

Note: This refers to the money you have paid out as a result of a request. This does NOT include money that you would have received if the offer had been legitimate.

Please indicate the amount in whole dollars. E.g. $1000.00 should be entered as $1000
Please indicate the amount sent before any intervention or repayment from insurance, your bank or legal action

- ☐ Don't know/ I can't recall
- ☐ I'd rather not say
- ☐ The amount in the box below

Please indicate the amount in whole dollars, do not include dollar signs ($):

If you responded to the scam by sending money or personal details or passwords, how many times were you in contact with the person(s) before you sent the money or personal information?

- ☐ Once only
- ☐ Two to five times
- ☐ Six to 10 times
- ☐ 11 to 20 times
- ☐ More than 20 times
- ☐ I can't recall

How many times over the last 12 months have you responded to this type of scam?

Note: Responding can include requesting further information, providing personal details, sending money etc.

- ☐ Once
- ☐ Twice
- ☐ Three times
- ☐ Four times
- ☐ Five or more times

Have you reported this scam to anyone? (Select all that apply)

- ☐ Not reported to anyone
- ☐ Family/ friends
- ☐ Police
- ☐ SCAMwatch website (www.scamwatch.gov.au)
- ☐ Australian Competition and Consumer Commission/ Fair Trading or Consumer Protection agencies
- ☐ The business represented (eg. bank, eBay etc)
- ☐ Internet Service Provider
- ☐ Legal aid, a lawyer, or a community legal services clinic
- ☐ Unable to recall
- ☐ Other

2. Money transfer scams

Over the last 12 months, have you been dishonestly contacted in any way (including by phone, SMS, email, letter, or on the internet and/or in person) by someone you don't personally know in relation to a request for assistance to transfer money out of another country (such as Nigeria)?

- ☐ Yes
- ☐ No

How were you contacted in relation to receiving a scam invitation relating to a request for assistance to transfer money out of another country, and how many times were you contacted? (Select all that apply).

	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail	☐	☐	☐	☐	☐
Email	☐	☐	☐	☐	☐
Telephone (including landlines and mobile phones)	☐	☐	☐	☐	☐
SMS	☐	☐	☐	☐	☐
Internet site/social networking site	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

If 'other' please provide details for the most frequent type of other contact:

Over the last 12 months, have you responded in any way to a request for assistance to transfer money out of another country?

Responding includes contacting the person(s) in any way to request further information, providing your personal details, or sending money etc.

Do not include contact you have had with the person(s) if you were attempting to cease communication or engage in 'scam baiting' (pretending to respond to a scam invitation to annoy the scammer without any intention of providing money etc.).

- ☐ No
- ☐ Yes, I requested further information only
- ☐ Yes, I sent personal details or passwords
- ☐ Yes I sent money
- ☐ Yes I sent personal details and money

If you sent money as a result of a notice of a request to transfer money out of another country, what is your best estimate of the total amount of money you have sent in the last 12 months?

Note: This refers to the money you have paid out as a result of a request. This does NOT include money that you would have received if the offer had been legitimate.

Please indicate the amount in whole dollars. E.g. $1000.00 should be entered as $1000

Please indicate the amount sent before any intervention or repayment from insurance, your bank or legal action

- [ ] Don't know/ I can't recall
- [ ] I'd rather not say
- [ ] The amount in the box below

Please indicate the amount in whole dollars, do not include dollar signs ($):

If you responded to a request for assistance to transfer money out of another country scam by sending money or personal details or passwords, how many times were you in contact with the person(s) before you sent the money or personal information?

- [ ] Once only
- [ ] Two to five times
- [ ] Six to 10 times
- [ ] 11 to 20 times
- [ ] More than 20 times
- [ ] I can't recall

How many times over the last 12 months have you responded to this type of scam?

Note: Responding can include requesting further information, providing personal details, sending money etc.

- [ ] Once
- [ ] Twice
- [ ] Three times
- [ ] Four times
- [ ] Five or more times

Have you reported this scam to anyone? (Select all that apply)

- [ ] Not reported to anyone
- [ ] Family/ friends
- [ ] Police

- [ ] SCAMwatch website (www.scamwatch.gov.au)
- [ ] Australian Competition and Consumer Commission/ Fair Trading or Consumer Protection agencies
- [ ] The business represented (eg. bank, eBay etc)
- [ ] Internet Service Provider
- [ ] Legal aid, a lawyer, or a community legal services clinic
- [ ] Unable to recall
- [ ] Other

If you reported to 'other', please specify:

3. Inheritance scams

Over the last 12 months, have you been dishonestly contacted in any way (including by phone, SMS, email, letter, or on the internet and/or in person) by someone you don't personally know in relation to a notification of an inheritance?

- [ ] Yes
- [ ] No

How were you contacted in relation to receiving a scam relating to a notification of an inheritance, and how many times were you contacted? (Select all that apply).

	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail	☐	☐	☐	☐	☐
Email	☐	☐	☐	☐	☐
Telephone (including landlines and mobile phones)	☐	☐	☐	☐	☐
SMS	☐	☐	☐	☐	☐
Internet site/social networking site	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

If 'other' please provide details for the most frequent type of other contact:

Over the last 12 months, have you responded in any way to a notification of an inheritance?

Responding includes contacting the person(s) in any way to request further information, providing your personal details, or sending money etc.

Do not include contact you have had with the person(s) if you were attempting to cease communication or engage in 'scam baiting' (pretending to respond to a scam invitation to annoy the scammer without any intention of providing money etc.).

- ☐ No
- ☐ Yes, I requested further information only
- ☐ Yes, I sent personal details or passwords
- ☐ Yes I sent money
- ☐ Yes I sent personal details and money

If you sent money as a result of an inheritance scam, what is your best estimate of the total amount of money you have sent in the last 12 months?

Note: This refers to the money you have paid out as a result of a request. This does NOT include money that you would have received if the offer had been legitimate.

Please indicate the amount in whole dollars. E.g. $1000.00 should be entered as $1000

Please indicate the amount sent before any intervention or repayment from insurance, your bank or legal action

- ☐ Don't know/ I can't recall
- ☐ I'd rather not say
- ☐ The amount in the box below

Please indicate the amount in whole dollars, do not include dollar signs ($):

If you responded to the inheritance scam by sending money or personal details or passwords, how many times were you in contact with the person(s) before you sent the money or personal information?

- ☐ Once only
- ☐ Two to five times

- [ ] Six to 10 times
- [ ] 11 to 20 times
- [ ] More than 20 times
- [ ] I can't recall

Have you reported this scam to anyone? (Select all that apply)

- [ ] Not reported to anyone
- [ ] Family/ friends
- [ ] Police
- [ ] SCAMwatch website (www.scamwatch.gov.au)
- [ ] Australian Competition and Consumer Commission/ Fair Trading or Consumer Protection agencies
- [ ] The business represented (eg. bank, eBay etc)
- [ ] Internet Service Provider
- [ ] Legal aid, a lawyer, or a community legal services clinic
- [ ] Unable to recall
- [ ] Other

If you reported to 'other', please specify:

4. Phishing scams

Over the last 12 months, have you been dishonestly contacted in any way (including by phone, SMS, email, letter, or on the internet and/or in person) by someone you don't personally know in relation to a request by a business to confirm your personal details or passwords (phishing scams)?

- [ ] Yes
- [ ] No

How were you contacted in relation to receiving a scam relating to a request by a business to confirm your personal details or passwords (a phishing scam), and how many times were you contacted? (Select all that apply).

	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail	☐	☐	☐	☐	☐
Email	☐	☐	☐	☐	☐
Telephone (including landlines and mobile phones)	☐	☐	☐	☐	☐
SMS	☐	☐	☐	☐	☐
Internet site/social networking site	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

If 'other' please provide details for the most frequent type of other contact:

Over the last 12 months, have you responded in any way to a phishing scam?

Responding includes contacting the person(s) in any way to request further information, providing your personal details, or sending money etc.

Do not include contact you have had with the person(s) if you were attempting to cease communication or engage in 'scam baiting' (pretending to respond to a scam invitation to annoy the scammer without any intention of providing money etc.).

- ☐ No
- ☐ Yes, I requested further information only
- ☐ Yes, I sent personal details or passwords
- ☐ Yes I sent money
- ☐ Yes I sent personal details and money

If you sent money as a result of a phishing scam, what is your best estimate of the total amount of money you have sent in the last 12 months?

Note: This refers to the money you have paid out as a result of a request. This does NOT include money that you would have received if the offer had been legitimate.

Please indicate the amount in whole dollars. E.g. $1000.00 should be entered as $1000

Please indicate the amount sent before any intervention or repayment from insurance, your bank or legal action

- [ ] Don't know/ I can't recall
- [ ] I'd rather not say
- [ ] The amount in the box below

Please indicate the amount in whole dollars, do not include dollar signs ($):

If you responded to the phishing scam by sending money or personal details or passwords, how many times were you in contact with the person(s) before you sent the money or personal information?

- [ ] Once only
- [ ] Two to five times
- [ ] Six to 10 times
- [ ] 11 to 20 times
- [ ] More than 20 times
- [ ] I can't recall

Have you reported this scam to anyone? (Select all that apply)

- [ ] Not reported to anyone
- [ ] Family/ friends
- [ ] Police
- [ ] SCAMwatch website (www.scamwatch.gov.au)
- [ ] Australian Competition and Consumer Commission/ Fair Trading or Consumer Protection agencies
- [ ] The business represented (eg. bank, eBay etc)
- [ ] Internet Service Provider
- [ ] Legal aid, a lawyer, or a community legal services clinic
- [ ] Unable to recall
- [ ] Other

If you reported to 'other', please specify:

5. Financial advice scams

Over the last 12 months, have you been dishonestly contacted in any way (including by phone, SMS, email, letter, or on the internet and/or in person) by someone you don't personally know in relation to a request to supply you with financial advice?

- ☐ Yes
- ☐ No

How were you contacted in relation to receiving a scam relating to a request to supply you with financial advice, and how many times were you contacted? (Select all that apply).

	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail	☐	☐	☐	☐	☐
Email	☐	☐	☐	☐	☐
Telephone (including landlines and mobile phones)	☐	☐	☐	☐	☐
SMS	☐	☐	☐	☐	☐
Internet site/social networking site	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

If 'other' please provide details for the most frequent type of other contact:

Over the last 12 months, have you responded in any way to a notification of an inheritance?

Responding includes contacting the person(s) in any way to request further information, providing your personal details, or sending money etc.

Do not include contact you have had with the person(s) if you were attempting to cease communication or engage in 'scam baiting' (pretending to respond to a scam invitation to annoy the scammer without any intention of providing money etc.).

- ☐ No
- ☐ Yes, I requested further information only

- [ ] Yes, I sent personal details or passwords
- [ ] Yes I sent money
- [ ] Yes I sent personal details and money

If you sent money as a result of a financial advice scam, what is your best estimate of the total amount of money you have sent in the last 12 months?

Note: This refers to the money you have paid out as a result of a request. This does NOT include money that you would have received if the offer had been legitimate.

Please indicate the amount in whole dollars. E.g. $1000.00 should be entered as $1000

Please indicate the amount sent before any intervention or repayment from insurance, your bank or legal action

- [ ] Don't know/ I can't recall
- [ ] I'd rather not say
- [ ] The amount in the box below

Please indicate the amount in whole dollars, do not include dollar signs ($):

If you responded to the financial advice scam by sending money or personal details or passwords, how many times were you in contact with the person(s) before you sent the money or personal information?

- [ ] Once only
- [ ] Two to five times
- [ ] Six to 10 times
- [ ] 11 to 20 times
- [ ] More than 20 times
- [ ] I can't recall

Have you reported this scam to anyone? (Select all that apply)

- [ ] Not reported to anyone
- [ ] Family/ friends
- [ ] Police

SCAMwatch website (www.scamwatch.gov.au)
Australian Competition and Consumer Commission/ Fair Trading or Consumer Protection agencies
The business represented (eg. bank, eBay etc)
Internet Service Provider
Legal aid, a lawyer, or a community legal services clinic
Unable to recall
Other

If you reported to 'other', please specify:

6. Boiler-room scams

Over the last 12 months, have you been dishonestly contacted in any way (including by phone, SMS, email, letter, or on the internet and/or in person) by someone you don't personally know in relation to a request to buy, sell or retain securities or other investments (including superannuation investments)?

Yes
No

How were you contacted in relation to receiving a boiler-room scam, and how many times were you contacted? (select all that apply).

	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail					
Email					
Telephone (including landlines and mobile phones)					
SMS					
Internet site/social networking site					
Other					

If 'other' please provide details for the most frequent type of other contact:

Over the last 12 months, have you responded in any way to a boiler-room scam?

Responding includes contacting the person(s) in any way to request further information, providing your personal details, or sending money etc.

Do not include contact you have had with the person(s) if you were attempting to cease communication or engage in 'scam baiting' (pretending to respond to a scam invitation to annoy the scammer without any intention of providing money etc.).

- ☐ No
- ☐ Yes, I requested further information only
- ☐ Yes, I sent personal details or passwords
- ☐ Yes I sent money
- ☐ Yes I sent personal details and money

If you sent money as a result of a boiler-room scam, what is your best estimate of the total amount of money you have sent in the last 12 months?

Note: This refers to the money you have paid out as a result of a request. This does NOT include money that you would have received if the offer had been legitimate.

Please indicate the amount in whole dollars. E.g. $1000.00 should be entered as $1000

Please indicate the amount sent before any intervention or repayment from insurance, your bank or legal action

- ☐ Don't know/ I can't recall
- ☐ I'd rather not say
- ☐ The amount in the box below

Please indicate the amount in whole dollars, do not include dollar signs ($):

If you responded to the boiler-room scam by sending money or personal details or passwords, how many times were you in contact with the person(s) before you sent the money or personal information?

- ☐ Once only
- ☐ Two to five times

- [ ] Six to 10 times
- [ ] 11 to 20 times
- [ ] More than 20 times
- [ ] I can't recall

Have you reported this scam to anyone? (Select all that apply)

- [ ] Not reported to anyone
- [ ] Family/ friends
- [ ] Police
- [ ] SCAMwatch website (www.scamwatch.gov.au)
- [ ] Australian Competition and Consumer Commission/ Fair Trading or Consumer Protection agencies
- [ ] The business represented (eg. bank, eBay etc)
- [ ] Internet Service Provider
- [ ] Legal aid, a lawyer, or a community legal services clinic
- [ ] Unable to recall
- [ ] Other

If you reported to 'other', please specify:

7. Work from home scams

Over the last 12 months, have you been dishonestly contacted in any way (including by phone, SMS, email, letter, or on the internet and/or in person) by someone you don't personally know in relation to an opportunity to work from home (a front for money laundering)?

- [ ] Yes
- [ ] No

How were you contacted in relation to receiving a work from home scam, and how many times were you contacted? (Select all that apply).

	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail	☐	☐	☐	☐	☐
Email	☐	☐	☐	☐	☐
Telephone (including landlines and mobile phones)	☐	☐	☐	☐	☐
SMS	☐	☐	☐	☐	☐
Internet site/social networking site	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

If 'other' please provide details for the most frequent type of other contact:

Over the last 12 months, have you responded in any way to a work from home scam?

Responding includes contacting the person(s) in any way to request further information, providing your personal details, or sending money etc.

Do not include contact you have had with the person(s) if you were attempting to cease communication or engage in 'scam baiting' (pretending to respond to a scam invitation to annoy the scammer without any intention of providing money etc.).

- ☐ No
- ☐ Yes, I requested further information only
- ☐ Yes, I sent personal details or passwords
- ☐ Yes I sent money
- ☐ Yes I sent personal details and money

If you sent money as a result of a work from home scam, what is your best estimate of the total amount of money you have sent in the last 12 months?

Note: This refers to the money you have paid out as a result of a request. This does NOT include money that you would have received if the offer had been legitimate.

Please indicate the amount in whole dollars. E.g. $1000.00 should be entered as $1000

Please indicate the amount sent before any intervention or repayment from insurance, your bank or legal action

- [ ] Don't know/ I can't recall
- [ ] I'd rather not say
- [ ] The amount in the box below

Please indicate the amount in whole dollars, do not include dollar signs ($):

If you responded to the work from home scam by sending money or personal details or passwords, how many times were you in contact with the person(s) before you sent the money or personal information?

- [ ] Once only
- [ ] Two to five times
- [ ] Six to 10 times
- [ ] 11 to 20 times
- [ ] More than 20 times
- [ ] I can't recall

Have you reported this scam to anyone? (Select all that apply)

- [ ] Not reported to anyone
- [ ] Family/ friends
- [ ] Police
- [ ] SCAMwatch website (www.scamwatch.gov.au)
- [ ] Australian Competition and Consumer Commission/ Fair Trading or Consumer Protection agencies
- [ ] The business represented (eg. bank, eBay etc)
- [ ] Internet Service Provider
- [ ] Legal aid, a lawyer, or a community legal services clinic
- [ ] Unable to recall
- [ ] Other

If you reported to 'other', please specify:

8. Computer support centre scam

Over the last 12 months, have you been dishonestly contacted in any way (including by phone, SMS, email, letter, or on the internet and/or in person) by someone you don't personally know in relation to a person representing themselves as someone from a computer support centre?

- ☐ Yes
- ☐ No

How were you contacted in relation to receiving a computer support centre scam, and how many times were you contacted? (Select all that apply).

	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail	☐	☐	☐	☐	☐
Email	☐	☐	☐	☐	☐
Telephone (including landlines and mobile phones)	☐	☐	☐	☐	☐
SMS	☐	☐	☐	☐	☐
Internet site/social networking site	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

If 'other' please provide details for the most frequent type of other contact:

Over the last 12 months, have you responded in any way to a computer support centre scam?

Responding includes contacting the person(s) in any way to request further information, providing your personal details, or sending money etc.

Do not include contact you have had with the person(s) if you were attempting to cease communication or engage in 'scam baiting' (pretending to respond to a scam invitation to annoy the scammer without any intention of providing money etc.).

- ☐ No
- ☐ Yes, I requested further information only

- [ ] Yes, I sent personal details or passwords
- [ ] Yes I sent money
- [ ] Yes I sent personal details and money

If you sent money as result from a computer support centre scam, what is your best estimate of the total amount of money you have sent in the last 12 months?

Note: This refers to the money you have paid out as a result of a request. This does NOT include money that you would have received if the offer had been legitimate.

Please indicate the amount in whole dollars. E.g. $1000.00 should be entered as $1000

Please indicate the amount sent before any intervention or repayment from insurance, your bank or legal action

- [ ] Don't know/ I can't recall
- [ ] I'd rather not say
- [ ] The amount in the box below

Please indicate the amount in whole dollars, do not include dollar signs ($):

If you responded to the computer support centre scam by sending money or personal details or passwords, how many times were you in contact with the person(s) before you sent the money or personal information?

- [ ] Once only
- [ ] Two to five times
- [ ] Six to 10 times
- [ ] 11 to 20 times
- [ ] More than 20 times
- [ ] I can't recall

Have you reported this scam to anyone? (Select all that apply)

- [ ] Not reported to anyone
- [ ] Family/ friends
- [ ] Police

- [ ] SCAMwatch website (www.scamwatch.gov.au)
- [ ] Australian Competition and Consumer Commission/ Fair Trading or Consumer Protection agencies
- [ ] The business represented (eg. bank, eBay etc)
- [ ] Internet Service Provider
- [ ] Legal aid, a lawyer, or a community legal services clinic
- [ ] Unable to recall
- [ ] Other

If you reported to 'other', please specify:

9. Dating and social networking scams

Over the last 12 months, have you been dishonestly contacted in any way (including by phone, SMS, email, letter, or on the internet and/or in person) by someone you don't personally know in relation to pursuing a personal relationship that turned out to be false?

- [ ] Yes
- [ ] No

How were you contacted in relation to receiving a dating or social networking scam, and how many times were you contacted? (Select all that apply).

	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail	☐	☐	☐	☐	☐
Email	☐	☐	☐	☐	☐
Telephone (including landlines and mobile phones)	☐	☐	☐	☐	☐
SMS	☐	☐	☐	☐	☐
Internet site/social networking site	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

If 'other' please provide details for the most frequent type of other contact:

Over the last 12 months, have you responded in any way to a dating or social networking scam?

Responding includes contacting the person(s) in any way to request further information, providing your personal details, or sending money etc.

Do not include contact you have had with the person(s) if you were attempting to cease communication or engage in 'scam baiting' (pretending to respond to a scam invitation to annoy the scammer without any intention of providing money etc.).

- ☐ No
- ☐ Yes, I requested further information only
- ☐ Yes, I sent personal details or passwords
- ☐ Yes I sent money
- ☐ Yes I sent personal details and money

If you sent money as result from a dating or social networking scam, what is your best estimate of the total amount of money you have sent in the last 12 months?

Note: This refers to the money you have paid out as a result of a request. This does NOT include money that you would have received if the offer had been legitimate.

Please indicate the amount in whole dollars. E.g. $1000.00 should be entered as $1000

Please indicate the amount sent before any intervention or repayment from insurance, your bank or legal action

- ☐ Don't know/ I can't recall
- ☐ I'd rather not say
- ☐ The amount in the box below

Please indicate the amount in whole dollars, do not include dollar signs ($):

If you responded to the dating or social networking scam by sending money or personal details or passwords, how many times were you in contact with the person(s) before you sent the money or personal information?

- ☐ Once only
- ☐ Two to five times

- [ ] Six to 10 times
- [ ] 11 to 20 times
- [ ] More than 20 times
- [ ] I can't recall

Have you reported this scam to anyone? (Select all that apply)

- [ ] Not reported to anyone
- [ ] Family/ friends
- [ ] Police
- [ ] SCAMwatch website (www.scamwatch.gov.au)
- [ ] Australian Competition and Consumer Commission/ Fair Trading or Consumer Protection agencies
- [ ] The business represented (eg. bank, eBay etc)
- [ ] Internet Service Provider
- [ ] Legal aid, a lawyer, or a community legal services clinic
- [ ] Unable to recall
- [ ] Other

If you reported to 'other', please specify:

10. Other scams

Over the last 12 months, have you been dishonestly contacted in any way (including by phone, SMS, email, letter, or on the internet and/or in person) by someone you don't personally know in relation to some other scam type?

- [ ] Yes
- [ ] No

Please give details of the type of scam you were most often contacted about:

How were you contacted in relation to receiving a scam relating to some other scam type, and how many times were you contacted? (Select all that apply).

	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail	☐	☐	☐	☐	☐
Email	☐	☐	☐	☐	☐
Telephone (including landlines and mobile phones)	☐	☐	☐	☐	☐
SMS	☐	☐	☐	☐	☐
Internet site/social networking site	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

If 'other' please provide details for the most frequent type of other contact:

Over the last 12 months, have you responded in any way to some other scam?

Responding includes contacting the person(s) in any way to request further information, providing your personal details, or sending money etc.

Do not include contact you have had with the person(s) if you were attempting to cease communication or engage in 'scam baiting' (pretending to respond to a scam invitation to annoy the scammer without any intention of providing money etc.).

☐ No
☐ Yes, I requested further information only
☐ Yes, I sent personal details or passwords
☐ Yes I sent money
☐ Yes I sent personal details and money

If you sent money as result from some other scam type, what is your best estimate of the total amount of money you have sent in the last 12 months?

Note: This refers to the money you have paid out as a result of a request. This does NOT include money that you would have received if the offer had been legitimate.

Please indicate the amount in whole dollars. E.g. $1000.00 should be entered as $1000

Please indicate the amount sent before any intervention or repayment from insurance, your bank or legal action

- [ ] Don't know/ I can't recall
- [ ] I'd rather not say
- [ ] The amount in the box below

Please indicate the amount in whole dollars, do not include dollar signs ($):

If you responded to the other scam type by sending money or personal details or passwords, how many times were you in contact with the person(s) before you sent the money or personal information?

- [ ] Once only
- [ ] Two to five times
- [ ] Six to 10 times
- [ ] 11 to 20 times
- [ ] More than 20 times
- [ ] I can't recall

Have you reported this scam to anyone? (Select all that apply)

- [ ] Not reported to anyone
- [ ] Family/ friends
- [ ] Police
- [ ] SCAMwatch website (www.scamwatch.gov.au)
- [ ] Australian Competition and Consumer Commission/ Fair Trading or Consumer Protection agencies
- [ ] The business represented (eg. bank, eBay etc)
- [ ] Internet Service Provider
- [ ] Legal aid, a lawyer, or a community legal services clinic
- [ ] Unable to recall
- [ ] Other

If you reported to 'other', please specify:

11.

If you received any scams that you did not respond to in any way, what was your reason for not responding? (Select all that apply)

- [ ] I did not receive a scam invitation
- [ ] Seemed too good to be true
- [ ] Had received similar offers before and thought they were scams
- [ ] Had seen/ heard this was a type of scam in the media or from a public source
- [ ] Was told it was a scam by someone I knew
- [ ] Someone I know has been a victim of a scam before
- [ ] Wanted to respond but could not afford to participate
- [ ] Something was not quite right with the offer or invitation
- [ ] Offer was identified as spam/ declared unsafe by Internet filter
- [ ] Other

If 'other', please provide details for your main reason for not responding to the scam:

12.

If you received a scam that you did report to a formal agency, what was your reason for doing so? (Select all that apply)

- [ ] I did not receive a scam invitation
- [ ] Not applicable (I did not report any scams)
- [ ] Desired the apprehension of offender(s)
- [ ] Wanted to prevent others from being scammed
- [ ] Knew it was the right thing to do

- [ ] To assist in the investigation of an offence
- [ ] To support your insurance claim
- [ ] Other

If 'other', please provide details for the primary reason you reported the scam to a formal agency:

13.

If you received a scam that you did not report to a formal agency, what was your reason for not doing so? (Select all that apply)

- [ ] I did not receive a scam invitation
- [ ] Not worth the effort
- [ ] Didn't think it was illegal
- [ ] Unsure of which agency to contact
- [ ] Feared I would get into trouble
- [ ] Didn't think anything would be done
- [ ] Received too many to report
- [ ] Other

If 'other' please provide details for the primary reason you did not report the scam to a formal agency:

14.

Have you reported any of the scams specified in Q1-10, on behalf of anyone else?

- [ ] Yes
- [ ] No

If 'yes' please indicate the category of peron on behalf of whom you reported the scam (select all that apply).

- [ ] Your child (son or daughter)

☐ Your older relative (brother/ sister, parent, grandparent, aunt/ uncle)
☐ Your younger relative (niece / nephew, brother/ sister)
☐ A friend
☐ A colleague
☐ A student (if you are a teacher or in some similar capacity)
☐ Other

If 'other', please specify

15.

How do you regard each of the following scam incidents? (Select one response for each type of scam listed)

Type of Scam	A crime	Wrong but not a crime	Just something that happens
Notification of having won a lottery or some other prize	☐	☐	☐
A request for assistance to transfer money out of another country (such as Nigeria)	☐	☐	☐
A notification of an inheritance	☐	☐	☐
A request by a business to confirm your personal details or passwords (phishing scams)	☐	☐	☐
A request to supply you with financial advice	☐	☐	☐
A request to buy, sell or retain securities or other investments (including superannuation investments)	☐	☐	☐
An opportunity to work from home (a front for money laundering)	☐	☐	☐
Pursuing a personal relationship that later turned out to be false	☐	☐	☐
Computer support centre scam	☐	☐	☐
Other type of scam	☐	☐	☐

If ‘other’ please provide details for the most frequent scam received:

16.

How did you find out about this survey? (Select all that apply)

- ☐ Media article
- ☐ A Government website
- ☐ SCAMwatch website (www.scamwatch.gov.au)
- ☐ Poster or pamphlet
- ☐ Referred by other agency
- ☐ Word of mouth (family, friends etc)
- ☐ Other

If ‘other’, please provide details for how you heard about the survey:

17.

Have you responded to this online survey in any previous years? (Select all that apply)

- ☐ 2012
- ☐ 2011
- ☐ 2010
- ☐ 2009
- ☐ 2008
- ☐ Never

18.

Are you aware of the 2013 fraud awareness campaign run by the Australasian Consumer Fraud Taskforce?

- [ ] Yes
- [ ] No

19.

Were you aware of any previous campaigns run by the Australasian Consumer Fraud Taskforce?

- [ ] Yes
- [ ] No

20.

Which age group do you belong to?

- [ ] 17 and under
- [ ] 18-24
- [ ] 25-34
- [ ] 35-44
- [ ] 45-54
- [ ] 55-64
- [ ] 65+

21.

What is your sex?

- [ ] Male
- [ ] Female

22.

Where do you normally reside?

- [ ] Australian Capital Territory
- [ ] New South Wales

- [ ] Northern Territory
- [ ] Queensland
- [ ] South Australia
- [ ] Tasmania
- [ ] Victoria
- [ ] Western Australia
- [ ] New Zealand
- [ ] Resident of a country other than Australia or New Zealand (please specify below)

Please specify country, if other than Australia or New Zealand:

If you normally reside in Australia what is your postcode?

If you normally reside in New Zealand, what is your postcode?

23.

What was your gross income from all sources for the year 2011-2012 (i.e. before tax deductions)?

- [ ] Under $20,000
- [ ] $20,000 – <$40,000
- [ ] $40,000 – <$60,000
- [ ] $60,000 – <$80,000
- [ ] $80,000 or over
- [ ] I'd rather not say

24.

Why did you choose to complete this survey? (Select all that apply).

- [ ] Recently been scammed
- [ ] Receive scams but have not been scammed
- [ ] Want to assist in research to combat scammers
- [ ] To learn more about scams
- [ ] Other

If 'other', please provide details for the primary reason you participated in the survey:

25.

In which capacity did you fill out this survey? (Select one only)

- [ ] Member of the public
- [ ] Retiree
- [ ] Member of the police
- [ ] My employer is an Australasian Consumer Fraud Taskforce Government member
- [ ] My employer is an Australasian Consumer Fraud Taskforce private sector partner
- [ ] My employer is another government agency

Thank you for completing the 2013 Australasian Consumer Fraud Taskforce Survey. If you are happy with your responses please click the "submit" button below. Alternatively you can review and change your responses and then submit.

Appendix 2: Newspaper articles relating to consumer fraud published 17 to 23 June 2013

- Collier K 2013. Online scams a growth industry. *Herald Sun* 17 June.
- The Cairns Post 2013 Scams rip off $93m. *The Cairns Post* 18 June.
- The Mercury 2013. Australians lose $93m to scams. *The Mercury* 18 June.
- Sunshine Coast Daily 2013. Online shoppers ripe for scams. *Sunshine Coast Daily* 17 June.
- Colley A 2013. Australians lose $93 million to scams. *The Australian* 17 June.
- Flower W 2013. False text messages racket cashes in on mobile phone charges. *The Sun Herald* 23 June.
- Daily News 2013. Buyers urged to sidestep scams. *Daily News* 18 June.
- Bainbridge A 2013. Australians lose $93m to online scams. *The World Today* Australian Broadcasting Corporation 17 June.
- Baker M 2013. Aussies are falling for online scams. *The Examiner* 23 June.
- Taranaki Daily News 2013. Scams rely on good guys and the gullible. *Taranaki Daily News* 19 June.
- Gold Coast Sun—Central 2013. Scammers on the increase. *Gold Coast Sun—Central* 20 June.
- The Gympie Times 2013. Tell local police of an online fraud. *The Gympie Times* 18 June.
- Free Press Leader 2013. Street Watch. 19 June.
- Wannan O 2013. Family shock at $160,000 ripoff. *The Press* 17 June.
- Tran D 2013. Conman Cometh. *Monash Weekly* 17 June.
- The Advertiser 2013. Scam victims chalk up losses totalling $93m. *The Advertiser* 18 June.
- Whyte S 2013. Heartbreak with a heavy load as online dating dupes people out of millions: Consumer Affairs. *The Sydney Morning Herald* 17 June.
- Bainbridge A 2013. ACCC forum hears online shopping 'licence' could help stamp out fraud. *ABC Premium News* 18 June.
- Whyte S 2013. Scammers dupe online lovers out of millions. *The Canberra Times* 17 June.
- Geelong Advertiser 2013. You've been had for $93 m. *The Geelong Advertiser* 18 June.
- The Daily Advertiser 2013. Scammers fleeced Aussies out of more than $93 million. *The Daily Advertiser* 18 June.
- Higgins K 2013. Fight the fraudsters. *Townsville Bulletin* 21 June.

- Townsville Bulletin 2013. Scammers took Aussies for a $93m ride last year. *Townsville Bulletin* 18 June.
- The Southern Star 2013. Conversations. *The Southern Star* 19 June.
- The Standard 2013. Criminals love the internet and more of them are hiding. *The Standard* 18 June.
- Wannan O 2013. Cruel dating scam hits dying mother. *Dominion Post* 17 June.
- The Gold Coast Bulletin 2013. How to avoid web of deceit. *The Gold Coast Bulletin* 22 June.
- Waikato Times. 2013. Dating scam cost woman inheritance. *Waikato Times* 17 June.
- Taranaki Daily News 2013. Emails leave a tragic trail in an internet romance gone wrong. *Taranaki Daily News* 17 June.
- Bainbridge A 2013. Online shopping licence mooted for consumers. *ABC Premium News* 18 June.
- The Northern Territory News 2013. Scammers cost us $500,000. *The Northern Territory News* 21 June.
- The Queensland Times 2013. In Brief. *The Queensland Times* 17 June.
- Knox Leader 2013. Street Watch. *Knox Leader* 18 June.
- The Chronicle 2013. In Brief. *The Chronicle* 21 June.
- Caboolture Shire Herald 2013. Caution needed on the internet. *Caboolture Shire Herald* 20 June.
- The Chronicle 2013. In Brief. *The Chronicle* 22 June.

AIC Reports
Technical and Background Paper 58

Australia's national research and
knowledge centre on crime and justice

aic.gov.au