Australian Government
Australian Institute of Criminology

Australasian Consumer Fraud Taskforce: Results of the 2012 online consumer fraud survey

Penny Jorna
Alice Hutchings

AIC Reports
Technical and Background Paper 56

Australasian Consumer Fraud Taskforce: Results of the 2012 online consumer fraud survey

Penny Jorna
Alice Hutchings

AIC Reports
Technical and
Background Paper
56

www.aic.gov.au

ISSN 1836-2052
ISBN 978 1 922009 43 2

Project no. 0132

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

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

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

Edited and typeset by the Australian Institute of Criminology

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

Foreword

Each year, since 2007, the Australian Institute of Criminology (AIC) has collected information on consumer scams by conducting an online survey of Australians who have received scam invitations during the preceding 12 months. The research is conducted on behalf of the Australasian Consumer Fraud Taskforce (ACFT), which is comprised of 22 government regulatory agencies and departments in Australia and New Zealand who work alongside private sector, community and non-government partners to prevent fraud of this nature. In order to understand the dynamics of consumer fraud victimisation, the ACFT has conducted a range of fraud prevention and awareness-raising activities over the last eight years. The annual survey seeks to obtain a snapshot of the public's exposure to consumer scams, to assess the range of ways in which scams can affect victims and their families, to determine how victims respond and to identify emerging typologies and issues that could be used to inform fraud prevention initiatives. Survey respondents are not representative of the whole Australian population, as the sample is made up of those individuals who choose to participate, although in 2012, over 1,500 people completed the survey with good levels of representation from all states and territories, and other demographic categories.

This report presents the results of the survey conducted in conjunction with the 2012 campaign, *Slam scams! Press 'delete', throw it out, shut the door or just hang up*. The campaign theme was concerned with scam delivery methods that focused on raising awareness about the many ways in which scammers try to deliver scam invitations. A phone call, SMS, mobile application, house visit, letter, email, fax, blog, online chat or dating service—scammers will use any of these means to target victims. The primary message was simple—stop the contact at the point of delivery; if you don't engage with a scammer in the first place, you can avoid being scammed.

As in previous years, a high proportion of respondents had received a scam invitation (95%), with almost a quarter responding to the scam in some way. Unfortunately, eight percent reported having lost money—approximately $8,000 per person or almost $850,000 in total. The most prevalent scam type involved fraudulent lotteries, while this year, the second-most prevalent scam concerned computer support scams, which are sometimes a means of extracting payments for non-existent services from victims or, on other occasions, a means of installing malicious software that can be used to extract personal information at a later time. In terms of delivery methods, although email continued to be the most common method by which scams were delivered, the use of landline and mobile telephones (including SMS) to target potential scam victims increased.

This report also includes some additional information on online shopping scams—the subject of the consumer fraud awareness week in June 2013. The prevalence of scams targeting those who sell or buy high-value items online, such as motor vehicles, was high in 2012, indicating a need for enhanced awareness of the risks involved in this form of consumer activity.

Adam Tomison
Director

Contents

Figures

Tables

Acknowledgements

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

This paper would not have been possible without those who gave up their time to participate in the online survey. Particular thanks go to those participants who have responded to previous Australasian Consumer Fraud Taskforce surveys.

Acronyms

ACCC	Australian Competition & Consumer Commission
ACFT	Australasian Consumer Fraud Taskforce
AIC	Australian Institute of Criminology
SMS	short message service

Executive summary

Background

The Australasian Consumer Fraud Taskforce (ACFT) comprises 22 government regulatory agencies and departments in Australia and New Zealand that work alongside private sector, community and non-government partners to prevent fraud. The ACFT has conducted a range of fraud prevention and awareness-raising activities since 2006. One key activity of the ACFT is to hold an annual consumer fraud survey to obtain a snapshot of the public's exposure to consumer scams, to assess their impact, to determine how victims respond and to identify emerging typologies and issues. As the survey participants were not randomly sampled, the survey findings are not representative of the general population.

The Australian Institute of Criminology (AIC) is a member of the ACFT and chair of the research sub-group. This report presents the results of the 2012 survey, which ran for three months commencing from 1 January 2012. This period encompassed National Fraud Prevention Week, which coincides with global awareness-raising activities. The theme of the 2012 campaign was *Slam Scams!* This theme aimed to raise awareness about scam delivery methods so that scams could be identified at the point of contact. The survey explored scams where respondents were contacted by phone, short message service (SMS), email, letter, via the internet and/or in person by someone who they did not know in relation to:

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

The survey was made available for completion on the AIC's website. Participants who did not reside in Australia or New Zealand were excluded from the survey, as were invalid responses. In 2012, 1,576 participants completed the survey. Outliers, typically very large loss figures from respondents who appeared to have misunderstood the question, were removed from the analysis.

The 2012 survey suffered from a number of limitations that made it difficult to generalise its findings to the greater Australasian population, in particular the self-selection bias of the survey design. As the sample was not randomly selected, those who participated in the survey may be different from the general population.

Delivery of scams

The 2012 survey asked respondents about the types of scams they had received, as well as how the scam invitations had been delivered to them. Results indicated that:

- Ninety-five percent of respondents reported having received at least one scam invitation in the 12 months preceding the survey.
- The most common type of scams reported to have been received were lottery scams (received by 60% of the total sample), computer support centre scams (53%) and phishing scams (45%).
- The least common type of scams received were dating or romance scams, reported by 13 percent of the total sample.
- Email was the most common scam delivery method, with 72 percent of the sample reporting having received a scam this way.

Responding to scam invitations

Respondents reported that they had responded to scam invitations by requesting further information, providing personal details and/or suffering a financial loss. Key findings included:

- Twenty-two percent of the respondents responded in some way to a scam invitation in the 12 months preceding the survey:
  - seven percent sent their personal details;
  - three percent of respondents reported a financial loss; and
  - five percent reported both sending their personal details and having experienced a financial loss.
- The median amount reported lost to scams was $500. With outliers removed, a total financial loss of $846,170 was reported.
- The top two reasons given for not responding to scam invitations were 'had seen/heard this was a type of scam in the media or from a public source' (55% of the total sample of 1,576) and 'had received similar offers before and thought they were scams' (55%).

Victim demographics

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

- Of those survey respondents who identified their gender (98%), 16.5 percent of females and 12.4 percent of males reported victimisation in 2012.
- In 2012, respondents in the age categories who reported the highest percentage of victimisation were '35 to 44 years' and 'over 65 years' (16.5% of total respondents within those age categories).
- In 2012, respondents in the income category who reported the highest percentage of victimisation earned $20,000 to less than $40,000 (20% of total respondents within that income category).

Reporting scams

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

- In 2012, 69 percent of the total sample reported a scam to at least one person or organisation.
- Family and friends were the most common recipients of scam complaints, with 43 percent of the total sample reporting to this category in 2012.
- The most common reasons provided for not reporting scams were 'unsure of which agency to contact' (40% of the total sample), 'I didn't think anything would be done' (32%) and 'not worth the effort' (29%).
- The most common reasons for reporting scams were 'wanted to prevent others from being scammed' (39% of the total sample), 'knew it was the right thing to do' (28%) and 'to assist in the investigation of an offence' (26%).

Perceptions of scams

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

- In 2012, the top three scam types to be considered to be a crime by respondents were advance fee fraud (81%), phishing (81%) and computer support scams (79%).

Recommendations for future campaigns

The 2012 findings were used to develop recommendations for future education and awareness campaigns. It was suggested that future campaigns should focus on:

- highlighting the use of new technologies, yet keeping people aware that scammers are adaptive and will find new ways to use older technology, such as the Computer Support Centre scams of 2011 and 2012;
- awareness campaigns to educate members of the public around victimisation, in particular to encourage a change in societal attitudes towards victims of scams and online frauds; and
- continuing to raise awareness of the importance of personal information in an age of identity crime and online transactions.

Introduction

The purpose of this paper is to report the findings from the ACFT 2012 survey in order to provide an overall picture of the nature of consumer fraud in Australasia.

Australasian Consumer Fraud Taskforce

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

The 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, and Hutchings and Lindley (2012) for the 2010 and 2011 survey results. The survey reported in this paper ran for three months between January and March 2012, which included the annual Fraud Week conducted by the Taskforce.

Defining scams

According to the Australian Bureau of Statistics, scams are defined as '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 2008: 5).

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. There are a range of consumer fraud activities that may be

classified as scams. Eight common types of consumer frauds were explored in the 2012 ACFT survey, namely advance fee fraud, dating scams, financial advice scams, inheritance scams, lottery scams, phishing, work from home scams and computer support scams. Definitions for these scam types are provided in Table 1. Consumer scams target individuals and consumers, rather than businesses or governments (Budd & Anderson 2011).

Table 1 Common scams and their definitions

Advance fee fraud/Nigerian 419 scams	Advance fee frauds or Nigerian 419 scams have existed throughout history and have adapted to advances in technology. Generally, these scams are communicated by email or letter and seek assistance to transfer a large amount of money overseas. These are the most commonly complained about scams in Australia according to the ACCC
Dating/social networking scams	Dating and social networking scams may 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, scammers may hook victims by claiming to have an unwell relative or severe financial trouble and seek assistance. Due to the trust already established, victims may be more easily duped and in disbelief when scammers no longer remain in communication after money has been sent
Financial advice scams	Financial advice scams involve cold calls by scammers operating from overseas who offer 'advice' on shares, mortgage or real estate 'investments', 'high-return' schemes, option trading or foreign currency trading. The advice generally does not involve a legitimate investment nor lead to increased wealth
Inheritance scams	Inheritance scams 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 potential victim a large inheritance
Lottery scams	A lottery scam may be delivered by email, text message or pop-up screen falsely claiming you have 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 scams (money laundering)	Work from home scams are often promoted through spam emails or advertisements on noticeboards, however, are generally not advertising real jobs. Work from home scams are generally fronts for illegal money-laundering activities or pyramid schemes
Computer support centre scams	Computer support centre scams occur when recipients receive mainly telephone calls from scammers claiming they are from well-known computer manufacturers or businesses that can fix problems with the recipients' computers. Scammers may ask for money, personal details or passwords or seek to sell worthless products to fix computers

Source: ACCC 2012a, 2011; AIC ACFT Survey 2012

Method

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

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

Each year, between 1 January and 31 March, an anonymous online survey hosted by the AIC has been used to collect data. This timeframe was chosen to correspond with the ACFT fraud awareness campaign of each year (which ran from 19 to 25 March in 2012), as well as to collect data before and after the campaign period to assess the impact of the campaign on participation rates.

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

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

Survey questions

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

- lottery scams;
- advance fee fraud;
- inheritance scams;
- phishing;
- financial advice scams;
- work from home scams;
- dating scams; and
- computer support scams.

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

There were two substantial changes to the 2012 survey compared with previous years. The first change was the inclusion of computer support scams as a scam category. The second change was an additional question that requested a postcode for respondents who indicated that they resided in Australia.

Media coverage

A search of media databases for the periods 1 January 2012 to 31 March 2012 found nine newspaper articles inviting readers to participate in the survey. These were:

- The Canberra Times 2012. Dob in a scammer. *The Canberra Times* 20 January.
- The Manning River Times 2012. Scam survey. *The Manning River Times* 1 February.
- Chamberlain S 2012. Scams under the spotlight. *Daily Liberal and Macquarie Advocate* 2 February.
- Dubbo Daily Liberal 2012. Government declares war on weeds. *Dubbo Daily Liberal* 2 February.
- McCarthy J 2012. Too good to be true. *Newcastle Herald* 4 February.
- Canterbury Bankstown Express 2012. Near you news from your suburb. *Canterbury Bankstown Express* 7 February.
- Macarthur Chronicle 2012. Help turn tables on fraudsters. *Macarthur Chronicle* 7 February.
- The Express 2012. Help lift lid on scammers. *The Express* 7 February.
- Pryor P 2012. How to beat the web of deceit. *The Sun-Herald* 26 February.

Radio interviews conducted with AIC staff in 2012 also promoted the survey and sought respondents. These included an interview with Graeme Stewart on ABC Radio North New South Wales on 24 January 2012 and interviews with Leon Delaney on Radio 2SM Sydney, Jorian Gardner on Radio 2CC Canberra and Red Symons on ABC Radio Melbourne, all on 17 January 2012.

Additional media reports during the week-long campaigns that did not mention the survey may have nevertheless generated visits to the websites where links to the survey were provided. A search of media databases identified 41 additional newspaper articles that discussed consumer fraud published between 19 to 25 March 2012 (refer to *Appendix 2*).

Limitations of the survey

The 2012 AIC survey experienced the same methodological constraints as those identified in previous years (see Budd & Anderson, 2010; Hutchings & Lindley 2012; Smith & Akman, 2008). Limitations associated with the relatively small sample sizes and the self-selection bias of the samples make generalising the findings to the wider population problematic, particularly as those who have received a scam invitation and/or fallen victim may be more likely to complete the survey than those who have not. Directly completing the survey was also limited to those who had computer access, however, this was not considered overly restrictive, as SCAMwatch employees were able to fill out survey over the phone on the client's behalf.

It can be difficult to measure fraud incidents within a given timeframe as it is not always easy to determine when fraud occurs due to the time lapse between when they are received or carried out, identified by the victim and then reported (if indeed they are). The reference period for the 2012 AIC online survey was the previous 12 months and respondents were asked about whether they had received and responded to scams in this time. It is possible that some incidents may have begun before this time period and these may have been missed by the survey questions. As a result, the survey results cannot provide a robust measurement of consumer fraud victimisation rates in Australasia, nor of the success of the 2012 Fraud Awareness week. The results are also unable to identify whether the campaign increased people's awareness of consumer frauds or scams.

Despite these limitations, the annual survey is a valuable tool to inform policymakers and the public about what is happening in the scam threat landscape. The report provides context to scam invitations that do not result in the loss of personal information or a direct financial loss, as well as outlining actual victimisation. The results of the survey are another way that people can be educated about the types of scams that they may face and the survey collects information about how scams are perceived by the public.

Analysis of results

Due to the limitations of the data as outlined above, descriptive statistics were predominantly used to report the results, particularly frequency distributions and percentages. As the survey was designed to capture information relating to respondents residing in Australia or New Zealand, respondents who indicated they resided elsewhere were excluded from the sample. Outliers, typically very large loss figures from respondents who appeared to have misunderstood the question, were removed for the analysis. In the following sections, the key results from the 2012 ACFT survey are presented.

The 2012 consumer fraud survey results

Sample characteristics

Between 1 January and 31 March 2012, 1,593 people responded to the survey hosted on the AIC's website (www.aic.gov.au). Seventeen respondents were removed as they did not reside in Australia or New Zealand, leaving 1,576 responses who formed the sample subject to analysis.

Seventy-six percent of respondents (n=1,205) reported that they completed the survey in their capacity as a member of the public. A further 15 percent (n=242) of respondents identified themselves as retirees. Fourteen respondents (0.9%) were members of the police, 21 (1.3%) were employed by an ACFT government agency, two respondents (0.1%) were employed by an ACFT private sector partner and 68 (4.3%) were employed by another government agency.

Websites were the most popular way respondents were directed to the survey, with government websites referring 526 respondents (33.4%) and the SCAMwatch site referring another 400 respondents (25.4%). The media generated 183 responses (11.6%), posters and pamphlets directed three respondents (0.2%) and 98 respondents (6.2%) were referred to the survey by another agency. A further 109 respondents (6.9%) found out about the survey through word of mouth.

Sixteen percent (n=253) were aware of the ACFT's campaign and 14 percent (n=225) were aware of campaigns that had been run in previous years. Thirty-five respondents (2.2%) had completed the 2011 survey, 19 respondents (1.2%) had completed the 2010 survey, nine (0.6%) had completed the 2009 survey, eight (0.5%) had completed the 2008 survey and seven respondents (0.4%) had previously completed the 2007 survey.

There was an average of 121 responses a week in the 11 weeks prior to the 2012 campaign (n=1,328); 187 participants completed the survey during the week-long campaign, while the remaining 61 participants completed the survey in the week following the campaign.

Respondents were asked why they chose to complete the survey. Most respondents (n=1,168, 74.1%) wanted to 'assist in research to combat scammers'. A further 631 participants (40.0%) completed the survey because 'they had received scams, but not been scammed'; 271 respondents (17.6%) 'wanted to learn more about scams' and 231 respondents (14.7%) had 'recently been scammed'.

Demographics

Females comprised 54.6 percent of the sample (n=861), while males comprised 43.4 percent of the sample (n=685). Thirty respondents (1.9%) did not disclose their gender. Table 2 shows the breakdown of respondents by their age group.

As shown in Figure 1, most respondents resided in New South Wales (29.6%, n=466), Victoria (20.2%, n=318), Queensland (17.4%, n=274) and Western Australia (9.5%, n=150). Thirty-one respondents (2.0%) resided in New Zealand. South Australia (7.7%, n=121), Tasmania (3.2%, n=51) and the Northern Territory (1.0%, n=16) were the least represented states and territories in Australia.

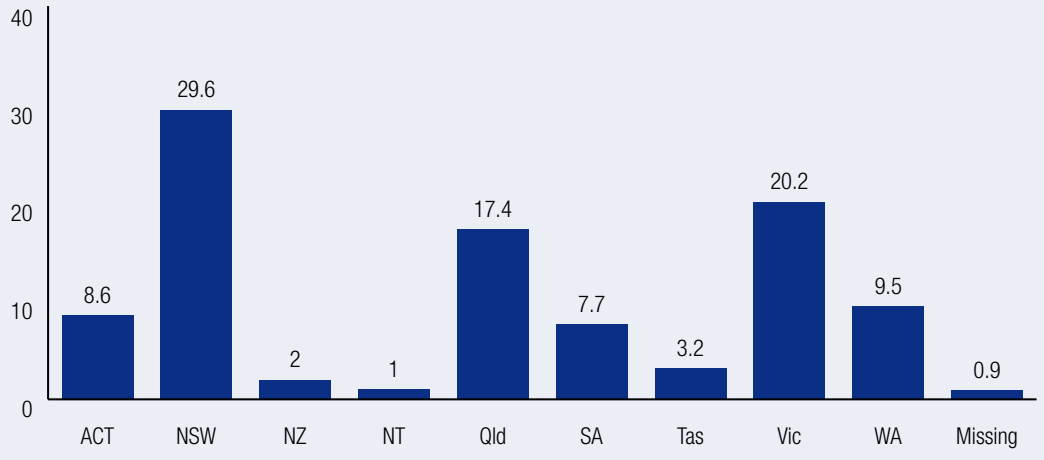
When asked about income, most respondents (n=421, 26.7%) responded that they would rather not disclose their income level and a further three percent (n=48) did not respond to the question. Most respondents (n=614, 38.9%) earned an income somewhere in the middle categories provided ($20,000 to $80,000), while 13.5 percent (n=213) earned less than $20,000 and 17.8 percent (n=280) earned in excess of $80,000 per annum. This is shown in Figure 2.

Table 2 Respondents by age

Age category (years)	n	%
17 and under	79	5.0
18–24	86	5.5
25–34	235	14.9
35–44	279	17.7
45–54	330	20.9
55–64	329	20.9
Over 65	224	14.2
Missing	14	0.9
Total	1,576	100

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

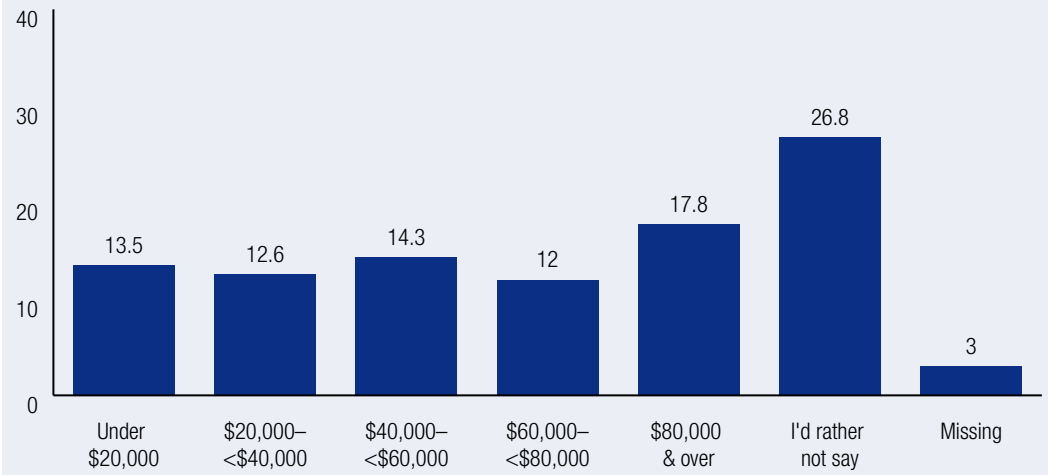
Figure 1 Respondents by location (%)



Note: Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Figure 2 Respondents by annual income (%)



Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Table 3 Scam invitation received by scam type

Scam type	Received scam invitation (n)	Received a scam invitation (%) (n=1,490)	Total sample (%) (n=1,576)
Lottery scams	945	63.4	60.0
Advance fee fraud	674	45.2	42.8
Inheritance scams	577	38.7	36.6
Phishing	709	47.6	45.0
Financial advice scams	360	24.2	22.8
Work from home scams	619	41.5	39.3
Dating scams	207	13.9	13.1
Computer support scams	838	56.2	53.2
Other	496	33.3	31.5

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Table 4 Scams by delivery method

Method of delivery	Received a scam invitation (n)	Received a scam invitation (%) (n=1,490)	Total sample (%) (n=1,576)
Mail	268	18.0	17.0
Email	1,128	75.7	71.6
Telephone	843	56.6	53.5
SMS	310	20.8	19.7
Internet site/social networking	320	21.5	20.3
Other	86	5.8	5.5

Source: ACFT Consumer Fraud Survey 2012 [AIC data

Receiving scams

Of the 1,576 survey participants in 2012, 1,490 (94.5%) had received at least one scam invitation. The number and percentage of respondents who had received at least one scam invitation by scam type is provided in Table 3. Respondents may have received invitations for more than one scam type. The most common type of scams received, reported by 945 (60%) of the survey participants, were lottery scams. This was followed by computer support centre scams (received by 53.2% of survey participants and 56.2% of those who had received a scam invitation). The least likely type of scam invitation reported to have been received was dating scams, received by 207 of the survey respondents, representing 13.9 percent of the sample who had received a scam invitation and 13.1 percent of the total sample.

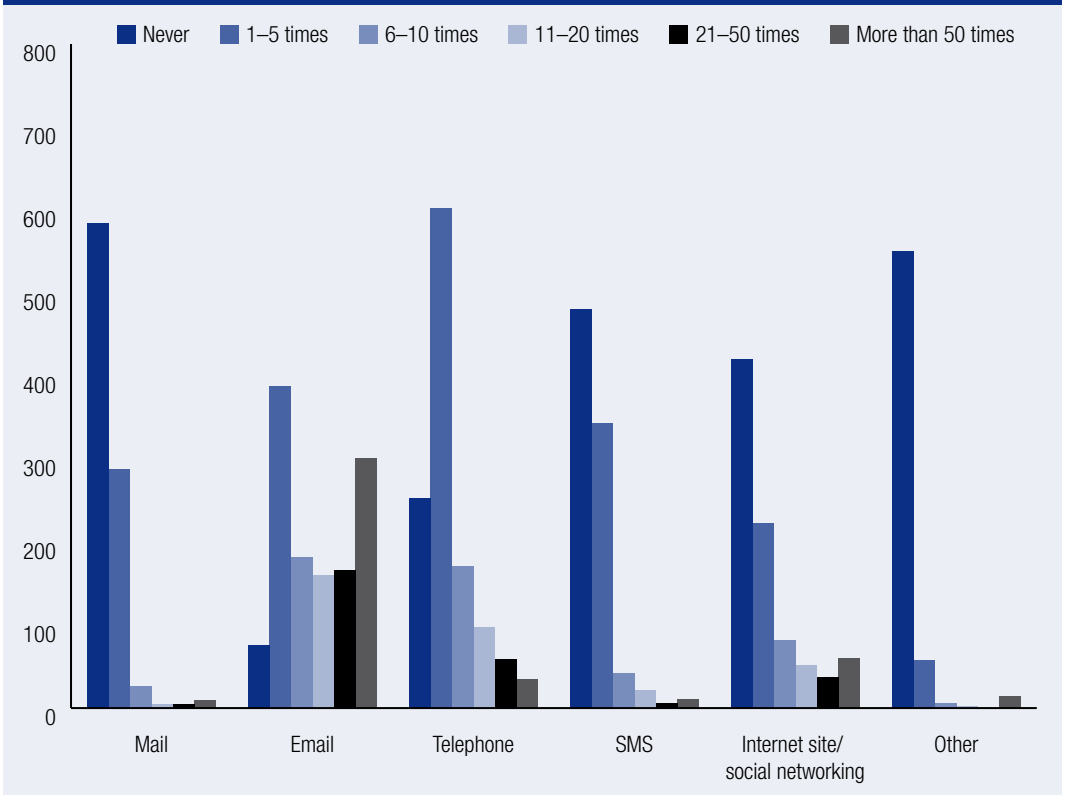
Details of the types of delivery methods by which respondents reported receiving scams are provided in Table 4. It is noted that participants could have received more than one scam invitation; therefore, multiple responses are recorded. Email was the most popular delivery method, with 75.7 percent of respondents who had received a scam invitation receiving at least one invite this way.

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

Responding to scams

During the 12 months prior to the survey, 350 (22.2%) of survey participants responded to a scam invitation by way of requesting further information, providing personal details or suffering

Figure 3 Scams received by delivery method (n)



Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Table 5 Loss of personal details by scam type

Scam type	Provided personal details (n)	Received a scam invitation (%) (n=1,490)	Total sample (%) (n=1,576)	Received an invitation to that type of scam (%)
Lottery scams	28	1.9	1.8	3.0
Advance fee fraud	23	1.5	1.5	3.4
Inheritance scams	13	0.9	0.8	2.3
Phishing	35	2.3	2.2	4.9
Financial advice scams	14	0.9	0.9	3.9
Work from home scams	21	1.4	1.3	3.4
Dating scams	19	1.3	1.2	9.2
Computer support scams	37	2.5	2.3	4.4
Other	76	5.1	4.8	15.3

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Table 6 Loss of money by scam type

Scam type	Suffered a financial loss (n)	Received a scam invitation (%) (n=1,490)	Total sample (%) (n=1,576)	Received an invitation to that type of scam (%)
Lottery scams	18	1.2	1.1	1.9
Advance fee fraud	15	1.0	1.0	2.2
Inheritance scams	7	0.5	0.4	1.2
Phishing	16	1.1	1.0	2.3
Financial advice scams	11	0.7	0.7	3.1
Work from home scams	14	0.9	0.9	2.3
Dating scams	19	1.3	1.2	9.2
Computer support scams	29	1.9	1.8	3.5
Other	56	3.8	3.6	11.3

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

a financial loss. This represented 23.5 percent of those who had received a scam invitation during the 12 month period.

Sixteen percent of the sample who had received an invitation sent their personal details, suffered a financial loss or both in response to at least one scam (n=231, 14.7% of the total sample). One hundred and six participants (7.1% of the sample who received a scam invitation and 6.7% of the total sample) sent their personal details only, 46 participants (3% of the sample who received a scam invitation and 2.9% of the total sample) suffered a financial loss only, and 79 participants (5.3% of the sample who received a scam invitation and 5% of the total sample) lost money as well as sent their personal details.

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

Inheritance scams were the least likely to result in the reported loss of personal details and/or money.

Dating scams continued to be among the most likely to lead to the loss of personal details or financial loss in relation to their prevalence, with nine percent of the sample who received a dating scam invitation reporting the loss of personal details and nine percent reporting a financial loss. In total, the financial loss due to dating scams alone was over $203,000—this amount was supplied from just 16 respondents.

Of the 231 victims who reported having suffered a financial loss, 108 (46.8%) disclosed the amount. This reportedly ranged from $3 to $1,000,000. With outliers removed ($1,000,000 reportedly lost due to a scam reported in the 'other' category), the reported financial loss totalled $846,170, ranging from $3 to $195,000 (mean=$7,908.13, median=$500.00).

Participants were able to select multiple responses when asked why they did not respond to scam invitations. Their responses are provided in Table 7. The most common reasons for not responding to scams included 'had seen/heard this was a type of scam in the media or a public source (reported by 55.2% of the total sample), 'had received similar offers before and thought they were scams' (54.9% of the total sample), or 'something was not quite right with the offer or invitation' (53.9% of the total sample).

Victim demographics

For the purpose of this report, scam victims were defined as those who had provided scammers with

Table 7 Reasons for not responding to scams received

Reason for not responding	n	Received a scam invitation (%) (n=1,490)	Total sample (%) (n=1,576)
Seemed too good to be true	775	52.0	49.2
Had received similar offers before and thought they were scams	865	58.1	54.9
Had seen/heard this was a type of scam in the media or a public source	870	58.4	55.2
Was told it was a scam by someone I knew	271	18.2	17.2
Someone I know has been a victim of a scam before	132	8.9	8.4
Wanted to respond but could not afford to participate	16	1.1	1.0
Something was not quite right with the offer or invitation	850	57.0	53.9
Offer was identified as spam/unsafe by internet filter	464	31.1	29.4
Other	257	17.2	16.3

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Table 8 Victims by age in years

Age category (years)	n	%	Respondents within that age category (%)
17 and under	11	4.8	13.9
18–24	14	6.1	16.3
25–34	25	10.8	10.6
35–44	46	19.9	16.5
45–54	54	23.4	16.4
55–64	43	18.6	13.1
Over 65	37	16.0	16.5
Missing	1	0.4	7.1

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

their personal details and/or suffered a financial loss as the result of a scam. Of the 231 victims who had lost personal details or suffered a financial loss as the result of the scam, 142 (61.5%) identified themselves as female, 85 (36.8%) identified themselves as male and four (1.7%) declined to reveal their gender. Therefore, of the respondents who disclosed their gender, 16.5 percent of the 861 female respondents experienced victimisation, compared with 12.4 percent of the 685 males.

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

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

Table 10 shows victims by the location in which they resided, as well as the percentage of total respondents within that location who reported victimisation. Most victims resided in New South Wales (n=66, 28.6% of the sample who reported victimisation), Queensland (n=50, 21.6% of the sample who reported victimisation) and Victoria (n=45, 19.5% of the sample who reported victimisation). Fourteen of the respondents residing in New Zealand reported victimisation. As there were 31 respondents from New Zealand,

Table 9 Victims by annual income

Annual income	n	%	Respondents within that income category (%)
Less than $20,000	41	17.7	19.2
$20,000–<$40,000	40	17.3	20.1
$40,000–<$60,000	40	17.3	17.7
$60,000–<$80,000	20	8.7	10.6
Over $80,000	34	14.7	12.1
I'd rather not say	54	23.4	12.8
Missing	2	0.9	4.2

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Table 10 Victims by location

Location	n	%	Respondents within that location (%)
Australian Capital Territory	14	6.1	10.4
New South Wales	66	28.6	14.2
New Zealand	14	6.1	45.2
Northern Territory	5	2.2	31.3
Queensland	50	21.6	18.2
South Australia	14	6.1	11.6
Tasmania	4	1.7	7.8
Victoria	45	19.5	14.2
Western Australia	18	7.8	12.0
Missing	1	0.4	7.1

Note: Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Table 11 Reporting of scams by agency

Organisation or person reported to	n	Received a scam invitation (%) (n=1,490)	Total sample (%) (n=1,576)
Not reported to anyone	443	29.7	28.1
Family/friends	683	45.8	43.3
Police	120	8.1	7.6
SCAMwatch website (www.scamwatch.gov.au)	310	20.8	19.7
Australian Competition and Consumer Commission	122	8.2	7.8
The business represented (eg bank, eBay etc)	272	18.3	17.3
Internet Service Provider	90	6.0	5.7
Legal aid, a lawyer, or a community legal services clinic	11	0.7	0.7
Unable to recall	18	1.2	1.1
Other	210	14.1	13.3

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Table 12 Reporting of victimisation by agency

Organisation or person reported to	n	Reported victimisation (%) (n=231)
Not reported to anyone	40	17.3
Family/friends	112	48.5
Police	40	17.3
SCAMwatch website (www.scamwatch.gov.au)	75	32.5
Australian Competition and Consumer Commission	35	15.2
The business represented (eg bank, eBay etc)	64	27.7
Internet Service Provider	15	6.5
Legal aid, a lawyer, or a community legal services clinic	9	3.9
Unable to recall	6	2.6
Other	44	19.0

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

this resulted in a 45 percent victimisation rate of respondents from that location. Similarly, although only five victims resided in the Northern Territory, they comprised 31.3 percent of respondents from that location.

Reporting scams

Almost 74 percent of respondents who had received a scam invitation reported it to at least one other person or organisation (n=1,094; 69.4% of the total sample). The reporting rate dropped to 51.7 percent of the sample who had received a scam invitation (n=770; 48.8% of the total sample) when friends and family were excluded. Friends and families were the most common recipients of scam complaints, as they were in previous years. Forty-six percent of those who received a scam invitation reported it to a friend or family member. Only 8.1 percent of respondents who had received a scam invitation reported it to the police, 8.2 percent reported it to the ACCC and 20.8 percent reported it to the SCAMwatch website. Table 11 details who

complaints were made to; it is noted that respondents were permitted to select more than one option.

Of the 231 respondents who reported falling victim to a scam, 192 (83.1%) reported scams to at least one other person or organisation. When friends and family were excluded, the reporting rate dropped to 72.3 percent (n=167) of the victim respondents who had reported to an external agency. Table 12 shows those organisations or persons victimisation was reported to, with respondents permitted to select more than one option. Victims were most likely to report scams to friends and family (48.5%), the SCAMwatch website (32.5%) and the business represented (27.7%). Policing agencies received complaints from 17.3 percent of victims and the ACCC received complaints from 15.2 percent. Respondents were given the option to provide other people or organisations that they have reported scams to and these ranged from 'work IT departments' to government departments and computer software organisations. Respondents also noted that when they realised acquaintances' email or social networking sites had been hacked, they reported to the owners of the email address or person who created site.

Respondents were asked why they reported scams they had received to a formal agency. Participants could select more than one reason for reporting scams. The most common reasons for reporting a scam included 'wanting to prevent others from being scammed' (41.4% of sample who received a scam invitation) and 'knew it was the right thing to do' (29.4% of the sample who received a scam invitation). The responses are detailed in Table 13. Other reasons for reporting scams ranged from 'wanting to get money back' to wanting to garner greater publicity about the scam to warn others. Another respondent reported the scam as they felt it was 'a breach of security that they have my details'.

Cited reasons for not reporting scam invitations are outlined in Table 14. The most commonly provided reasons included 'unsure of which agency to contact' (42.3% of the sample who had received a scam invitation) and 'didn't think anything would be done' (34% of the sample who had received a scam invitation). It is noted that participants may have reported some scams but not others and may have had multiple reasons for not reporting. Respondents were given the option to supply their own reason for not reporting a scam. A recurring reason for those who received a scam invitation and did not report it was that 'the scams were already well-known'. On respondent noted I 'wondered if the report a scam email address was also a scam' and several respondents advised that nothing had happened in the past when they had reported and so they no longer report scams.

The survey asked whether respondents had reported scams on behalf of anyone else. One hundred and eleven respondents (7%) indicated that they had. Table 15 indicates on whose behalf scams were reported, with participants permitted to select all options that applied to them.

Perceptions of scams

Respondents were asked how they perceived each scam type. They were asked to indicate whether they considered each scam type as a 'crime', 'wrong but not a crime', or 'just something that happens'. Respondents were permitted to select more than one response. The results are outlined in Table 16. Advance fee fraud and phishing were most likely to be considered a crime (by 80.9% and 80.5% of the sample respectively). Again, respondents were given the opportunity to provide their own responses in a 'free text box'. Some of the responses demonstrate the need for greater education around victims of scams (eg 'If you're stupid enough to give your money away to these scammers, you don't deserve it anyway, but I still think that it is a crime'). These types of responses indicate that, while people understand the illegal nature of fraud and scams, the financial and emotional impact that scams may have on victims is perhaps not fully appreciated.

The perception of scams by respondents who reported victimisation from that scam type was also explored. Again, it is noted that participants could select more than one response. The results are outlined in Table 17. Advance fee fraud was most likely to be considered a crime by victims of this scam. It should be noted that some respondents chose to not respond to the questions.

Table 13 Reasons for reporting scams received

Reason for reporting scam invitation	n	Received a scam invitation (%) (n=1,490)	Total sample (%) (n=1,576)
Desired the apprehension of offender(s)	340	22.8	21.6
Wanted to prevent others from being scammed	617	41.4	39.2
Knew it was the right thing to do	438	29.4	27.8
To assist in the investigation of an offence	414	27.8	26.3
To support your insurance claim	11	0.7	0.7
Other	81	5.4	5.1

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Table 14 Reasons for not reporting scams received

Reason for not reporting	n	Received a scam invitation (%) (n=1,490)	Total sample (%) (n=1,576)
Not worth the effort	456	30.6	28.9
Didn't think it was illegal	65	4.4	4.1
Unsure of which agency to contact	630	42.3	40.0
Feared I would get into trouble	24	1.6	1.5
Didn't think anything would be done	507	34.0	32.2
Receive too many to report	409	27.4	26.0
Other	218	14.6	13.8

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Table 15 Scams reported on behalf of someone else

Scam reported on behalf of	n	Total sample (%) (n=1,576)
Child (son or daughter)	36	2.3
Older relative (brother/sister, parent, grandparent, aunt/uncle)	56	3.5
Younger relative (niece/nephew, brother/sister)	12	0.8
A friend	36	2.3
A colleague	18	1.1
A student (if you are a teacher or in some similar capacity)	3	0.2
Other	33	2.1

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Table 16 Perceptions of scams by scam type

Scam type	A crime		Wrong but not a crime		Just something that happens	
	n	%	n	%	n	%
Lottery scams	1,036	65.7	321	20.4	92	5.8
Advance fee fraud	1,275	80.9	113	7.2	41	2.6
Inheritance scams	1,073	68.1	285	18.1	57	3.6
Phishing	1,269	80.5	120	7.6	31	2.0
Financial advice scams	739	46.9	508	32.2	154	9.8
Work from home scams	1,061	67.3	232	14.7	111	7.0
Dating scams	809	51.3	476	30.2	103	6.5
Computer support scams	1,238	78.6	184	11.7	49	3.1
Other	664	42.1	124	7.9	124	7.9

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

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

Scam type	A crime		Wrong but not a crime		Just something that happens	
	n	%	n	%	n	%
Lottery scams (n=36)	33	91.7	1	2.8	2	5.6
Advance fee fraud (n=29)	27	93.1	2	7.1	0	0.0
Inheritance scams (n=16)	14	87.5	1	6.3	1	6.3
Phishing (n=40)	32	80.0	2	5.0	5	12.5
Financial advice scams (n=20)	12	60.0	6	30.0	2	10.0
Work from home scams (n=28)	19	67.9	5	17.9	2	7.1
Dating scams (n=26)	20	76.9	5	19.2	0	0.0
Computer support scams (n=48)	42	87.5	3	6.3	2	4.2
Other (n=100)	59	59.0	6	6.0	8	8.0

Source: ACFT Consumer Fraud Survey 2012 [AIC data file]

Online shopping and auction frauds

The theme of the 2013 National Consumer Fraud Week is online shopping and auction frauds. Accordingly, participants in the 2012 survey that had been exposed to, or been victimised as a result of, scams via these mediums are discussed in this section. Although this was not a specific scam category included in the survey, there were numerous inclusions in the 'other' scam category that revealed scams had been attempted or undertaken on online shopping or auction sites.

There were 496 respondents who reported they had received a scam categorised as 'other'. Of these, 112 (22.6%) reportedly took place on an online shopping or auction site. Fifty-three respondents reported that they had been contacted by a scammer when advertising their vehicle for sale, 38 when advertising other items for sale, 10 when purchasing products online and 11 did not provide specific details.

Vehicle sales

Almost half (47.3%, n=53) of the scams that took place on online shopping and auction sites involved the sale of a vehicle. In addition to cars, it was reported that scammers had targeted boats (n=3) and motorcycles (n=3), as well as one trailer and one caravan. Where respondents had provided details of the scams, they followed similar themes. These typically included:

- an overseas buyer;
- the buyer wanting to see the vehicle sight unseen;
- being offered a larger amount than what was advertised;
- being requested to pay an agent or courier/ shipping service fee, with a promise that this would be reimbursed; and/or
- a fake remittance notice being sent advising that a payment had been made to the seller's account.

Examples of responses that were provided by survey respondents included:

> An attempt to purchase a car, unseen, for a larger amount than asked. Refused to call, all correspondence via email after initial SMS.
>
> Have motor vehicle for sale on website, twice approached to pay 'broker' on their behalf.
>
> Hoax car purchase—request to txfr courier fees before receiving money for car.
>
> Offer to purchase used car that I am selling, sight unseen, offering more $.
>
> Purchase of second hand car saying they don't need to see it as they trust me.

Selling a car online…money sent for transfer and payment to a third party.

Twenty-three respondents included in their response the website that they had been using to advertise their vehicle. Nine different trading sites were mentioned, one of which account for over half (n=12) of the reports.

One respondent advised that they had lost money as a result of a vehicle sale scam. The amount lost was $1,000, which was reportedly transferred to an 'agent' using a money transfer service. A further six respondents revealed that they had disclosed personal information to the scammer.

Sale of other items

Thirty-eight participants reported that they had been targeted when selling other items, excluding vehicles, online. In addition to being targeted through auction sites and trading post sites, it appeared that small business owners who operated their own websites were being targeted. Products targeted in these scams (where specified) included furniture, pets, electronic and computer equipment, and wine. The main methodology employed by scammers appeared to be similar to that used for the vehicle sale scams, in that they posed as an overseas buyer, requested transport fees be paid for by the seller, offered to pay more than the item was advertised for and sent fake remittance notices advising that a payment had been made. However, buying sight unseen was not mentioned as being a red flag for the sale of other items, probably because by contrast with selling vehicles, this is normal practice when purchasing items online. The following illustrates the types of responses received:

Buyer responding to online ad—offering to pay more than listed price with instructions to wire excess funds overseas.

Prospective buyer of my for sale item wanted money transferred to them in advance of sale.

Purchase goods from me to be sent with their chosen shipping company to Asia and they want to pay in full by credit card. Chosen shipping company does not accept credit cards.

Purchasing of an item I had for sale to transfer money to pick up agent in UK.

To purchase goods from me by credit card payment and have me pay their international freight invoice on their behalf.

Another scam variation was as follows:

African company placing order for goods and paying by credit card. Later cancelling and asking for a cash refund and 'take out 10% for your trouble'.

Twenty-five respondents indicated the site they had advertised their products on. In total, three sites were mentioned and of these, one accounted for 21 (84%) of such reports. This site was the same one that accounted for the majority of vehicle sale scam contacts.

Three respondents advised that they had sent money as well as their personal information as a result of being scammed in this way. The amounts reportedly lost were $800, $900 and $760. Seven respondents revealed that they had disclosed personal information only.

Purchasing goods

Ten respondents indicated that they had been exposed to scams while purchasing products online. While three respondents did not provide specific details about the type of scam they had received, two reported that they had found counterfeit items offered for sale and another two found products that would not offer the advertised benefits; one of these respondents reported a loss of $20 for the purchase of a 'useless product'. Two respondents reported that they had purchased computers and electronic goods online that had never been received. The financial losses were $400 and $560, and both reported that they had also provided their personal information. Another respondent supplied his personal information to an advertiser, but did not purchase the product after being supplied with false information about the seller.

Other unspecified online shopping and auction frauds

Eleven respondents indicated that they had been exposed to online shopping auction frauds, however did not provide specific details. These were mainly identified by the respondent naming an online shopping or auction site. One respondent reported the loss of $68 and their personal information as the result of an '*online shopping scam'.*

A further two respondents reported they had experienced financial losses from online auction sites, with the amounts totalling $493 and $600. Three respondents reported the loss of the personal information only from internet trading sites.

Conclusion

Findings and discussion

As in previous years, scam invitations were received by a large proportion of the survey respondents, with 94.5 percent of participants reported receiving a scam invitation in the 12 months prior to the survey. The most commonly received scams were lottery scams, computer support centre scams and phishing scams.

Consistent with the 2010 and 2011 ACFT survey findings (Hutchings & Lindley 2012), dating scams resulted in the greatest level of victimisation, although they were the least prevalent scam type. Victims of dating scams reported losses exceeding $200,000. This finding remains consistent with scam complaints made to the ACCC (2012a). In 2012, the ACCC issued voluntary best practice guidelines for dating sites to prevent the proliferation of romance scams. These guidelines include:

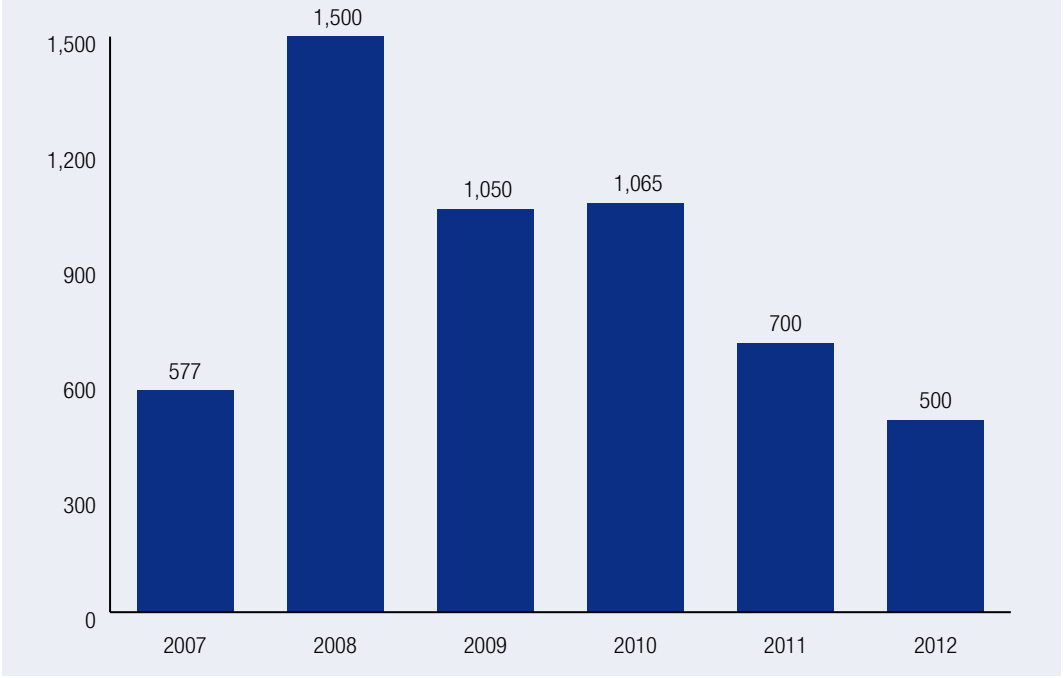
- displaying simple and direct warning messages in appropriate locations;
- implementing a vetting and checking system to identify advertisements that have been created by scammers; and
- providing a mechanism whereby users can report scams (ACCC 2012b).

Dating sites that comply with these guidelines and provide services that are relatively free from scammers may enjoy an enhanced reputation and users may have an increased confidence in the site. Future scam surveys will assist in determining what effects these efforts to raise awareness of dating and romance scams (as well as disrupting scam activities) will have on rates of reported victimisation.

Twenty-two percent of respondents disclosed that they had responded to a scam invitation in the 12 months prior to the survey. Responding could mean sending money or personal details or asking for more information. Almost seven percent stated that they sent personal information as a result of a scam invitation, 2.9 percent sent money and five percent of the sample disclosed that they had sent personal details and experienced a financial loss. While the loss of money can be damaging, perhaps future campaigns need to highlight that in the 21st century, personal information can be a type of currency itself. With the rise of online transactions and the importance of identity-related information in economic commerce, identity is now a legal concept as well as a commodity (UNODC 2011).

As shown in Figure 4, the median financial loss reported each year has been steadily declining since 2010. The median financial loss of $500 reported in 2012 is the lowest reported in the AIC's annual consumer fraud survey thus far and is one-third of the median reported loss in 2008.

Figure 4 Median reported financial loss by year ($)



Source: ACFT Consumer Fraud Surveys 2007, 2008, 2009, 2010, 2011 and 2012 [AIC data files]

The ACCC (2012a) and Hutchings and Lindley (2012) noted that between 2010 and 2011, there had been an increase in unsolicited telephone calls as the preferred scam delivery method. While overall, email remained the most common method by which scams were delivered, the findings from the current ACFT survey continue to show high levels of scams disseminated by telephone and SMS. The main difference with these two scam delivery methods is that, while many respondents reported receiving scam invitations by phone, most reported receiving just one to five scam invitations this way. By contrast, more participants reported receiving multiple scam invitations by email. Of those who reported receiving scam invitations by email, over one-quarter (26.7%) had received more than 50 solicitations this way.

Included in the 2012 survey was a new scam category 'computer support scams'. A computer support scam was defined as *a person representing themselves as someone from a computer support centre*. This category was included in the 2012 survey as, in the 'other' category in the 2011 ACFT survey there was a high proportion (over 150 respondents) who indicated they had received a scam that was purportedly from a computer software company or a computer service centre area. The findings showed that the computer support centre scam was one of the most common type of scams received by respondents (53.2% of respondents indicated they had received this type of scam invitation), second only to lottery scams. No doubt as a result of the prevalence of this type of scam, respondents indicated that the computer support centre scam was in the top three scam types likely to be considered a crime by participants. This type of scam demonstrates the adaptability of scammers and while recent scams have relied on new and emerging communication technologies (such as SMS ringtone scams or premium text messages), scams that rely on older technology (such as telephones) remain a concern. This is especially so with the widespread use of Voice over Internet Protocols (VOIP), which allows scammers to make telephone calls very cheaply.

It has previously been noted that the rate of reporting scams to law enforcement and regulatory agencies is generally quite low (Hutchings & Lindley

2012). This continues to be evident in the 2012 findings, with only 17.3 percent of victims reporting the scam to police and 15.2 percent reporting the scam to the ACCC. It was concerning to note that the most common reason for not reporting a scam invitation in the survey was that respondents were unsure of which agency to contact. A low reporting rate affects resources that may be allocated to combat scams and it also impacts the overall knowledge and understanding that agencies have to develop awareness and education campaigns. For example, it has been consistently demonstrated in this survey over the years that it is not the most commonly received scams, such as lottery scams, that cause the most victimisation. While reporting rates are low, when respondents did report a scam invitation, the most frequent reasons for doing so was to prevent others from becoming a victim of the scam and because they knew it was the right thing to do.

Online trading and auction sites

As scams and frauds that take place on online trading and auction sites was the focus of the 2013 National Consumer Fraud week, survey results relating to this scam type were examined in detail. Interestingly, scams involving goods offered for sale by the intended victim were reportedly more common than scams involving the purchase of goods, such as for non-existent, stolen or counterfeit goods, the non-delivery of items, or the misrepresentation of products. Scammers typically offered sellers a larger amount for the item than was advertised and requested the seller to cover the costs associated with an overseas agent or courier service, promising that they would be reimbursed. It appears that the 'agent' or 'courier service' were fronts for the receipt of the scammed funds and scammers also commonly faked remittance notices to indicate that a payment had been made when it had not. Vehicles, such as cars, were common targets for scammers, presumably due to their high value, as well as the costs associated with shipping overseas.

None of the respondents reported shill bidding, where the price is artificially inflated due to false bids, or fee stacking, whereby additional fees are added on after the auction (Yar 2006).

It was noted that one online trading site was overrepresented in respondents' accounts of scam attempts and actual victimisation. This site accounted for 52.2 percent of vehicle sale scams and 84 percent of scams involving the sale of other items, where the site was known. The website in question was examined and it was noted that this overrepresentation was despite the provision of warning notices identifying the common methodologies used by scammers (as of April 2013). One reason for this overrepresentation may be because unlike another popular trading site, payment methods are not offered by the website, which would mean that the transaction would be kept onsite and would be harder to falsify.

Suggestions for future campaigns

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

- developing a greater awareness about the potential harms associated with disclosing personal details. The disclosure of personal details can lead to further victimisation such as identity crimes and financial losses. Future campaigns could focus on the value of personal information and how those details may be used by scammers;
- changing the perception of victims. Survey findings indicate that respondents may hold negative views about people who fall victim to scams. This type of belief undermines people wanting to report victimisation and scam invitations. Campaigns could highlight the sophistication of some scams and the damage they cause, including the emotional impacts on victims and their families; and
- new technologies that scammers may focus on, yet still maintaining an awareness of how older scams or older technologies (such as landline telephones) can be used by scammers.

References

URLs correct as at May 2013

Australian Bureau of Statistics (ABS) 2008. *Personal fraud 2007*. cat no. 4528.0. Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/4528.02007?OpenDocument

Australian Competition & Consumer Commission (ACCC) 2012a. *Targeting scams: Report of the ACCC on scam activity 2011*. Canberra: ACCC. http://www.accc.gov.au/content/index.phtml/itemId/1039349

Australian Competition & Consumer Commission (ACCC) 2012b. *Best practice guidelines for dating websites*. Canberra: ACCC. http://transition.accc.gov.au/content/index.phtml/itemId/1032533

Australian Competition & Consumer Commission (ACCC) 2011. *The little black book of scams: Your guide to scams, swindles, rorts and rip-offs*. Canberra: ACCC. http://transition.accc.gov.au/content/item.phtml?itemId=816453&nodeId=ef518e04976145ffed4b13dd0ecda1a6&fn=Little%20Black%20Book%20of%20Scams.pdf

Budd C & Anderson J 2011. Consumer fraud in Australasia: Results of the Australasian consumer fraud taskforce online Australia surveys 2008 and 2009. *Technical and Background Paper series* no. 43. Canberra: 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://www.aic.gov.au/publications/current%20series/tbp/41-60/tbp050.html

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

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

United Nations Office on Drugs and Crime (UNODC) 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

Yar M 2006. *Cybercrime and society*. London: SAGE Publications Ltd

Appendices

Appendix 1 2012 consumer fraud survey

Australasian Consumer Fraud Taskforce Online Survey 2012

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

   a) Having won a lottery or some other prize,

   b) A request for assistance to transfer money out of another country (such as Nigeria),

   c) A notification of an inheritance,

   d) A request by a business to confirm your personal details or passwords (phishing scams),

   e) A request to supply you with financial advice,

   f) An opportunity to work from home (a front for money laundering),

   g) A person representing themselves as someone from a computer support centre

   h) Pursuing a personal relationship that turned out to be false, or

   i) Some other scam type

- ○ Yes
- ○ No (Skip to Q15)

2. How were you contacted in relation to each of the following scams? (Select all responses that apply for each type of scam listed)

	Delivery method						
Type of Scam	Mail	Email	Telephone (including landlines and mobile phones)	SMS	Internet site/social networking site	Other	N/A
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	☐	☐	☐	☐	☐	☐	☐
An opportunity to work from home (a front for money laundering)	☐	☐	☐	☐	☐	☐	☐
Pursuing a personal relationship that later turned out to be false	☐	☐	☐	☐	☐	☐	☐
Computer support centre scam	☐	☐	☐	☐	☐	☐	☐
Other type of scam	☐	☐	☐	☐	☐	☐	☐

If 'other', please specify

3. How many times over the last 12 months have you received scams via each of the following methods?

Note: Select one response for each method of scam listed as applicable

	How many times received					
Scam method	Never	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail	○	○	○	○	○	○
Email	○	○	○	○	○	○
Telephone (including landlines and mobile phones)	○	○	○	○	○	○
SMS	○	○	○	○	○	○
Internet site/ social networking	○	○	○	○	○	○
Other	○	○	○	○	○	○

If 'other', please specify

4. Over the last 12 months, have you responded in any way to these scams?

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).

- Yes
- No (Skip to Q10)

5. How many times over the last 12 months have you responded to each of the following types of scams? (Select one response for each type of scam listed)

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

6. Have you ever sent money as a result of any of these scams? (Select one response for each type of scam listed)

Type of Scam	Yes	No	Don't know/ I can't recall
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			
An opportunity to work from home (a front for money laundering)			
Pursuing a personal relationship that later turned out to be false			
Computer support centre scam			
Other type of scam			

If 'other', please specify

7. If you responded 'yes' to any of the options in Q6, what is your best estimate of the total amount of money you have sent in the last 12 months? If you responded 'no' to Q6, skip to Q8.

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 ($).

8. Have you ever disclosed personal details or passwords as a result of these scams? (Select one response for each type of scam listed)

Type of Scam	Yes	No	Don't know/ I can't recall
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	○	○	○
An opportunity to work from home (a front for money laundering)	○	○	○
Pursuing a personal relationship that later turned out to be false	○	○	○

Other type of scam

If 'other', please specify

9. If you responded 'yes' to Q6 or Q8, how many times were you in contact with the person(s) before you sent money or personal information? (Select one option only)

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

10. 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)

- 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 specify

11. Have you reported any of these scams to anyone? (Select all that apply)

- Not reported to anyone (go to Q13)
- Family/ friends
- Police
- SCAMwatch website (www.scamwatch.gov.au)
- Australian Competition and Consumer Commission / Fair Trading or Consumer Protection agencies

- [ ] The business represented (e.g. bank, ebay etc)
- [ ] Internet Service Provider
- [ ] Legal aid, a lawyer, or a community legal services clinic
- [ ] Unable to recall
- [ ] Other

If 'other', please specify

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)

- [ ] Desired the apprehension of offender(s)
- [ ] Wanted to prevent others from being scammed
- [ ] Knew it was the right thing to do
- [ ] To assist in the investigation of an offence
- [ ] To support your insurance claim
- [ ] Other

If 'other', please specify

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 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 specify

14. Have you reported any of the scams specified in Q11, on behalf of anyone else?

- ( ) Yes
- ( ) No

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

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

If 'other', please specify

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

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

If 'other', please specify

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 specify

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

- [ ] 2011
- [ ] 2010
- [ ] 2009
- [ ] 2008
- [ ] 2007
- [ ] Never

18. Are you aware of the 2012 fraud awareness campaign run by the Australasian Consumer Fraud Taskforce?

- ○ Yes
- ○ No

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

- ○ Yes
- ○ No

20. Which age group do you belong to?

- ○ 17 and under

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65+

21. What is your sex?

- Male
- Female

22. Where do you normally reside?

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

Please specify country

If you normally reside in Australia what is your postcode?

23. What was your gross income from all sources for the year 2010-2011 (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?

- ☐ 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 specify

25. In which capacity did you fill out this survey?

- ○ Member of the public
- ○ Retiree
- ○ Member of the police
- ○ My employer is an Australasian Consumer Fraud Taskforce Government member
- ○ My employer is an Australasian Consumer Fraud Taskforce private sector partner
- ○ Other Government agency

Thank you for completing the 2012 Australasian Consumer Fraud Taskforce Survey. If you are happy with your responses please click the "submit" button below. Alternatively you can review and change your responses and then submit.

Appendix 2 Newspaper articles relating to consumer fraud published 19 to 25 March 2012

Elsworth S 2012. Con artists net $85m scammers suck in victims over phone. *The Mercury* 19 March

Elsworth S 2012. Phone fraud cases double. *The Courier-Mail* 19 March

Herald Sun 2012. Scams ring up $85m. *Herald Sun* 19 March

Niesche C 2012. $85m lost in business scams last year. *The Age* 19 March

Niesche C 2012. Mounting scams target busy owners. *Sydney Morning Herald* 19 March

Rochfort S 2012. Now meet ASIC, the co-regulator. *Sydney Morning Herald* 19 March

Seedy K 2012. Another cheap trick. Lilydale *Yarra Valley Leader* 18 March

The Advertiser 2012. Scammers swindle $85m in year. *The Advertiser* 19 March

Wells R 2012. Scam losses double to $85m. *The Age* 19 March

Advocate 2012. Don't fall victim as scammers get smarter. *Advocate* 20 March

Dastgheib S 2012. Online trader wiser after being stung by fraudster. *Dominion Post* 20 March

Geelong Advertiser 2012. Rorts double in a year, cost Australians $85 million scams skyrocket. *Geelong Advertiser* 20 March

Herald 2012. Scammers make call on change from net. *Herald* 20 March

Manawatu Standard 2012. Online bank fraud alert. *Manawatu Standard* 20 March

Pullar-Strecker T 2012. Government urged to hunt overseas scammers; Locked up. *Dominion Post* 20 March

Sunshine Coast Daily 2012. Tax chief in scam warning. *Sunshine Coast Daily* 20 March

The Gold Coast Bulletin 2012. Scam losses top $85m. *The Gold Coast Bulletin* 20 March

The Marlborough Express 2012. Online bank fraud alert. *The Marlborough Express* 20 March

The Marlborough Express 2012. Scammers fleecing Kiwis of millions. *The Marlborough Express* 20 March

The Nelson Mail 2012. Bankers' group warns of online fraud. *The Nelson Mail* 20 March

The Northern Territory News 2012. Aussies conned of $85m. *The Northern Territory News* 20 March

The Observer 2012. Telstra issues warning. *The Observer* 20 March

The Queensland Times 2012. Scam schemes get new scrutiny. *The Queensland Times* 20 March

The Standard 2012. The number of scams reported to Australia's. *The Standard* 20 March

Fraser Coast Chronicle 2012. News briefs. *Fraser Coast Chronicle* 21 March

Mt Druitt - St Mary's Standard 2012. Fast Lane. Mt Druitt - *St Mary's Standard* 21 March

News Mail Bundaberg 2012. Just briefly. *News Mail Bundaberg* 21 March

The Chronicle. 2012. INBrief. *The Chronicle* 21 March

The Northern Territory News 2012. Con jobs by phone. *The Northern Territory News* 21 March

The Redcliffe & Bayside Herald 2012. Beware, scammers are about. *The Redcliffe & Bayside Herald* 21 March

Heaney C 2012. Let proprietor beware. *Herald Sun* 22 March

The Queensland Times 2012. Telco warns of shift to phone scams. *The Queensland Times* 22 March

Central Coast Express Advocate 2012. Phone scams on the rise. *Central Coast Express Advocate* 23 March

Sunshine Coast Daily 2012. Door-to-door tree warning. *Sunshine Coast Daily* 23 March

The Courier 2012. Warning on mobile-phone scams. *The Courier* 23 March

The Gold Coast Bulletin 2012. Mobile banking scam. *The Gold Coast Bulletin* 23 March

The Queensland Times 2012. Police urge tightening of internet security. *The Queensland Times* 23 March

Barrington M 2012. Ambulance scammer active. *The Northern Advocate* 24 March

Daily Examiner 2012. Scam warning. *Daily Examiner* 24 March

The Advocate 2012. Beware of phone conmen. *The Advocate* 24 March

St George and Sutherland Shire Leader 2012. Mobile scams warning. *St George and Sutherland Shire Leader* 25 March

AIC Reports
Technical and Background Paper 56

The Australasian Consumer Fraud Task Force has conducted a range of fraud prevention and awareness raising activities since 2006. This report presents the results of the 2012 online consumer fraud survey conducted in conjunction with the 2012 campaign, *Slam Scams*!

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

www.aic.gov.au