Australian Government
Australian Institute of Criminology

AIC reports
Research report 01

Australasian Consumer Fraud Taskforce: Results of the 2014 online consumer fraud survey

Penny Jorna

ISSN (Online) 2206-7280
ISBN (Print) 978 1 922009 96 8

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6243 6666
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.

All publications in the Research Report series are subject to peer review – either through a double-blind peer review process, or through stakeholder peer review. This report was subject to an extensive stakeholder peer review process.

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

General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

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

Tables

Figures

Acknowledgements

This research was conducted on behalf 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 entities 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.

Executive summary

The Australasian Consumer Fraud Taskforce (ACFT) is a group of 22 government regulatory agencies and departments in Australia and New Zealand. It works with private sector, community and non-government partners to prevent fraud. The ACFT has run a range of fraud prevention and awareness-raising activities since 2005. One of its key initiatives is to run an annual consumer fraud survey to take a snapshot of the public's exposure to consumer fraud and fraudulent invitations, to assess their impact, determine how victims respond, and identify emerging typologies and issues. The Australian Institute of Criminology (AIC), as a taskforce member and chair of its research subgroup, hosts the survey on behalf of the ACFT. It should be noted that the survey participants were not randomly sampled and so survey findings are not representative of the general population.

This report presents the results of the 2014 survey, which ran for six months from 1 January 2014. This period encompassed National Fraud Prevention week, which coincides with global fraud awareness-raising activities. The theme of the 2014 campaign was *Know who you're dealing with*, and it was aimed at raising awareness about relationship scams by asking people to think twice before transferring money to people they did not know personally.

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 (fraudulent lottery invitations);
- a request for assistance to transfer money out of another country, such as Nigeria (advance fee frauds);
- a notification of an inheritance (fraudulent invitations about inheritances);
- a request by a business to confirm personal details or passwords (phishing);
- a request to buy, sell or retain securities or other investments (fraudulent boiler-room invitations);
- a request to supply financial advice (fraudulent financial advice invitations);
- an opportunity to work from home (a fraudulent invitation to earn large sums of money by working from home);
- a person representing themselves as someone from a computer support centre to 'fix' their computer (fraudulent computer support centre invitations);
- pursuing a personal relationship that turned out to be false (fraudulent dating or social networking invitations); and
- other fraud types.

The survey could be completed on the AIC's website. Participants not living in Australia or New Zealand were excluded, as were invalid responses. In 2014, 879 participants completed the survey. Excluding participants from overseas, 865 responses were available for analysis.

The findings of the 2014 survey cannot be taken as representative of the experiences of the greater Australasian population, given the self-selected, online sampling used in the survey design. As the sample was not randomly selected, those who participated may have differed from the general population in terms of their experience of consumer fraud. The results do, however, reflect the experiences of a large sample of individuals from across Australia and New Zealand.

Delivery of fraudulent invitations

The 2014 survey asked respondents about the types of fraudulent invitations they had received, as well as how the invitations had been delivered to them. Results indicated that:

- 98 percent of respondents reported having received at least one fraudulent invitation in the 12 months preceding the survey;
- the most common type of fraudulent invitation received was computer support centre fraud (received by 63% of the total sample), fraudulent lottery invitation (61%) and phishing schemes (55%);
- the least common type of fraudulent invitation received was the boiler-room invitation, which was reported by just six percent of the total sample; and
- email was the most common delivery method, with 77 percent of those who received a fraudulent invitation reporting that they had received it via email.

Responding to fraudulent invitations

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

- 25 percent of survey participants responded in some way to a fraudulent invitation in the 12 months preceding the survey;
- five percent of respondents (who received an invitation in the 12 months prior to the survey) sent personal details or passwords as a result of the invitation;
- six percent of respondents reported sending money as a result of a fraudulent invitation in the 12 months preceding the survey;
- three percent of respondents reported both sending their personal details and having experienced a financial loss;
- eighteen respondents suffered a financial loss and sent personal details to multiple fraudulent invitations in the 12 months preceding the survey;
- the median amount reported lost to fraudulent invitations was $900, with a total financial loss of $230,707.75. This is the lowest loss amount reported since the AIC began the surveys; and
- the top two reasons for not responding to a fraudulent invitation were that the respondent had received similar offers before and thought they were fraudulent (51% of the total sample) and ‘had seen/heard this was a type of fraud in the media or from a public source’ (48% 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 fraudulent invitation. Analysis of the demographic variables of the victims indicated that:

- of the survey respondents who disclosed their gender (98% of respondents disclosed their gender) 67 percent of respondents who experienced victimisation (n=88 victims) were female and 33 percent were male;
- in 2014, the age category that reported the highest percentage of victimisation was 'over 65' years (13% of total respondents within that age category); and
- in 2014, individuals earning between $20,000 and $40,000 a year reported the highest percentage of victimisation (16% of total respondents in that income category). This does not include the 'I'd rather not say' category.

Reporting consumer fraud

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

- in 2014, 73 percent of the total sample (75% of those who received a fraudulent invitation) reported a fraudulent invitation to at least one person or organisation;
- family and friends were the most common recipients of fraud complaints, with 51 percent of the total sample reporting to this category in 2014;
- the most common reasons for reporting fraudulent invitations were 'wanted to prevent others from being scammed' (33% of the total sample), and 'knew it was the right thing to do' (22% of the total sample); and
- the most common reasons provided for not reporting fraudulent invitations were 'unsure of which agency to contact' (37% of the total sample), 'I didn't think anything would be done' (32% of the total sample), and 'not worth the effort' (29% of the total sample).

Perceptions of consumer fraud

Respondents were asked whether they considered each fraudulent invitation type to be *a crime*, *wrong but not a crime*, or *just something that happens*. The results indicated that:

- in 2014, the top three fraudulent invitation types to be considered a crime by respondents were exactly the same as those reported in the 2013 survey, namely, advance fee fraud (84%), phishing (82%) and computer support fraud (76%).

Protecting personal information

The theme of the 2015 National Consumer Fraud Week was: *Get smarter with your data*. The focus of the week was to raise awareness of consumer fraud and the need for individuals to

protect themselves against fraudulent invitations, with a focus on protecting personal details and passwords. With that theme in mind the 2014 survey participants who had been exposed to or victimised as a result of fraudulent invitations, especially phishing and similar frauds, were reviewed. It was reported that:

- forty-one respondents (47% of victims in the sample) sent personal information or passwords as a result of a fraudulent invitation;
- email and the telephone were the most common methods of delivery of fraudulent invitations received by victims who lost personal details as a result of the fraud; and
- thirty-four percent of respondents who had received a phishing invitation reported the invitation to an organisation or a statutory authority.

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:

- *how people react to receiving fraudulent invitations*. Future campaigns could examine why people respond to invitations, what would reduce the likelihood of their responding, and how their online behaviour changes after recognising a fraud; and
- *educating the public on common themes used in fraudulent invitations*. The 2014 survey identified quite a few respondents who were the victims of multiple different fraudulent invitations. An awareness campaign that identified elements common to most frauds could help people to better understand the deception involved with frauds and inform the development of more targeted prevention initiatives.

Introduction

The purpose of this paper is to report the findings from the Australasian Consumer Fraud Taskforce (ACFT) 2014 survey to provide an overall picture of the nature of consumer fraud in Australasia.

Australasian Consumer Fraud Taskforce

The ACFT, chaired by the Australian Competition and Consumer Commission (ACCC), was formed in March 2005. It is made up of 22 Australian and New Zealand governmental regulatory agencies and departments responsible for consumer protection regarding frauds and scams, including consumer protection and policing agencies at the state and federal levels. The taskforce also has a range of partners from the community, non-government and private sectors with an interest in increasing the level of fraud awareness in the community. The aim of the ACFT is to take a coordinated approach to reducing the number of incidents, and the impact of consumer frauds and scams. Each year the taskforce coordinates a week-long information campaign, timed to coincide with global consumer fraud prevention activities.

The Australian Institute of Criminology (AIC) has conducted an annual survey to assess consumer fraud experiences since 2006. 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, Jorna and Hutchings (2013) for the 2012 survey results and Jorna (2015) for the results of the 2013 survey. The survey reported in this paper ran for six months between January and June 2014, which included the taskforce's annual fraud week.

Defining consumer fraud and fraudulent invitations

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 fraud category, with fraud referring to matters involving dishonesty and deception. A range of consumer fraud activities may be classified as fraudulent invitations. Nine common types of consumer frauds were explored in the 2014 ACFT survey namely: advance fee fraud,

dating schemes, financial advice fraud, boiler-room fraudulent invitations, inheritance schemes, lottery fraud, phishing, work from home schemes, and fraud involving computer support. An additional 'other' category was offered to respondents for fraud types that did not fall into the supplied categories. Definitions for these fraudulent invitations are provided in Table 1. Consumer frauds target individuals and consumers, rather than businesses or governments (Budd & Anderson 2011).

Table 1: Common fraudulent schemes and their definitions

Fraudulent money transfers	Advance fee frauds have existed throughout history and have adapted to advances in technology. Generally, these frauds are communicated by email or letter and seek help to transfer a large amount of money overseas. These are the most commonly complained about frauds in Australia, according to the ACCC.
Dating/social networking schemes	Dating and social networking schemes may exist through illegitimate or legitimate dating or social networking websites and may require payment for each email sent and received by a potential match. Alternatively, fraudsters may hook victims by claiming to have a sick relative or severe financial trouble and seeking assistance. Due to the trust already established, victims may be more easily duped and are often shocked when fraudsters no longer communicate after money has been sent.
Fraudulent financial advice	Fraudulent financial advice schemes are offered by fraudsters cold-calling from overseas and sharing 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 or investment fraud	Requests to buy, sell or retain securities or other investments (including superannuation investments) that are usually offered through cold-calling by fraudsters who seek to sell worthless shares or investments to recipients.
Inheritance frauds	Inheritance frauds are usually sent by a 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 victim a large inheritance.
Lottery fraud	A lottery fraud may be delivered by email, text message or pop-up screen falsely claiming the victim has won a prize or competition.
Phishing	Phishing refers to emails that trick people into giving out their personal details and banking information. They are increasingly also sent by SMS.
Work from home fraudulent invitations	Working from home frauds are often promoted through spam emails or advertisements on noticeboards, however they are generally not advertising real jobs. Working from home frauds 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 fraud occurs when recipients receive mainly telephone calls from fraudsters claiming they are from well-known computer manufacturers or businesses that can fix problems with the recipients' computers. Fraudsters may ask for money, personal details or passwords or seek to sell worthless products to fix computers.

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 fraud;
- the types of frauds or fraudulent invitations that attracted the most victims;
- the factors relevant to victimisation; and
- what affects the reporting of fraud and fraudulent invitations.

Each year, an anonymous online survey hosted by the AIC has been used to collect data. As with the 2013 survey period, the 2014 survey ran from 1 January until 30 June 2014. The survey timeframe was chosen to correspond with the ACFT fraud awareness campaign (16 to 22 June) and to enable data to be collected before and after the campaign to assess its impact 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 to a large public audience and does not involve administration costs such as postage or interview expenses. It also allows respondents to remain anonymous, which was considered an advantage 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 respondent's exposure to, and victimisation from, consumer fraud (see Appendix 1). These questions were developed in consultation with taskforce committee members. Information was sought on the following consumer frauds:

- lottery frauds;
- advance fee frauds;

- inheritance frauds;
- phishing;
- fraudulent financial advice;
- boiler-room or investment frauds;
- fraudulent work from home invitations;
- frauds involving computer support; and
- dating and social networking frauds.

An 'other' response category was also included to capture additional fraudulent invitations. Questions related to respondents' experience of consumer fraud in the 12 months prior to the survey, as well as their personal demographics and awareness of ACFT activities.

Only minor changes were made to the questionnaire which:

- asked about satisfaction with reporting;
- restructured how many times responded and then how many times in contact; and
- asked about the outcome of reporting.

Limitations of the survey

The 2014 AIC survey experienced the same methodological constraints as those identified in previous years (Budd & Anderson 2011; Hutchings & Lindley 2012; Jorna & Hutchings 2013; Smith & Akman 2008). Limitations associated with the non-stratified sample and the non-random, self-selection aspect of the survey make it difficult to generalise the findings to the wider population. This is because those who had received a fraudulent invitation and/or fallen victim may be more likely to complete the survey than those who had not. In addition, the survey was not representative of age groups, gender or location compared with national specifications. A further difficulty was that completing the survey was limited to those who had access to a computer, which may have meant that those without access were unable to participate. To overcome this limitation, SCAMwatch employees were able to complete a survey over the phone on behalf of those respondents without access.

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 gaps between when fraudulent invitations are received or carried out, identified by the victim and then reported (if indeed they are reported). The reference period for the 2014 AIC online survey was the previous 12 months, with respondents being asked about whether they had received and responded to fraudulent invitations in that time. As the 2014 survey ran from January to June 2014, this could potentially include 18 months within the survey period. It is possible that respondents may have forgotten some incidents or incorrectly recalled dates and events.

In addition to those difficulties specific to this survey there are general problems common with using 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 no way to determine whether the

responses given are accurate reflections of the events reported. As a result, the survey findings cannot provide a robust measurement of consumer fraud victimisation rates in Australasia.

Due to the limitations of the data as outlined above, descriptive analyses were predominantly used to report the results, particularly frequency distributions and percentages. As the survey was designed to capture information relating to respondents living in Australia or New Zealand, respondents who indicated they lived elsewhere were excluded from the sample. Only completed responses were included in the sample for analysis.

The following sections present the key results from the 2014 ACFT survey.

The 2014 consumer fraud survey results

Sample characteristics

Between 1 January and 30 June 2014, 874 people responded to the survey hosted on the AIC's website (www.aic.gov.au). Nine respondents were removed, as they did not live in Australia or New Zealand, leaving 865 responses to form the sample for analysis.

Eighty-eight percent of respondents (n=762) reported that they completed the survey in their capacity as a member of the public. Of that 88 percent, 175 (23%) were retirees. Six respondents (0.7%) were police, 18 (2.1%) were employed by an ACFT government agency, three (0.3%) were employed by a taskforce private sector partner, and 71 (8.2%) were employed by another government agency.

Websites were the most popular way in which respondents were directed to the survey, with the SCAMwatch site referring 303 (35%) respondents, and other government websites referring 172 (19.9%). The media generated 122 responses (14.1%); posters and pamphlets attracted six respondents (0.7%) with 54 respondents (6.2%) being referred to the survey by another agency. A further 62 respondents (7.2%) found out about the survey through word of mouth. Two hundred and sixteen respondents had learnt about the survey through other means, such as 'neighbourhood watch newsletters', local police notifications and social networking sites such as Twitter and Facebook.

Seventeen percent (n=144) were aware of the ACFT's 2014 campaign, and 16 percent (n=135) were aware of campaigns that had been run in previous years. Forty-four respondents (5%) had completed the 2013 survey, 27 (3.1%) had completed the 2012 survey, 11 (1.3%) had completed the 2011 survey and seven respondents (0.8%) had completed the 2010 survey. A total of 783 respondents (90.5%) had never previously completed the survey.

The survey received an average of 36 responses a week in the 24 weeks before the 2013 campaign (n=859); five participants completed the survey during the week-long campaign; while the remaining five completed the survey in the week following the campaign. Fifty-two percent (n=451) of participants completed the survey within the first month of the survey opening (January 2014).

Survey respondents were asked why they chose to complete the survey. Most (n=652, 75%) wanted to 'assist in research to combat scammers'. A further 362 participants (72%) chose to participate because 'they had received scams, but not been scammed'; whereas 120 participants (14%) completed the survey because they had 'recently been scammed' and 183 completed the survey as they 'wanted to learn more about scams'. Fifty-eight participants provided 'other' reasons for completing the survey. These ranged from family members or friends falling victim to fraudulent invitations, 'wanting to create awareness of new scams', and people believing that personal fraud had not been taken seriously enough.

Demographics

Females made up 57 percent of the sample (n=491), and males 41 percent (n=356). Two percent (n=18) declined to disclose their gender. Table 2 shows the breakdown of respondents by age group.

Sixty-six percent of the sample was aged over 45 years. Those 17 years and under were the least likely to complete the survey, with only 12 participants (1.4%) in that category (see Table 2).

As shown in Figure 1, most survey participants lived in New South Wales (28.2%, n=244), Queensland (22.9%, n=198) and Victoria (17.5%, n=151). As with previous years, the least number of respondents lived in New Zealand (0.7%, n=6). Tasmania (3.9%, n=34), the Northern Territory (0.9%, n=8) and Western Australia (6.8%, n=59) were the least represented states and territories in Australia.

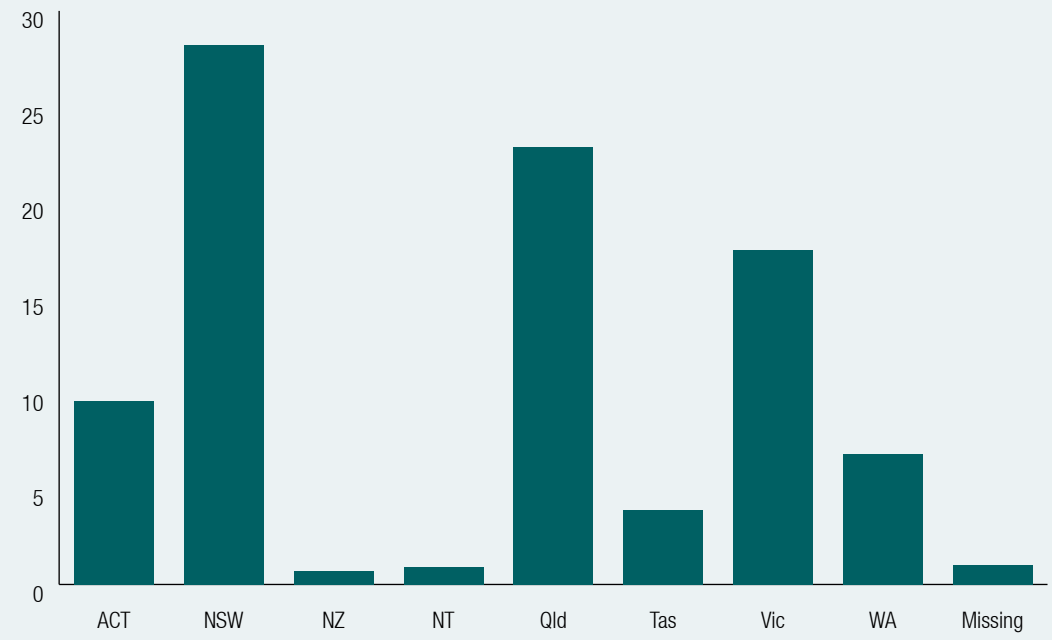
When asked about income, almost a third of respondents (n=272, 31.5%) responded that they would rather not disclose their income details. More than a third of the sample, 321 (37%) reported income levels that ranged between $20,000 to less than $80,000. Thirteen percent (n=116) reported an annual income of less than $20,000 and 18 percent (n=156) earned more than $80,000 a year. This is shown in Figure 2.

Table 2: Respondents by age (n and %)

Age category (years)	n	%
17 and under	12	1.4
18–24	31	3.6
25–34	98	11.3
35–44	137	15.8
45–54	208	24.1
55–64	191	22.1
65 and over	171	19.8
I'd rather not say	17	2.0
Total	865	100.0

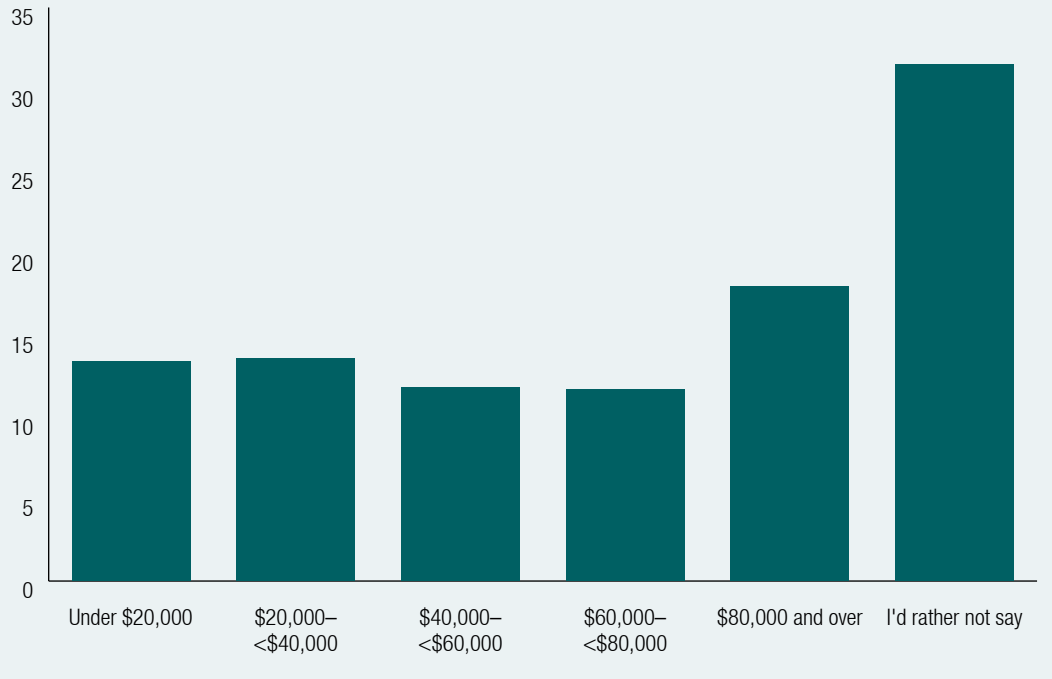
Note: Percentages may not total 100 due to rounding
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Figure 1: Respondents by region (%)



Note: Percentages may not total 100 due to rounding
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Figure 2: Respondents by annual income (%)



Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Receiving fraudulent invitations

Of the 865 survey participants in 2014, 844 (98%) had received at least one unsolicited fraudulent invitation. The number and percentage of invitations is provided by fraud type in Table 3.

Respondents may have received an invitation for more than one fraud type. The most common type received, reported by 545 (63%) of survey participants, was the fraudulent computer support centre scheme. This was followed by lottery fraud invitation, received by 527 participants (61% of survey participants). The least common was the boiler-room fraud invitation, received by just 41 (5%) survey participants.

The types of delivery methods by which respondents reported receiving fraudulent invitations are provided in Table 4. If participants received more than one fraudulent invitation, multiple responses are recorded.

Table 3: Fraudulent invitations received by fraud type

Fraud	Received invitation (n)	Received invitation (%) (n=844)	Total sample (%) (n=865)
Lottery frauds	527	62.4	60.9
Advance fee fraud	373	44.2	43.1
Inheritance fraud	297	35.2	34.3
Phishing	473	56.0	54.7
Financial advice schemes	121	14.3	14.0
Boiler-room fraud	41	4.9	4.7
Work from home fraudulent invitations	309	36.6	35.7
Fraudulent computer support schemes	545	64.6	63.0
Dating/social networking fraud	131	15.5	15.1
Other	281	33.3	32.5

Note: Percentages may not total 100 due to rounding
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

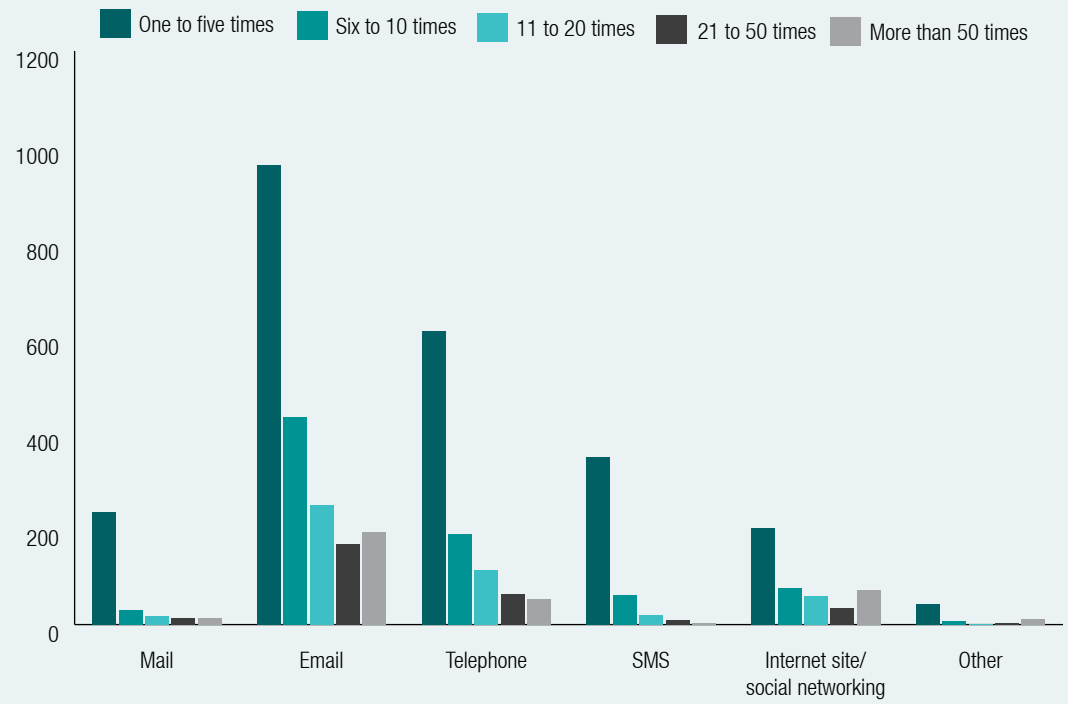
Table 4: Fraudulent invitations by delivery method			
Method of delivery	Received an invitation (n)	Received an invitation (%) (n=844)	Total sample (%) (n=865)
Mail	211	25.0	24.4
Email	646	76.5	74.7
Telephone	624	73.9	72.1
SMS	312	37.0	36.1
Internet site/social networking	251	29.7	29.0
Other	47	5.6	5.4

Note: Respondents could select multiple delivery methods therefore percentages will not total 100
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Email was the most popular delivery method, with 76.5 percent (n=646) of respondents who had received a fraudulent invitation, receiving this via email. Following the trends from recent years, the landline telephone closely followed email as the most common delivery method and was reported by 624 (74%) respondents who had received a fraudulent invitation. The least popular method for delivering fraudulent invitations was via mail, reported by only 211 respondents (25% of those who received an invitation).

Respondents were asked how many times over the previous 12 months had they received fraudulent invitations by each delivery method. The responses are shown in Figure 3. As in past years, email remains the most common fraud delivery method and people can receive multiple invitations this way. However, it should be noted that invitations received by landline telephone are also becoming a common delivery method, with fraudulent invitations received via this method increasing from 67 percent of the sample in 2013 to 72 percent of the total current sample. Some examples of 'Other' delivery methods included face-to-face fraud delivery and respondents spotting what they perceived to be fraudulent invitations in magazines and pamphlets.

Figure 3: Number of fraudulent invitations received by delivery method (n)



Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Responding to fraudulent invitations

In the 12 months before the survey completion date, 220 (25%) of the survey participants responded to a fraudulent invitation by requesting further information, providing personal details, suffering a financial loss, or providing personal information and suffering a financial loss. This represented 26 percent of those who had received a fraudulent invitation during the 12-month period.

Ten percent of the sample who had received an invitation sent their personal details, suffered either a financial loss or lost both money and personal details in response to at least one invitation (n=88, 10% of the total sample). Forty-one participants (5% of the sample who received a fraudulent invitation and 4.7% of the total sample) sent their personal details or passwords only, and 28 participants (3% of the total sample) sent money only to at least one invitation. Twenty-four participants (2.8% of the total sample and 11% of the sample who had responded to a fraudulent invitation) sent personal details and suffered a financial loss as a result of a fraudulent invitation or in some cases, multiple fraudulent invitations (see Table 7).

Tables 5 and 6 show the number of respondents who provided personal details or lost money to each type of fraud, as well as the percentage of the total sample who received any type of fraudulent invitation, and the percentage of the sample who received that particular fraudulent invitation. Table 7 shows the number of respondents who, as a result of the fraud, provided

personal data and suffered a financial loss. Some respondents provided personal details and/or lost money as the result of multiple frauds. Eighteen respondents advised that they had sent money (multiple times), personal details and sometimes both as a result of a fraudulent invitation.

Table 5: Loss of personal details only by fraudulent invitation type

Invitation type	Personal details provided (n)	Received an invitation (%) (n=844)	Total sample (%) (n=865)	Received an invitation to that particular fraud type (%)
Lottery fraud	6	0.71	0.70	1.14
Advance fee fraud	1	0.12	0.12	0.27
Inheritance fraud	0	0	0	0
Phishing	17	2.01	2.00	3.59
Financial advice fraud	2	0.24	0.23	1.65
Boiler-room frauds	0	0	0	0
Work from home fraud	2	0.24	0.23	0.65
Computer support centre frauds	10	1.18	1.17	1.83
Dating or social networking fraud	2	0.24	0.23	1.53
Other types of fraudulent invitations	12	1.42	1.39	4.27

Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Table 6: Loss of money only by fraudulent invitation type

Invitation type	Suffered a financial loss (n)	Received an invitation (%) (n=844)	Total sample (%) (n=865)	Received an invitation to that particular fraud type (%)
Lottery fraud	3	0.36	0.35	0.57
Advance fee fraud	6	0.71	0.69	1.60
Inheritance fraud	0	0	0	0
Phishing	2	0.24	0.23	0.42
Financial advice fraud	1	0.12	0.12	0.83
Boiler-room frauds	0	0	0	0
Work from home fraud	0	0	0	0
Computer support centre frauds	4	0.47	0.46	0.73
Dating or social networking fraud	7	0.83	0.81	5.34
Other types of fraudulent invitations	12	1.42	1.39	4.27

Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

In the 2014 survey, no respondents reported losing money to a fraudulent inheritance invitation, a boiler-room fraud, or a fraudulent invitation to work from home. Likewise, no respondents advised providing personal details to fraudulent invitations about inheritances or boiler-room frauds. Consistent with surveys from prior years, dating/social networking fraudulent invitations had the highest conversion rates, that is, they were the type of fraudulent invitation that would lead to respondents sending money as a result of the invitation. Of all the respondents who received a dating or social networking fraudulent invitation, more than five percent (n=7 of the 131 respondents who received that type of invitation) suffered a financial loss. The type of fraudulent invitation that had the lowest conversion rate in terms of suffering a financial loss was the phishing invitation. This fraud type caused the most respondents (aside from 'other fraudulent invitations') to lose personal details or passwords as a result of those fraudulent invitations (3.6% of the 473 participants who received those invitations).

Quite a few respondents advised they had sent money and/or personal details to more than one fraudulent invitation. Two respondents had sent personal details or passwords to more than one fraudulent invitation, and a further two suffered financial losses as a result of multiple fraudulent invitations. One respondent sent personal details or passwords to one fraudulent invitation and then suffered a financial loss as a result of another fraudulent invitation.

Table 7: Loss of money and personal details

Fraud type	Suffered loss of money and personal details	Received an invitation (%) (n=844)	Total sample (%) (n=865)	Received an invitation to that particular fraud type (%)
Lottery fraud	3	0.36	0.35	0.57
Advance fee fraud	3	0.36	0.35	0.80
Inheritance fraud	0	0	0	0
Phishing	3	0.36	0.35	0.63
Financial advice fraud	2	0.24	0.23	1.65
Boiler-room frauds	1	0.12	0.12	2.44
Work from home fraud	1	0.12	0.12	0.32
Computer support centre frauds	4	0.47	0.46	0.73
Dating or social networking fraud	7	0.83	0.81	5.34
Other types of fraudulent invitations	9	1.07	1.04	3.20

Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

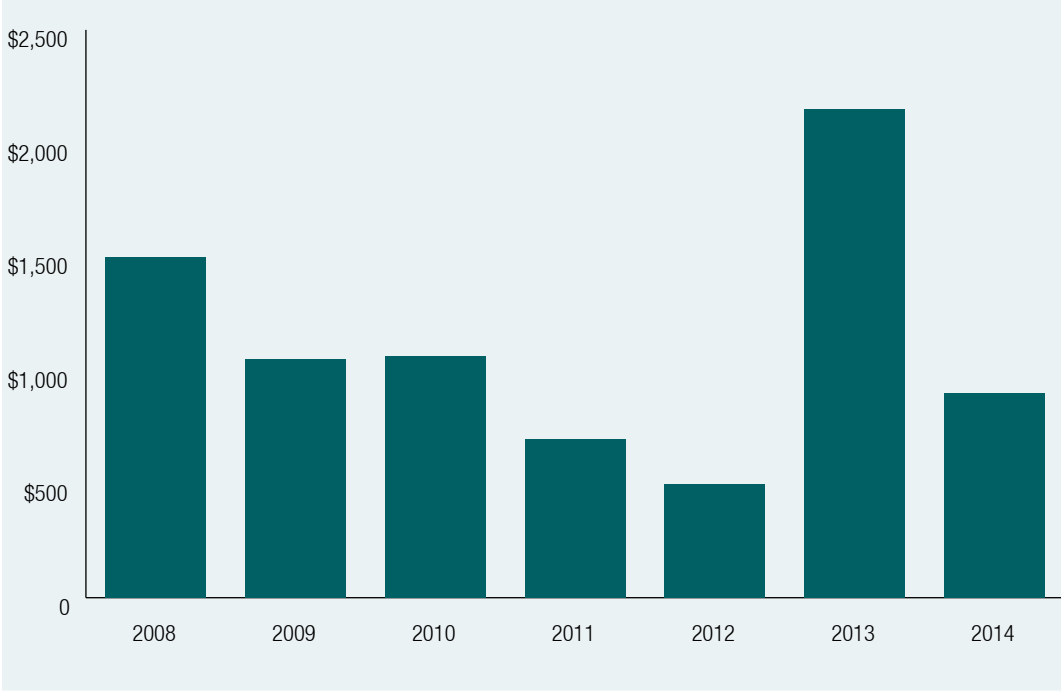
Of the 52 participants in the survey who reported suffering a financial loss (either sending money only to a fraudulent invitation, or having sent money and personal details in response

to a fraudulent invitation), 51 (99%) disclosed the amount sent. This ranged from $49.95–$38,000. For the first year since the AIC began conducting the survey no obvious outliers were included in the amounts lost and so all amounts were included in the analysis. The reported financial losses incurred by participants totalled $230,707.75, (mean=$4,500, median=$900).

As shown in Figure 4, the median financial loss reported over the years that the ACFT survey has been running had been steadily declining until 2013, when the amount lost by respondents spiked. In 2014 the median financial loss decreased to $900, which, aside from 2013, was still higher than other reported losses since 2010.

Participants were able to select multiple responses when asked why they did not respond to fraudulent invitations (see Table 8). The most common reasons for not responding to fraudulent invitations included 'had received similar offers before and thought they were fraudulent' (reported by 50.5% of the total sample), and 'had seen/heard this was a type of fraudulent invitation in the media or a public source' (48% of the total sample). The least common reason for not responding to a fraudulent invitation was 'wanted to respond but could not afford to participate' (0.7% of the total sample).

Figure 4: Median reported financial loss by year ($)



Source: ACFT Consumer Fraud Surveys 2008–14 [AIC computer file]

Table 8: Reasons for not responding to fraudulent invitations received

Reason for not responding	n	Received an invitation (%) (n=844)	Total sample (%) (n=865)
Seemed too good to be true	331	39.2	38.3
Had received similar offers before and thought they were fraudulent	437	51.8	50.5
Had seen/heard this was a type of fraudulent invitation in the media or a public source	415	49.2	48.0
Was told it was fraudulent by someone I knew	124	15.0	14.3
Someone I know has been a victim of a fraud before	64	7.6	7.4
Wanted to respond but could not afford to participate	6	0.7	0.7
Something was not quite right with the offer or invitation	377	44.7	43.6
Offer was identified as spam/ unsafe by internet filter	201	23.8	23.2
Other	142	16.8	16.4

Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Victim demographics

In this report, victims are defined as those who had provided their personal details or passwords and/or suffered a financial loss as a result of a fraudulent invitation. Of the 88 victims who had unwittingly provided personal details or suffered a financial loss as a result of the fraud, 59 (67% of victims) identified themselves as female and 29 (33% of victims) as male. Those respondents who advised that they were victims of a fraudulent invitation identified their gender. Of the total respondents who chose to disclose their gender (n=18, 2% of the 865 participants declined to disclose their gender), 12 percent of the 491 females experienced victimisation due to fraudulent invitations compared with 16.6 percent of 356 males.

Table 9 shows the age of victims, including the percentage of total respondents within that age category who reported being a victim. Of the 88 respondents who were identified as victims in the survey, more than 26 percent were aged 45–54 years. No victims were aged 17 years or younger.

Table 10 presents victims' annual income levels, as well as the percentage of total respondents within that income category who reported victimisation. The most frequent income category among victims was for those who earned between $20,000 and less than $40,000 (22%), closely followed by those earning less than $20,000 (20%).

Table 11 shows victims by the region in which they lived, as well as the percentage of total respondents within that region who reported victimisation. Most of those who identified as victims lived in New South Wales (n=27, 31% of the sample who reported victimisation), Queensland (n=19, 22%) and Victoria, where respondents living there also accounted for the same proportion of victims as Queensland (n=19, 22%). No respondents living in New Zealand or the Northern Territory reported they were victims of a fraudulent invitation in the 12 months prior to completing the survey.

Table 9: Victims by age

Age category (years)	n=88	% of victims	Number of respondents in that age category (n)	Respondents within that age category (%)
17 and under	0	0	12	0
18–24	2	2.27	31	6.45
25–34	9	10.23	98	9.18
35–44	11	12.50	137	8.03
45–54	23	26.14	208	11.06
55–64	18	20.45	191	9.42
65 and over	22	25.00	171	12.87
Respondents who chose not to disclose	3	3.41	17	17.65

Note: Percentages may not total 100 due to rounding
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Table 10: Victims by annual income

Annual income	n=88	% of victims	Number of respondents in that income range (n)	Respondents within that income category (%)
Less than $20,000	18	20.45	116	13.41
$20,000 to <$40,000	19	21.59	118	13.64
$40,000 to <$60,000	7	7.95	102	11.79
$60,000 to <$80,000	16	18.18	101	11.68
Over $80,000	12	13.64	156	18.03
I'd rather not say	16	18.18	272	31.45

Note: Percentages may not total 100 due to rounding
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Table 11: Victims by region			
Annual income	n	% (n=88)	Respondents within that region (%)
Australian Capital Territory	8	9.09	9.60
New South Wales	27	30.68	28.21
New Zealand	0	0	0.69
Northern Territory	0	0	0.92
Queensland	19	21.59	22.89
South Australia	7	7.95	8.44
Tasmania	4	4.55	3.93
Victoria	19	21.59	17.46
Western Australia	3	3.41	6.82
Missing	1	1.14	0.12

Note: Percentages may not total 100 due to rounding
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Reporting fraudulent invitations

Respondents were asked for each fraudulent invitation they had received if they had reported the invitation to anyone. Almost 75 percent of respondents who had received a fraudulent invitation reported it to at least one other person or organisation (n=631, 73.0% of the total sample). They most commonly reported fraudulent invitations to 'friends and/or family' (51.9% of respondents who received a fraudulent invitation)—see Table 12.

Of the 88 respondents who reported falling victim to a fraudulent invitation, 79 (89.8%) reported the invitation to at least one other person. When friends and family were excluded the reporting rate declined to just 31.8 percent (n=28) of the victim respondents who had reported to an external organisation. Table 13 shows those organisations or persons that victims reported to, with respondents permitted to select more than one option. Aside from family and friends, victims were most likely to report frauds to the business represented in the fraudulent invitation, for example a bank or online shopping business. Twenty victims of fraudulent invitations reported the incident to a person not provided in the survey. These ranged from 'ombudsman' and Crime Stoppers to government departments and the Do Not Call register set up by the Australian government.

Respondents were asked if they had reported fraudulent invitations they had received to a formal agency, and their reasons for doing so. Participants could select more than one reason for reporting a fraudulent invitation. Results are reported in Table 14 below. The most common reasons for reporting a fraudulent invitation included 'wanting to prevent others from being scammed' (34% of the sample who received an invitation) and 'knew it was the right thing to do' (22% of the sample who received an invitation). Respondents were given the option to provide their own reasons for reporting the fraudulent invitation. These varied from being angry at the attempted fraud and being sick of receiving those types of invitations, to wanting to find out what had happened to personal information and data.

Table 12: Reporting of fraudulent invitations by agency			
Organisation or person reported to	n	Received an invitation (%) (n=844)	Total sample (%) (n=865)
Not reported to anyone	234	27.7	27.1
Family/friends	438	51.9	50.6
Police	70	8.3	8.1
SCAMwatch website (www.scamwatch.gov.au)	147	17.4	17.0
Australian Competition and Consumer Commission	48	5.7	5.6
The business represented (eg bank, eBay etc)	171	20.3	19.8
Internet service provider	56	6.6	6.5
Legal aid, a lawyer, or a community legal services clinic	5	0.6	0.6
Unable to recall	14	1.7	1.6
Other	126	14.9	14.6

Note: Participants could select more than one option so columns will not total 865
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Table 13: Reporting of victimisation by agency		
Organisation or person reported to	n	Reported victimisation (%) (n=88)
Not reported to anyone	9	10.2
Family/friends	51	58.0
Police	27	30.7
SCAMwatch website (www.scamwatch.gov.au)	27	30.7
Australian Competition and Consumer Commission	12	13.6
The business represented (eg bank, eBay etc)	34	38.6
Internet service provider	8	9.1
Legal aid, a lawyer, or a community legal services clinic	4	4.5
Unable to recall	3	3.4
Other	20	22.7

Note: Participants could select more than one organisation or person to report to
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Table 14: Reasons for reporting fraudulent invitations received			
Reason for reporting invitation	n	Received an invitation (%) (n=844)	Total sample (%) (n=865)
Desired the apprehension of offender(s)	137	16.23	15.8
Wanted to prevent others from being scammed	289	34.24	33.4
Knew it was the right thing to do	188	22.27	21.7
To assist in the investigation of an offence	172	20.38	19.9
To support insurance claim	6	0.71	0.7
Other	60	7.11	6.9

Note: Participants could select more than one option
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Table 15: Reasons for not reporting fraudulent invitations			
Reason for not reporting	n	Received an invitation (%) (n=844)	Total sample (%) (n=865)
Not worth the effort	251	29.74	29.0
Didn't think it was illegal	27	3.20	3.1
Unsure of which agency to contact	318	37.68	36.8
Feared I would get in trouble	4	0.47	0.5
Didn't think anything would be done	279	33.06	32.3
Receive too many to report	233	27.61	26.9
Other	137	16.23	15.8

Note: Participants could select more than one option
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Reasons for not reporting fraudulent invitations are outlined in Table 15. The most commonly provided reasons included 'unsure of which agency to contact' (38% of the sample who had received an invitation) and 'didn't think anything would be done' (33%). It should be noted that respondents may have reported some fraudulent invitations that they received, but not all, and they may have had more than one reason for not reporting the invitation. Another reason that may impact the reporting of fraudulent invitations is that most computers have anti-spam ware in email software, which could mean that people were unaware that they had actually received fraudulent invitations, as they were automatically blocked by computer security software.

Respondents were also provided with the opportunity to supply their own reasons for not reporting any fraudulent invitations they had received. As with past ACFT surveys, a common

reason was the assumption that the fraud was well-known. Other responses included 'I had no information to provide authorities with' while others believed 'I have the knowledge to avoid most scams'. Some respondents believed that by completing the survey they had indeed reported the invitation. This was demonstrated by the response, 'I am reporting to you'.

The survey asked whether respondents had reported fraudulent invitations on behalf of anyone else. Fifty respondents (5.8%) indicated that they had, see Table 16 below. Participants were allowed to select all options that applied to them. Some examples included in the 'other' were 'spouse' and on behalf of the business or work that was being used in the fraud.

Table 16: Fraudulent invitations reported on behalf of someone else

Invitation reported on behalf of	n	Total sample (%) (n=865)
Child (son or daughter)	4	0.5
Older relative (brother/sister, parent, grandparent, aunt/uncle)	35	3.9
Younger relative (niece/nephew, brother/sister)	2	0.2
A friend	6	0.7
A colleague	7	0.8
A student (if you are a teacher or in a similar capacity)	2	0.2
Other	9	1.0

Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Perceptions of fraudulent invitations

Respondents were asked how they perceived each fraudulent invitation—whether they considered each invitation as a *crime*; *wrong, but not a crime*; or *just something that happens*. They also had the option of indicating *I don't know* if unsure of the response. The results are outlined in Table 17. Some respondents chose not to respond to the question, and are categorised as '*missing'.*

Advance fee fraud was the type of fraudulent invitation most likely to be considered a crime by respondents (84% of the sample), followed by fraudulent invitations via phishing (82%). While more respondents saw those types of invitations as crimes, the types less likely to be viewed as crimes and perhaps just something that happens were unsolicited invitations for financial advice. Only 48 percent of respondents considered those types of invitations a crime. Thirty percent of respondents considered dating or social networking fraudulent invitations to be wrong, but not a crime. Fraudulent invitations that could not be classified elsewhere caused the most confusion among respondents, with 24 percent not being able to decide if they were a crime, wrong but not a crime, or just something that happens (see Table 17).

The survey also explored the perception of fraudulent invitations by respondents who reported victimisation via those particular frauds. Eighteen respondents reported being a victim of multiple frauds. Accordingly, the number of victims in Table 18 does not total the 88 respondents identified as victims. One victim of a boiler-room fraud considered the invitation to be a crime. As with Table 18, respondents who were victims of advance fee fraud were most likely to consider those types of fraudulent invitations a crime. No victims of a fraudulent invitation considered the frauds as just something that happens, although a few respondents did not know how to classify the invitations.

Table 17: Perceptions of fraudulent invitations

	A crime		Wrong, but not a crime		Just something that happens		I don't know		Missing	
Invitation type	n	%	n	%	n	%	n	%	n	%
Lottery	564	65.2	179	20.7	52	6.0	28	3.2	40	4.9
Advance fee	725	83.8	63	7.3	24	2.8	15	1.7	38	4.4
Inheritance	610	70.5	152	17.6	36	4.2	25	2.9	42	4.9
Phishing	711	82.2	76	8.8	19	2.2	16	1.9	43	5.0
Financial advice	419	48.4	272	31.5	88	10.2	40	4.6	46	5.3
Boiler-room	542	62.7	172	19.9	52	6.0	48	5.6	51	5.9
Work from home	589	68.1	144	16.7	54	6.2	50	3.7	46	5.3
Computer support	656	75.8	121	14.0	25	2.9	27	3.1	36	4.2
Dating or social networking	449	51.9	262	30.3	51	5.9	50	5.8	53	6.1
Other	330	38.2	68	7.9	31	3.6	205	23.7	231	26.7

Note: Percentages may not total 100 due to rounding
Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Table 18: Perceptions of fraudulent invitations by respondents who reported victimisation by a particular fraud

Invitation type	A crime		Wrong but not a crime		Just something that happens		I don't know	
(number of victims)	n	%	n	%	n	%	n	%
Lottery (12)	7	58.3	3	25.0	0	0	2	16.6
Advance fee (8)	7	87.5	0	0	0	0	1	14.3
Inheritance (0)	0	0	0	0	0	0	0	0
Phishing (20)	16	80.0	2	10.0	0	0	2	10.00
Financial advice (5)	3	60.0	1	20.0	0	0	1	20.0
Boiler-room (1)	1	100.0	0	0	0	0	0	0
Work from home (3)	2	66.7	0	0	0	0	1	33.3
Computer support (18)	12	66.7	6	33.3	0	0	0	0
Dating or social networking (14)	10	71.4	3	21.4	0	0	1	7.1
Other (32)	19	59.4	2	6.3	0	0	11	34.5

Note: 18 victims of a fraud were victims of multiple consumer frauds, therefore the number of victims for each fraud type totals more than the 88 victims identified

Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Specific fraudulent invitations

As previously noted, 844 respondents received at least one fraudulent invitation in the 12 months before completing the survey. Of those, 102 received only one invitation, leaving 742 respondents who had received multiple invitations. Of the 102 respondents who received just one invitation, four respondents sent personal details in response to that invitation and another four sent money to the scammer. Five respondents sent both money and personal details or passwords in response to a single fraudulent invitation. As with the previous report, the most common fraudulent invitations received by respondents were those relating to fraudulent computer support schemes. This was also the case for respondents who received a single fraudulent invitation. The next most frequently received fraudulent invitation for respondents who only received one invitation was under the 'other' category.

Fraudulent computer support centre invitations resulted in the most people seeking further information from fraudsters, with 40 respondents who received that particular invitation (n=545) requesting further information. In the 2014 survey no respondents identified as victims of a fraudulent inheritance invitation, however seven respondents did request further information. As with the previous year's report, the 'other' fraudulent invitation category,

comprising a range of diverse fraud types, also had a number of respondents who requested further information about the invitation. Fifteen percent of respondents who received that type of fraudulent invitation requested further information from the fraudster (n=43).

The highest number of victims who sent personal details or passwords had responded to fraudulent invitations or emails that used phishing tactics. A total of 473 respondents received that type of invitation and six percent (n=17) advised that they had disclosed their personal details and/or passwords as a result.

The fraudulent invitation with the highest conversion rate—that is, number of victims per fraudulent invitation sent—was dating and social networking fraud. Eleven percent of respondents who received an invitation of that nature (n=131) disclosed they were victims of a fraudulent invitation. Twelve respondents provided details of the amount of money they sent to fraudsters. The total amount of money reportedly lost to dating and/or social networking fraud in 2014 was $104,100 and the median amount sent by victims was $4,500. The amounts sent as a result of a dating or social networking fraudulent invitation ranged from $500 to $35,000. In the 2014 survey, losses due to dating and social networking invitations alone comprised 45 percent of the total losses reported in the survey. No respondents aged 24 years or younger were victims of a dating and/or social networking fraud, nor aged 35–44 years.

After dating and social network fraudulent invitations, those involving financial advice caused the next highest losses for respondents. Three respondents suffered a financial loss and/or lost personal details (one sent money only and two sent money and personal details). Those respondents reported a total loss of $57,565. The range of financial loss experienced ranged from $165 up to $38,000 (experienced by one victim of a financial advice fraud). It should be noted that the 'other' fraudulent invitation type (comprising less prevalent fraudulent invitations) had 14 respondents, the largest number of any fraud type, with a combined financial loss of $20,472. Examples included 'false advertising scam', 'fraudulent online sales', and 'prize on website'. A few respondents advised they had lost money by paying shipping fees for goods that never arrived.

Reporting habits by specific fraudulent invitation

Table 19 shows the reporting habits of victims of specific fraudulent invitations. The only type of invitation not resulting in victimisation was that relating to false inheritance claims. All other fraud types resulted in some degree of victimisation for respondents. Excluding inheritance frauds, there were three types of frauds where all victims of those frauds reported their victimisation to a person or organisation—advance fee frauds, boiler-room frauds and fraudulent work from home invitations. Victims of fraudulent lotteries or prizes were the least likely to report being the victim of a fraud, with 33 percent (n=4) of all victims of that fraud type not reporting the fraud. Fifty percent (n=4) of victims of advance fee frauds reported the incident to police, the highest percentage of respondents to report their experience to police.

Respondents were given the opportunity to report other places or people to whom they may have reported the fraud victimisation. These varied from government agencies, such as the Department of Foreign Affairs and Trade and the Australian Federal Police, to the post office

and bank fraud squads. Respondents could indicate if they were unable to recall to whom they had reported the victimisation; those responses are not included in Table 19.

Table 19: Reporting habits by victimisation of specific fraudulent invitation type (n)

Invitation type and number of victims of fraud (n=88)	No report	Report to friends and family	Report to police	Report to SCAM-watch	Report to ACCC or regulatory agency	Report to the business used in the invitation	Report to internet service provider	Report to lawyer or Legal Aid	Other
Lottery (n=12)	4	5	4	3	1	4	0	0	1
Advance fee fraud (n=8)	0	3	4	5	2	3	2	0	1
Inheritance (n=0)	0	0	0	0	0	0	0	0	0
Phishing (20)	5	9	5	4	1	9	1	0	3
Financial fraud (5)	1	3	2	2	1	1	0	1	0
Boiler-room fraud (1)	0	0	0	0	0	0	0	0	1
Work from home fraud (3)	0	2	0	0	1	2	2	0	0
Computer support centre (18)	4	9	5	4	1	10	2	0	1
Dating or social networking (14)	3	6	4	4	2	1	0	2	1
Other (32)	4	15	10	10	3	7	1	1	6

Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Loss of personal information or passwords as a result of fraudulent invitations

The theme of the 2015 National Consumer Fraud Week was *Get smarter with your data*. The week was designed to raise awareness of consumer fraud and the need for individuals to protect themselves, their personal details and their passwords against fraudulent invitations. This section discusses participants in the 2014 survey who had been exposed to, or had been victimised as a result of, fraudulent invitations. It focuses on phishing, or frauds where victims lost personal information and/or details. As fraudulent invitations involving phishing tactics were a specific category in the 2014 survey, some details have already been discussed. However, this section aims to explore in greater detail the loss of personal information, passwords and details as a result of a fraudulent invitation, looking not just at phishing invitations but other forms of invitations.

Use of phishing invitations

Phishing involves the use of deceptive websites that have been copied from real websites in order to trick victims into supplying personal or account information (Smith 2011). Misuse of personal information and/or passwords can lead to a range of criminal activity, including various forms of identity crime (ACCC 2014). Credit card or bank card fraud is another type of identity-related crime, and skimming is one method of gaining card details from the magnetic strips located on the back of credit cards and bank cards (Smith 2011). Smith and Hutchings (2014) found that the most successful way to dishonestly obtain personal information is through fraudulent invitations or phishing. With the rise of online transactions and the importance of identity-related information in commerce, identity is now a legal concept as well as a commodity (UNODC 2011). The ACCC (2014) noted in its 2013 *Targeting scams* report that phishing, while the most common method of obtaining personal information and passwords, was just one approach used by fraudsters. Other methods may include using malicious software or spying using social networking forums.

A total of 473 participants had received a fraudulent invitation with phishing characteristics in the 12 months before completing the survey. The most frequent method was via email (see Table 20). Some 207 had received phishing invitations through more than one mode of delivery.

Email was the most popular way to deliver fraudulent phishing invitations, with 81 percent of respondents who received such an invitation receiving at least one this way. It should be noted that respondents may have received multiple phishing invitations via a variety of delivery methods. However, as noted previously, the telephone is growing in popularity as a delivery method of fraudulent invitations.

All Australian jurisdictions and New Zealand participants reported receiving phishing invitations. Forty-one survey participants responded that they had sent personal details or passwords as a result of a fraudulent invitation and 20 participants advised that they were victims of phishing invitations. The highest number of victims of a phishing invitation lived in Victoria (10%), with none living in Western Australia, Tasmania, the Northern Territory or New Zealand. One participant did not disclose their location.

Of the 473 respondents who had received a phishing invitation in the 12 months prior to completing the survey, those aged 17 years and under (n=3, 0.6%) and those aged 18–24 years (n=19, 4.0%) received the least invitations of all the age categories. Those aged 17 years and under were the least likely to receive a phishing invitation with only 25 percent (n=3) of respondents within that age category receiving an invitation of that nature. Respondents aged 45–54 years received the most phishing invitations—26.6 percent (n=126) of all phishing invitations. Of those who received a phishing invitation, six chose not to disclose their age.

Table 20: Mode of delivery of phishing invitations and the number of times they were received (n)

	1–5 times	6–10 times	11–20 times	21–50 times	More than 50 times
Mail	15	3	3	4	3
Email	181	73	47	42	41
Telephone	83	25	17	8	3
SMS	44	7	2	1	0
Internet	26	11	4	2	4

Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Table 21: Locations where phishing invitations were received and loss of personal details (n)

State/territory or New Zealand	Received phishing invitation	Sent personal details or passwords to an invitation (any invitation)	Sent both personal details and money to any invitation	Victim of a phishing invitation
New South Wales	122	11	11	5
Victoria	84	10	4	8
Queensland	123	8	6	2
Western Australia	30	1	1	0
South Australia	38	4	0	2
Tasmania	15	3	0	0
Australia Capital Territory	48	4	1	2
Northern Territory	4	0	0	0
New Zealand	3	0	0	0

Source: ACFT Consumer Fraud Survey 2014 [AIC data file]

Loss of personal information through phishing frauds and other fraudulent invitations

A victim for the purposes of the 2014 survey was defined as someone who had sent money or personal details, or both money and personal details, to a fraudster as a result of a fraudulent invitation.

Forty-one participants (5% of the total sample and 47% of those identified as victims) reported in the survey that they had sent personal information or passwords as a result of a fraudulent invitation (both phishing and other types of invitations). Twenty-four participants (3% of the total sample, 27% of all victims in the survey) had sent both money and personal details in response to a fraudulent invitation. Twenty-five respondents requested further information from the fraudster.

Some of the examples supplied by respondents in the 'other' category provided further clarification about how they came to lose both personal details and money. One respondent explained how selling items online led to the loss of bank account information and other personal details. In another example the respondent explained how a false computer support centre representative was able to remotely access their personal computer and gain access to information and photos stored on the computer.

Losses

Twenty-eight of the 41 participants who had sent both money and personal details in response to a fraudulent invitation indicated that more than $150,000 had been lost to fraudsters. The money sent by respondents, along with personal information, ranged from a minimum of

$74.99 to a maximum of $38,000. Two victims of phishing frauds also sent money as well as personal details following a fraudulent invitation. Those amounts were $165 and $900.

Victim demographics

Of the 20 victims of a fraudulent phishing invitation, five were males (25%) and 15 were females (75%). The highest number of female victims were aged over 45 years (75% of females who identified as phishing victims). The largest percentage of males was aged over 55 years (80%). No victims of fraudulent phishing invitations were aged 17 years or younger.

Responding to victimisation

Participants were asked if they had reported the fraud to anyone. They could nominate family and friends, the police, SCAMwatch, the Australian Competition and Consumer Commission or another regulatory agency, the business represented in the fraud, an internet service provider or a lawyer or Legal Aid representative. In the 2014 survey, seven of the 20 victims of a phishing fraud reported their experiences to another person or organisation. Respondents were able to indicate if they had reported the victimisation to more than one person or organisation. When asked why respondents reported the phishing frauds, the main reason they selected was they 'wanted to prevent others being scammed' (n=10).

Conclusion and policy implications

Findings and discussion

As in previous years, a large proportion of survey respondents received consumer fraud invitations, with 98 percent receiving one in the 12 months prior to the survey. The most commonly received fraudulent invitations were those that used dishonest computer support centres, involved false winnings in lottery or prizes, or claimed to be from a legitimate business or organisation trying to obtain personal information (phishing fraud). These three fraudulent invitations were also the most common frauds experienced in the 2013 survey, although in that year invitations involving fraudulent prizes or lottery winnings were the most common.

Twenty-five percent of respondents disclosed that they had responded to a fraudulent invitation in the 12 months leading up to the survey. Responding could involve sending money or personal details (or both), or seeking further information. Five percent of respondents who had received a fraudulent invitation in the 12 months before completing the survey had sent personal details and/or passwords in response to the invitation and six percent sent money, with three percent disclosing they had sent personal details and experienced a financial loss. Some respondents suffered a financial loss and/or lost personal details to more than one fraudulent invitation. The percentage of people experiencing both a financial loss and losing personal details decreased from the 2013 survey (Jorna 2015).

The 2014 survey results relating how fraudulent invitations were delivered were consistent with findings from previous ACFT surveys (Hutchings & Jorna 2013; Jorna 2015), with email remaining the most common method. However, unsolicited telephone calls as a fraudulent invitation delivery method continued to gain popularity in the 2014 survey with 72 percent of respondents receiving an invitation via landline telephone—almost as high as the 75 percent who received an invitation via email last year. In 2013, the ACCC (ACCC 2014) found that the telephone had once again replaced email as the most common scam delivery method, with 52 percent of their scam-related contacts receiving a fraudulent invitation via telephone.

Since the ACFT started, the median financial loss reported in the surveys had been steadily declining until 2013, when the median reported loss rose to $2,100. In 2014 the median

financial loss decreased to $900, which, aside from 2013, was still higher than other reported losses since 2010. The reason for the decrease between 2013 and 2014 is that fewer respondents identified as victims who suffered a financial loss, and the amounts reportedly lost in the 2014 survey were much lower than those reported in 2013.

Once again, the fraudulent invitation that resulted in the highest losses experienced by victims was not one of the most common invitations received. Fraudulent invitations involving dating and social network frauds were again the most costly, with victims losing more than $104,000 to those frauds alone. The total financial impact of frauds experienced in the 2014 survey was more than $230,700, with dating and social network fraudulent invitations making up 45 percent of those losses. The only fraudulent invitation type that did not result in at least one self-identified victim was the fake inheritance scheme. All other fraudulent invitations resulted in at least one respondent identifying as a victim and suffering either a financial impact, loss of personal information or both.

Reporting fraudulent invitations to authorities has traditionally been low (Hutchings & Lindley 2012, Jorna & Hutchings 2013). However, the percentage of victims who reported the fraud to police increased to 31 percent in the 2014 survey. One reason may be the recent establishment of the Australian Cybercrime Online Reporting Network (ACORN)—a national online system that allows the public to securely report instances of cybercrime, and advises on how to recognise and avoid common types of this crime (ACORN 2015). Substantial media attention to the reporting system prior to ACORN's official launch may have influenced victims' reporting behaviour. That said, the percentage of victims of fraudulent invitations reporting to the ACCC's SCAMwatch was the same as those reporting to police—31 percent. This indicates that SCAMwatch still provides a valuable resource for educating consumer fraud victims on how to avoid fraudulent invitations and where assistance is available.

In the 2014 survey, nine respondents (10% of all victims) were identified as victims who did not report the victimisation to anyone, including friends or family. The most frequently cited reason for not reporting a fraudulent invitation was not knowing which agency to contact. It is hoped that the introduction of ACORN and the continuing success of SCAMwatch will ease this confusion, and that the impact of these important self-reporting services will be seen in future ACFT surveys.

Even if a person is not a victim of a fraudulent invitation they should report the type of invitation and how it was received to SCAMwatch or consumer protection agencies. This is important as it allows agencies to improve their knowledge and understanding of the types of frauds that are affecting the public. Reporting also helps them to develop awareness and education programs to reduce the level of victimisation. It can also guide the allocation of resources to combat or disrupt frauds. Overall, reporting rates of fraudulent invitations are increasing, and when respondents did report an invitation, the most frequent reasons for doing so were to prevent others from becoming a victim of the fraud, and because they knew it was the right thing to do. These top two reasons for reporting a fraudulent invitation were the same as those reported in the 2013 survey and continue to demonstrate that the key requirement to reducing the impact of consumer fraud is education in a variety of different formats.

Phishing invitations

The theme of the 2015 National Consumer Fraud Week was *Get smarter with your data*. The week was designed to raise awareness of consumer fraud and the need to protect individuals against fraudulent invitations, with a focus on protecting personal details and passwords. Phishing is the act of pretending to be a legitimate business or organisation and trying to obtain personal information or account details through emails or websites that may appear legitimate (Hutchings & Hayes 2009). Phishing invitations have been identified (Smith & Hutchings 2014) as one of the most successful means of dishonestly obtaining personal information that may be used to commit further identity crimes.

In the 2014 survey, 41 respondents (47% of those who were characterised as victims) sent personal details or passwords as a result of a fraudulent invitation. Twenty (4% of those who received an invitation of that nature) were victims of a phishing fraud. Two victims suffered a financial loss as a result of a phishing invitation and 17 victims lost personal information or passwords to fraudsters. One respondent suffered both a financial loss and lost personal data. Victims of phishing invitations were aged between 18 and over 65 years, with only those under 17 years not falling victim to fraudulent invitations of that nature. Email was the most common means of delivering phishing invitations.

Suggestions for future campaigns

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

- *how people react to receiving fraudulent invitations*. Developing a greater understanding of how people react to fraudulent invitations—for example, determining if they change their behaviour while using social networking sites of buying and selling products online to avoid the risk of victimisation or whether they choose to ignore potential risks. The 2014 survey found that 220 participants responded in some way to a fraudulent invitation by requesting further information or sending money and/or personal details. Future campaigns could examine why people respond, what would reduce the likelihood of their responding and how their behaviour online changes after recognising a fraud; and
- *educating the public on common themes used in fraudulent invitations*. The 2014 survey identified victims of multiple fraudulent invitations who lost money or personal data to more than one consumer fraud. Greater education on the common themes used in fraudulent invitations would be valuable in helping the public to recognise a fraud, and particularly useful in reducing the number of victims of multiple consumer frauds.

References

Australian Bureau of Statistics 2012. *Personal fraud 2010–11*. ABS cat. no. 4528.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/latestProducts/4528.0Media%20Release12010-2011

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

Australian Cybercrime Online Reporting Network (ACORN) 2015. Website. http://www.acorn.gov.au/

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: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tbp/41-60/tbp043.aspx

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: Australian Institute of Criminology. http://aic.gov.au/publications/current%20series/tbp/41-60/tbp050.html

Jorna P 2015. Australasian Consumer Fraud Taskforce: Results of the 2013 online consumer fraud survey. *Technical and background paper series no. 58*. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tbp/41-60/tbp058.html

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

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

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

Smith RG 2011. International identity crime, in Smith CJ, Zhang SX & Barberet R (eds), *Routledge handbook of criminology: An international perspective*. New York: Taylor & Francis: 142–52

Smith RG & Hutchings A 2014. Identity crime and misuse in Australia: Results of the 2013 online survey. *Research and public policy series no. 128*. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/121-140/rpp128.html

United Nations Office on Drugs and Crime 2011. Handbook on identity-related crime. Vienna: United Nations http://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf

Appendix 1

Australasian Consumer Fraud Taskforce Online Survey 2014

The Australasian Consumer Fraud Taskforce (ACFT) was formed in March 2005 and comprises 22 government regulatory agencies and departments. The ACFT also has a range of community, non-government and private sector organisations as partners in the effort to increase the level of scam awareness in the community. Further information about the ACFT can be found at www.scamwatch.gov.au

As part of an annual awareness campaign, the ACFT invites consumers to participate in this online survey to improve the prevention, detection and investigation of scam activities. The survey should take only 10 minutes to complete and all participants will remain anonymous. You will not be asked any questions designed to identify you and all information provided will be treated as confidential. If at any stage you choose not to continue with the survey you can close the survey and your responses will not be saved or recorded.

If you would like to assist us by completing the survey, please click on the 'next' arrow below.

You may print out your completed responses by clicking on the printer icon located at the top of the screen on each page.

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'.

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

   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	Not applicable
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 ($):

_____

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
- ☐ Not applicable

Thinking about the most recent time you responded to a scam invitation, how many times were you in contact with the person(s) before you sent 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
- ☐ Not applicable

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, website etc)
- ☐ Internet Service Provider
- ☐ Legal aid, a lawyer, or a community legal services clinic
- ☐ Unable to recall

☐ Other
Please specify

_____

What was the outcome of reporting either the scam invitation or scam victimisation?

☐ Not applicable, reported to family/friends
☐ Outcome
Please specify

_____

If you did report the scam invitation, how satisfied were you with the outcome of your experience of reporting?

☐ Extremely satisfied
☐ Satisfied
☐ Neither satisfied nor dissatisfied
☐ Dissatisfied
☐ Extremely dissatisfied
☐ Not applicable

2. *Money transfer scams - Requests for assistance to transfer large sums of money out of another country 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.*

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	Not applicable
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 ($):

_____

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

Thinking about the most recent time you responded to a scam invitation, how many times were you in contact with the person(s) before you sent 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
- ☐ Not applicable

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, website etc)
- ☐ Internet Service Provider
- ☐ Legal aid, a lawyer, or a community legal services clinic
- ☐ Unable to recall
- ☐ Other

Please specify

_____

What was the outcome of reporting either the scam invitation or scam victimisation?

- ☐ Not applicable, reported to family/friends
- ☐ Outcome

Please specify

_____

If you did report the scam invitation, how satisfied were you with the outcome of your experience of reporting?

- ☐ Extremely satisfied
- ☐ Satisfied
- ☐ Neither satisfied nor dissatisfied
- ☐ Dissatisfied
- ☐ Extremely dissatisfied
- ☐ Not applicable

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.*

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	Not applicable
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 ($):

_____

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

Thinking about the most recent time you responded to a scam invitation, how many times were you in contact with the person(s) before you sent 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
- ☐ Not applicable

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, website etc)
- ☐ Internet Service Provider
- ☐ Legal aid, a lawyer, or a community legal services clinic
- ☐ Unable to recall
- ☐ Other

Please specify

_____

What was the outcome of reporting either the scam invitation or scam victimisation?

- ☐ Not applicable, reported to family/friends
- ☐ Outcome

Please specify

_____

If you did report the scam invitation, how satisfied were you with the outcome of your experience of reporting?

- ☐ Extremely satisfied
- ☐ Satisfied
- ☐ Neither satisfied nor dissatisfied
- ☐ Dissatisfied
- ☐ Extremely dissatisfied
- ☐ Not applicable

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.*

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	Not applicable
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 ($):

_____

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

Thinking about the most recent time you responded to a scam invitation, how many times were you in contact with the person(s) before you sent 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
- ☐ Not applicable

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, website etc)
- ☐ Internet Service Provider
- ☐ Legal aid, a lawyer, or a community legal services clinic
- ☐ Unable to recall
- ☐ Other

Please specify

_____

What was the outcome of reporting either the scam invitation or scam victimisation?

- ☐ Not applicable, reported to family/friends
- ☐ Outcome

Please specify

_____

If you did report the scam invitation, how satisfied were you with the outcome of your experience of reporting?

- ☐ Extremely satisfied
- ☐ Satisfied
- ☐ Neither satisfied nor dissatisfied
- ☐ Dissatisfied
- ☐ Extremely dissatisfied
- ☐ Not applicable

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.*

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	Not applicable
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 illegitimate financial advice from a person you don't know?

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 ($):

_____

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

Thinking about the most recent time you responded to a scam invitation, how many times were you in contact with the person(s) before you sent 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
- ☐ Not applicable

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, website etc)
- ☐ Internet Service Provider
- ☐ Legal aid, a lawyer, or a community legal services clinic
- ☐ Unable to recall
- ☐ Other

Please specify

_____

What was the outcome of reporting either the scam invitation or scam victimisation?

- ☐ Not applicable, reported to family/friends
- ☐ Outcome

Please specify

_____

If you did report the scam invitation, how satisfied were you with the outcome of your experience of reporting?

- ☐ Extremely satisfied
- ☐ Satisfied
- ☐ Neither satisfied nor dissatisfied
- ☐ Dissatisfied
- ☐ Extremely dissatisfied
- ☐ Not applicable

6. *Boiler-room scams (investment scams) - 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.*

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	Not applicable
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 ($):

_____

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

Thinking about the most recent time you responded to a scam invitation, how many times were you in contact with the person(s) before you sent 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
- ☐ Not applicable

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, website etc)
- ☐ Internet Service Provider
- ☐ Legal aid, a lawyer, or a community legal services clinic
- ☐ Unable to recall

☐ Other
Please specify

_____

What was the outcome of reporting either the scam invitation or scam victimisation?

☐ Not applicable, reported to family/friends
☐ Outcome
Please specify

_____

If you did report the scam invitation, how satisfied were you with the outcome of your experience of reporting?

☐ Extremely satisfied
☐ Satisfied
☐ Neither satisfied nor dissatisfied
☐ Dissatisfied
☐ Extremely dissatisfied
☐ Not applicable

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.*

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?

☐ 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	Not applicable
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 ($):

_____

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

Thinking about the most recent time you responded to a scam invitation, how many times were you in contact with the person(s) before you sent 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

☐ Not applicable

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, website etc)
☐ Internet Service Provider
☐ Legal aid, a lawyer, or a community legal services clinic
☐ Unable to recall
☐ Other

Please specify

_____

What was the outcome of reporting either the scam invitation or scam victimisation?

☐ Not applicable, reported to family/friends
☐ Outcome

Please specify

_____

If you did report the scam invitation, how satisfied were you with the outcome of your experience of reporting?

☐ Extremely satisfied
☐ Satisfied
☐ Neither satisfied nor dissatisfied
☐ Dissatisfied
☐ Extremely dissatisfied
☐ Not applicable

8. *Computer support centre scam - Computer support centre scams occur when recipients receive, mainly telephone calls, from scammers claiming they are from well known computer manufactures 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.*

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	Not applicable
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 ($):

_____

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

Thinking about the most recent time you responded to a scam invitation, how many times were you in contact with the person(s) before you sent 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
- ☐ Not applicable

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, website etc)
- ☐ Internet Service Provider
- ☐ Legal aid, a lawyer, or a community legal services clinic
- ☐ Unable to recall
- ☐ Other

Please specify

_____

What was the outcome of reporting either the scam invitation or scam victimisation?

- ☐ Not applicable, reported to family/friends
- ☐ Outcome

Please specify

_____

If you did report the scam invitation, how satisfied were you with the outcome of your experience of reporting?

- ☐ Extremely satisfied
- ☐ Satisfied
- ☐ Neither satisfied nor dissatisfied
- ☐ Dissatisfied
- ☐ Extremely dissatisfied

☐ Not applicable

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.*

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	Not applicable
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 of 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 ($):

_____

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

Thinking about the most recent time you responded to a scam invitation, how many times were you in contact with the person(s) before you sent 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
- ☐ Not applicable

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, website etc)
- ☐ Internet Service Provider
- ☐ Legal aid, a lawyer, or a community legal services clinic
- ☐ Unable to recall

☐ Other
Please specify

_____

What was the outcome of reporting either the scam invitation or scam victimisation?

☐ Not applicable, reported to family/friends
☐ Outcome
Please specify

_____

If you did report the scam invitation, how satisfied were you with the outcome of your experience of reporting?

☐ Extremely satisfied
☐ Satisfied
☐ Neither satisfied nor dissatisfied
☐ Dissatisfied
☐ Extremely dissatisfied
☐ Not applicable

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

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	Not applicable
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 ($):

_____

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

Thinking about the most recent time you responded to a scam invitation, how many times were you in contact with the person(s) before you sent 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
- ☐ Not applicable

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, website etc)
- ☐ Internet Service Provider
- ☐ Legal aid, a lawyer, or a community legal services clinic
- ☐ Unable to recall
- ☐ Other

Please specify

_____

What was the outcome of reporting either the scam invitation or scam victimisation?

- ☐ Not applicable, reported to family/friends
- ☐ Outcome

Please specify

_____

If you did report the scam invitation, how satisfied were you with the outcome of your experience of reporting?

- ☐ Extremely satisfied
- ☐ Satisfied
- ☐ Neither satisfied nor dissatisfied
- ☐ Dissatisfied
- ☐ Extremely dissatisfied
- ☐ Not applicable

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)*

- ☐ Not applicable, 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)*

- ☐ Not applicable, I did not receive a scam invitation
- ☐ Not applicable, I did not report any of the scam invitations I received
- ☐ 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 my 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)*

- ☐ Not applicable, 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 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)*

	A crime	Wrong but not a crime	Just something that happens	I don't know
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)	☐	☐	☐	☐
Computer support centre scam	☐	☐	☐	☐
Pursuing a personal relationship that later turned out to be false	☐	☐	☐	☐
Other type of scam (if you received a scam invitation not mentioned above)	☐	☐	☐	☐

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)

- ☐ 2013
- ☐ 2012
- ☐ 2011
- ☐ 2010
- ☐ 2009
- ☐ 2008
- ☐ Never

18. *Are you aware of the 2014 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+
- ☐ I'd rather not say

21. *What is your sex?*

- ☐ Male
- ☐ Female
- ☐ I'd rather not say

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 financial year 2012-2013 (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 Governement member
- ☐ My employer is an Australasian Consumer Fraud Taskforce private sector partner
- ☐ My employer is another government agency

Thank you for completing the 2014 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.

AIC reports

Research report

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

aic.gov.au