Australian Government
Australian Institute of Criminology

Australasian Consumer Fraud Taskforce: Results of the 2010 and 2011 online consumer fraud surveys

Alice Hutchings
Jade Lindley

AIC Reports
Technical and Background Paper 50

Australasian Consumer Fraud Taskforce: Results of the 2010 and 2011 online consumer fraud surveys

Alice Hutchings
Jade Lindley

AIC Reports
Technical and
Background Paper
50

www.aic.gov.au

ISSN 1836-2052
ISBN 978 1 922009 12 8

Project no. 1326
Dataset no. 0104

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

The Australasian Consumer Fraud Taskforce (ACFT) includes 22 government regulatory agencies and departments in Australia and New Zealand that work alongside private sector, community and non-government partners to prevent fraud. In order to understand the dynamics of consumer fraud victimisation, 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 the range of ways scams can impact on victims and their families, to determine how victims respond to the experience and to identify any emerging typologies and issues.

This report presents the results of surveys conducted in conjunction with the 2010 campaign, *Online Offensive—Fighting Fraud Online*, and the 2011 campaign, *Scams: It's Personal*. Overall, in both surveys it was found that a high proportion of respondents had received a scam invitation, however the majority did not respond. Dating scams attracted the highest number of victims in 2010, whereas in 2011, lottery scams were the most common way in which respondents were victimised.

Although the survey relies on self-reported information, it still provides a useful means of identifying the nature of victimisation and personal fraud trends. Those who perpetrate consumer scams use a wide range of deceptive practices and methods of communication. While email continues to be the most common method by which scams are delivered, the use of landline and mobile telephones, including SMS, to target potential scam victims, has continued to increase. This points to the need for ongoing education on the risks of scam victimisation for those who make use of mobile phones and SMS, particularly younger people.

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

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

Executive summary

Research background and methodology

The Australasian Consumer Fraud Taskforce (ACFT) includes 22 government regulatory agencies and departments in Australia and New Zealand that work alongside private sector, community and non-government partners to prevent fraud. The ACFT has conducted a range of fraud prevention and awareness-raising activities since 2006. One key activity of the ACFT is to hold an annual consumer fraud survey to obtain a snapshot of the public's exposure to consumer 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 subgroup. This report presents the results of the 2010 and 2011 surveys, which each ran for three months commencing from 1 January and encompassed National Fraud Prevention week that coincides with global awareness-raising activities. The theme of the 2010 campaign was *Online Offensive—Fighting Fraud Online*, which focused on the increased prevalence of online fraud. In 2011, the campaign *Scams—It's Personal* aimed to increase awareness about personalised and targeted frauds and scams. Both surveys explored scams where respondents had been contacted by phone, SMS, email, letter, via the internet and/or in person by someone that 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 from 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); and
- other fraud types.

The surveys were available to complete on the AIC's website. Participants who did not reside in Australia or New Zealand were excluded from the survey and invalid responses were not counted. In 2010, 246 participants completed the survey; the number of respondents increased in 2011, with 1,145 respondents. The larger sample size in 2011 may be partly due to the increased coverage of the survey in the media. Outliers, typically very large loss figures from respondents who appeared to have misunderstood the question, were removed from the analysis.

The 2010 and 2011 surveys suffer from a number of limitations that make it difficult to generalise their findings to the greater Australasian population. These limitations include:

- The small sample size, particularly for the 2010 survey, for which only 246 valid responses were received. It is likely that the small response rate for 2010 can be attributed to the lack of media coverage surrounding the survey.
- The self-selection bias of the survey design. This means that those who participated in the survey may be different from the general population, making the findings difficult to generalise.
- The survey is limited to those who have computer and internet access.

- Differences between the 2010 and 2011 surveys made comparison difficult. For example, in the 2010 survey, participants were asked about 'unsolicited contacts', however, the wording in 2011 changed to 'scams'. Because of these differences, the surveys have been analysed separately in this report, however conclusions are drawn across the two years, where possible.

Delivery of scams

The 2010 and 2011 surveys asked respondents about the types of scams they had been sent, as well as how they had been delivered. Results indicated that:

- 89 percent of respondents in 2010 and 94 percent in 2011 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 in 2010 were lottery scams (received by 56% of the total sample), advance fee frauds (51%) and phishing scams (50%). In 2011, lottery scams remained the most common type of scam received (by 57% of the total sample). While advance fee frauds and phishing scams were also common (received by 41% of the sample each), their prevalence was exceeded by the proportion of work from home scams reported (by 41% of the total sample).
- The least common type of scams received in 2010 and 2011 were dating or romance scams, reported by 19 percent of the total sample in 2010 and by 11 percent of respondents in 2011.
- Email was the most common scam delivery method, with 76 percent of the sample receiving a scam this way in 2010 and 67 percent in 2011. However, the use of telecommunications to deliver scam invitations increased in 2011, with 39 percent of the sample receiving scams by telephone (either landline or mobile) and 15 percent receiving scams by short message service (SMS).

Responding to scam invitations

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

- Twenty-nine percent of those surveyed in 2010 and 29 percent in 2011 responded in some way to a scam invitation in the 12 months preceding the survey:
  - eight percent in 2010 and 2011 sent their personal details;
  - two percent of 2010 respondents reported a financial loss, compared with five percent in 2011; and
  - nine percent in 2010 and seven percent in 2011 reported both sending their personal details and having experienced a financial loss.
- Dating scams, although the least likely to be received, were the single category most likely to result in a financial loss or the disclosure of personal details by those who had been exposed to this scam type—as reported by respondents in both the 2010 and 2011 surveys.
- The median amount lost to scams was $1,065 in 2010 and $700 in 2011. With outliers removed (in both years there were some very large loss figures from respondents who appeared to have misunderstood the question), a total financial loss of $135,874 was reported in 2010 and a total loss of $6,999,718 in 2011.
- The top two reasons given for not responding to scam invitations was 'something was not quite right with the offer or invitation' (46% of the total sample in 2010 and 52% in 2011) and 'had received similar offers before and thought they were scams' (45% in 2010 and 49% in 2011).

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 disclosed their gender (96% in 2010 and 99% in 2011), 21 percent of females reported victimisation in 2010 and 18 percent in 2011. For male respondents, 16 percent reported victimisation in 2010 and 21 percent in 2011.
- In 2010, those in the 45 to 54 year old age group reported the highest percentage of victimisation (29% of total respondents within that age category). In 2011, those aged 65 years and over reported the highest levels of victimisation (23% of total respondents within that age category), closely followed by the 17 years and under category (23%).
- In 2010, those respondents earning $20,000 to $40,000 per annum reported the highest percentage of victimisation (40% of total respondents within that income category). In 2011, those earning less than $20,000 had the highest percentage of victimisation (29% 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 2010, 72 percent of the total sample reported a scam to at least one person or organisation compared with only 65 percent in 2011.
- Family and friends were the most common recipients of scam complaints, with 42 percent of the total sample reporting to this category in 2010 and 36 percent in 2011.
- The most common reasons provided for not reporting scams were 'didn't think anything would be done' (29% of the total sample in 2010 and 27% in 2011), 'unsure of which agency to contact' (25% in 2010 and 39% in 2011) and 'not worth the effort' (22% in 2010 and 25% in 2011). The 2011 survey included a new response category 'received too many to report', which was selected by 25 percent of the total sample.
- The 2011 survey included a new question about reasons for reporting scams. The top four responses selected were 'wanted to prevent others from being scammed' (41% of the total sample), 'knew it was the right thing to do' (30%), 'to assist in the investigation of an offence' (25%) and 'desired the apprehension of offenders' (25%).

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 2010, the top three scam types to be considered a crime by respondents were advance fee fraud (74%), phishing (73%) and lottery scams (61%).
- The top three scam types to be considered a crime by respondents to the 2011 survey were phishing (80%), advance fee fraud (77%) and work from home scams (66%).

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:

- increasing awareness about hidden fraud, where victims may not be aware that they have been scammed;
- the use of new technologies that may be misused by scammers;
- changing the culture where information is freely provided to third parties; and
- how to recognise scams and who to report them to, coinciding with a message aimed at reducing the stigma associated with falling victim to a scam.

Introduction

The purpose of this paper is to report findings from the 2010 and 2011 ACFT surveys, in order to provide an overall picture of the nature of consumer fraud in Australasia.

Australasian Consumer Fraud Taskforce

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

Since 2006, the AIC has conducted annual surveys to assess consumer fraud experiences (see Smith (2007) for the results of the pilot study conducted in 2006, Smith & Akman (2008) for the 2007 survey results, and Budd & Anderson (2011) for the results of the 2008 and 2009 surveys). The surveys reported in this paper ran for approximately three months each between January and March in 2010 and 2011, which encompassed the annual Fraud Week conducted by the Taskforce.

Defining scams

The Australian Bureau of Statistics (ABS 2008: 5) defines a scam 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.

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. Seven common types of consumer frauds were explored in the 2010 and 2011 ACFT survey,

namely—advance fee fraud, dating scams, financial advice scams, inheritance scams, lottery scams, phishing and work from home 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).

The hidden nature of consumer fraud

Incidents of consumer fraud may not be reported for a number of reasons. For example, victims may not be aware that they have been scammed, not be aware of law enforcement interest, feel responsible for becoming a victim, or not know to whom the scam should be reported. Over one-third (37%) of the 2009 ACFT survey respondents reported that they had received a scam invitation to a formal agency. Of those who responded to the scam (54%), most reported it to an office of fair trading or consumer affairs agency (34%), to the business involved (26%) or to the police (14%). In addition, 42 percent of all respondents and half (50%) of those who responded to the scam told their family or friends about the scam invitation (Budd & Anderson 2011). The AIC's 2010 and 2011 annual surveys are the first to explore reasons for not reporting victimisation.

One of the challenges currently facing criminal justice policymakers is a lack of knowledge about the extent of consumer frauds. This can be attributed to a low reporting rate, the multitude of state and federal government agencies within Australasia that collect this type of data, the way data are recorded and a lack of resources to enable victimisation surveys to be undertaken. For example, scam recipients and victims may report matters to policing agencies, state and territory consumer protection agencies, the ACCC, the Australian Communications and Media Authority, the Australian Securities and Investments Commission or the Australian Tax Office. Other organisations that may receive complaints about scams include banks and financial institutions, online trading and auction sites, as well as social media sites (ACCC 2012b).

It is noted that the Australian Government is planning to undertake a feasibility study in relation to establishing a national reporting facility for crime that takes place online, such as consumer frauds that are distributed using email, websites and other social media (DPMC

Table 1 Common consumer scams

Advance fee fraud/ Nigerian 419 scams	Advance fee frauds or Nigerian 419 scams have existed throughout history and have adapted to advances in technology. Generally, these scams are communicated by email or letter seeking assistance to transfer a large amount of money overseas. These are the most commonly complained about scams in Australia, according to the ACCC
Dating/social networking scams	Dating and social networking scams may 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 are offered through cold calling by scammers operating from overseas who pretend to share 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
Inheritance scams	Inheritance scams are usually sent by scammers posing as 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 target person a large inheritance
Lottery scams	A lottery scam may be delivered by email, text message or pop-up screen on a website, falsely claiming the recipient 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 being sent by SMS
Work from home scams (money laundering)	Working 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

Source: ACCC 2012a, 2011a; AIC ACFT Survey 2010

2011). Smith (2008) argued that a national reporting centre would allow for the development of an improved response in relation to prevention and intervention. It would also allow for the collation of information domestically, which could then be shared with the international community. Data collected by a national reporting centre could be used to raise awareness of victimisation, enable resources to be allocated more effectively and appropriately, evaluate intervention and prevention strategies, compile intelligence that can be used for policing and prevention activities, provide feedback to those who have detected and reported matters, enable information on new crime methodologies to be shared with others at risk of similar types of activities and compile statistical data for trend identification, data mining and analysis (Smith 2008).

Opportunities for fraud

Levi and Smith (2011) discuss the impact that the global financial crisis may have had on the nature and extent of fraud. Although not focusing primarily on consumer fraud, they note that opportunity often plays a role in scams. For example, with the increase in unemployment following the global financial crisis (by 1.3 percentage points in Australia), there is greater opportunity for employment scams (Levi & Smith 2011). Similarly, the recent strength in the Australian dollar may lead to greater consumer fraud exposure as shoppers turn to the internet to buy goods from overseas. The high value of the dollar would also make Australians an attractive target to scammers.

The development of new technologies also provides opportunities for scammers. For example, there have been recent media reports about the use of malicious quick response codes (images which, when scanned by a smartphone, link to a website or other digital content) being used by scammers. Examples of scams that may be distributed using quick response codes include the installation of malicious applications that send premium SMS without consent, obtain personal information or direct users to a phishing website (Shanklin 2011; Vuong, 2011). The ability to differentiate between legitimate and malicious quick response codes is particularly problematic and scammers may even use stickers to cover authentic codes with their own.

Scammers have also been found to take advantage of opportunities that may initially conceal their intentions. For example, dating websites provide a forum for strangers to contact each other and it is not unusual to receive a message from someone that is unknown to the potential victim. The victim may be groomed for some time before the scammer requests financial assistance. In 2011, dating and romance scams were one of the least reported to the ACCC, making up just 2.5 percent of complaints, however, this scam type was the most likely to result in financial loss, with 48 percent of complainants reporting they had lost money (ACCC 2011b). The ACCC has attempted to address the risk of romance scams by launching guidelines for dating websites. These guidelines include providing scam warnings and information, vetting and checking procedures to detect fraudulent profiles and effective complaint handling mechanisms (ACCC 2012c).

The popularity of goods and services also provides opportunities for scammers. For example, phishing attempts use the name of popular banks and financial institutions, social media sites and auction sites. In 2011, a joint warning was issued by SCAMwatch, Microsoft and the Australian Communications and Media Authority that there has been an increase in scammers calling individuals and claiming to be from a popular software vendor's computer support centre (ACCC 2011c). Typically, these scams involve obtaining remote access to a victim's computer, during which the scammer will claim that there is a virus or other problem that requires technical support at a cost. A victim may also have malicious software installed by the scammer, resulting in further inconvenience and cost.

Cost of consumer fraud

It is difficult to estimate the cost of consumer fraud (also known as mass marketing or personal fraud), particularly due to the inconsistent way scams are reported to various organisations.

One way to overcome the limitations of relying on official data to determine the extent of scams is to conduct victimisation surveys. The ABS conducted a *Personal Fraud* survey in 2010–11, in which approximately 26,405 respondents were surveyed. The ABS estimated that in the 12 month period prior to interview, 6.4 million Australians aged 15 years and over were exposed to a scam and 514,500 became scam victims, representing 35.8 and 2.9 percent of the population respectively. Scams included in this survey (and the victimisation rate) were lotteries (0.6% of Australians victimised), pyramid schemes (0.2%), fake offers from a bank (0.4%), fake offers from a business (0.8%), chain letters (0.1%), requests to send details (0.4%) and other scams, such as door-to-door sales and fraudulent repair work (2.9% each; ABS 2012). Overall, $1.4b was estimated to have been lost due to scams as well as other personal frauds, such as identity theft and credit card fraud, over the 12 month period (ABS 2012).

Ross and Smith (2011) surveyed Victorians who had been identified by the Australian Transaction Reports and Analysis Centre as having sent money to Nigeria in the 12 months to 31 March 2008. Of the 59 percent of respondents who were identified as being victims of advance fee fraud, the average amount sent overseas was $12,000. However, costs were not only financial, with 43 percent of victims reporting emotional trauma, 40 percent reporting a loss of confidence in other people and 12 percent experiencing marital or relationship problems as a result of victimisation. Financial hardship was also reported by 54 percent of victims (Ross & Smith 2011).

The ACCC is one of the Australian Government agencies that collect reports of consumer fraud from the public. These reports are accepted by telephone or online at the SCAMwatch website (www.scamwatch.gov.au). Scam reports are used to assist in monitoring scam trends and identifying new or emerging scams so that appropriate action, such as public education, can be undertaken (ACCC 2012d). The total amount reported to the ACCC as lost due to scams during 2011 was $85.6m (ACCC 2012a).

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 influences reporting of scams.

Each year between 1 January and 31 March, an anonymous online survey hosted by the AIC is used to collect data. This timeframe was chosen to correspond with recent ACFT fraud awareness campaigns, which operated from 1 to 7 March in 2010 and from 7 to 13 March in 2011, 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 by a large public audience and does not involve any administration costs such as postage or interview expenses. It also allows respondents to remain anonymous, which was considered advantageous as the survey asked questions about personal experience and possible victimisation.

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

Survey questions

The surveys contained a mixture of closed responses and open-ended, qualitative questions about respondent's exposure to, and victimisation from, consumer scams (see *Appendix A* and *Appendix B*). These questions were developed in consultation with 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; and
- dating 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 was a substantial change in the wording for the 2011 survey compared with the 2010 survey as respondents were asked about 'scams' rather than 'unsolicited contacts'. Additional questions were also posed in relation to:

- how many times scams were received by each method over the previous 12 month period;
- why respondents reported incidents to a formal agency; and
- whether respondents had reported any scams on behalf of anyone else.

There were also some changes and additions to the response categories provided for several of the forced-choice questions.

Media coverage

A search of media databases for the periods 1 January 2010 to 31 March 2010 and 1 January 2011 to 31 March 2011 indicated that there was greater coverage of the survey in the media during the latter period. Only one media article that invited readers to participate in the survey and provided a relevant link was identified in 2010—*Counter-attack on Online Fraud* was published in The Australian Financial Review on 1 March 2010, which coincided with the start of fraud week. By comparison, 13 newspaper articles were identified in 2011. These were:

Kalgoorlie Miner 2011. Scam survey seeks goldfields information. *Kalgoorlie Miner* 8 January

Mandurah Coastal Times 2011. Scam victims asked to complete short survey for Fraud Taskforce. *Mandurah Coastal Times* 19 January

Clitheroe P 2011. Beware of scams on email. *Geelong Advertiser* 24 January

Clitheroe P 2011. Don't be fooled by email scammers. *The Observer* 25 January

Clitheroe P 2011. Email scams—be on guard and just press delete button. *Sunshine Coast Daily* 25 January

The Morning Bulletin 2011. Use your sense on recognising email scams. *The Morning Bulletin* 25 January

Clitheroe P 2011. Best defence is common sense. *North Shore Times* 26 January

Kalgoorlie Miner 2011. Email scams mean big business. *Kalgoorlie Miner* 26 January

Melbourne Yarra Leader 2011. Don't get caught in the net. *Melbourne Yarra Leader* 31 January

Brimbank Leader 2011. Don't get caught in the net. *Brimbank Leader* 1 February

Cranbourne Leader 2011. Email scammers cast their net for victims. *Cranbourne Leader* 2 February

Noosa Journal 2011. Internet scams go global. *Noosa Journal* on 4 February

Ballina Shire Advocate 2011. Watch out for online scams. *Ballina Shire Advocate* 17 March

Radio interviews conducted with AIC staff in 2011 also promoted the survey and sought respondents. These included *Afternoon Live* on ABC News 24 on 8 March 2011 and *Weekends with George Moore and Paul B Kidd* on 2UE on 13 March 2011.

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 33 additional newspaper articles that discussed consumer fraud and were published between 1 to 7 March 2010 (refer to *Appendix C*). For the campaign that ran from 7 to 13 March 2011, 47 additional newspaper articles were identified (refer to *Appendix D*).

Limitations of the surveys

The 2010 and 2011 AIC surveys experienced the same methodological constraints as those identified in previous years (see Budd & Anderson 2010; 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. 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 surveys over the phone on the respondent's behalf.

It can also be difficult to measure fraud incidents within a given timeframe as it is not always easy to determine when fraud occurs. This is due to the time lapse between when scams are received or carried out, when they are identified by the victim and when they are subsequently reported (if indeed they are). The reference period for the 2010 and 2011 AIC online surveys 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.

Further, while the findings can be used to provide insight into the experiences of individuals in relation to exposure to, victimisation from and reporting of consumer fraud scams, identifying reliable trends over time cannot be confidently reported from the survey data as the 2010 survey questions were different from the 2011 survey. As a result, the survey results cannot provide a robust measurement of consumer fraud victimisation rates in Australasia, nor of the success of the 2010 or 2011 Fraud Awareness weeks. The results are also unable to identify whether the two campaigns increased people's awareness of consumer frauds or scams.

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.

The following sections present the key results from the 2010 and 2011 ACFT surveys.

The 2010 consumer fraud survey results

Online offensive—Fighting fraud online

The ACFT's 2010 annual education and awareness campaign ran from 1 to 7 March. The theme of the 2010 campaign was *Online Offensive—Fighting Fraud Online.* It aimed to raise awareness of online consumer fraud in Australasia and to alert the increasing number of people using the Internet about scams, which may be more prevalent as more people gain online access (ACCC 2011d).

Sample characteristics

Between 1 January and 31 March 2010, 249 people responded to the survey hosted on the AIC's website (www.aic.gov.au). One respondent was removed from the analysis, having submitted an incomplete response. A further two respondents were removed as they did not reside in Australia or New Zealand. This left 246 responses that formed the sample and were subject to analysis. Compared with previous years, the 2010 consumer fraud survey received substantially fewer responses (2010 n=246; 2009 n=692, 2008 n=919). This decline may be due to the lack of media coverage surrounding the 2010 survey.

Eighty-four percent (n=206) of respondents reported that they completed the survey as a member of the public. A further 10.6 percent (n=26) of respondents were reportedly employed by a government agency, but only 3.3 percent (n=8) identified that they were employed by ACFT-member government agencies. Two (0.8%) respondents identified that they were members of a policing agency.

Links provided on websites was the most common way respondents were directed to the survey, with 39 percent (n=96) following the links from a government website and 27.2 percent (n=67) directed from the SCAMwatch website. Word of mouth and the media accounted for 6.1 percent (n=15) and 4.5 percent (n=11) of respondents respectively.

Nineteen percent (n=47) of respondents were aware of the 2010 ACFT fraud awareness campaign and 9.8 percent (n=24) were aware of the ACFT campaigns held in previous years. A small group of respondents had participated in previous ACFT fraud surveys—12 (4.9%) in 2009; seven (2.8 %) in 2008; and five (2%) in 2007 and 2006.

In the eight weeks prior to the 2010 campaign, 124 participants completed the survey, averaging 15.5 responses per week; 56 participants completed the survey during the week-long campaign; while the remaining 66 participants completed the survey in

the four weeks following the campaign, averaging 16.5 responses per week. It would therefore seem reasonable to conclude that the campaign had a positive impact on participation rates, along with the associated media coverage published at the start of the week-long campaign.

Demographics

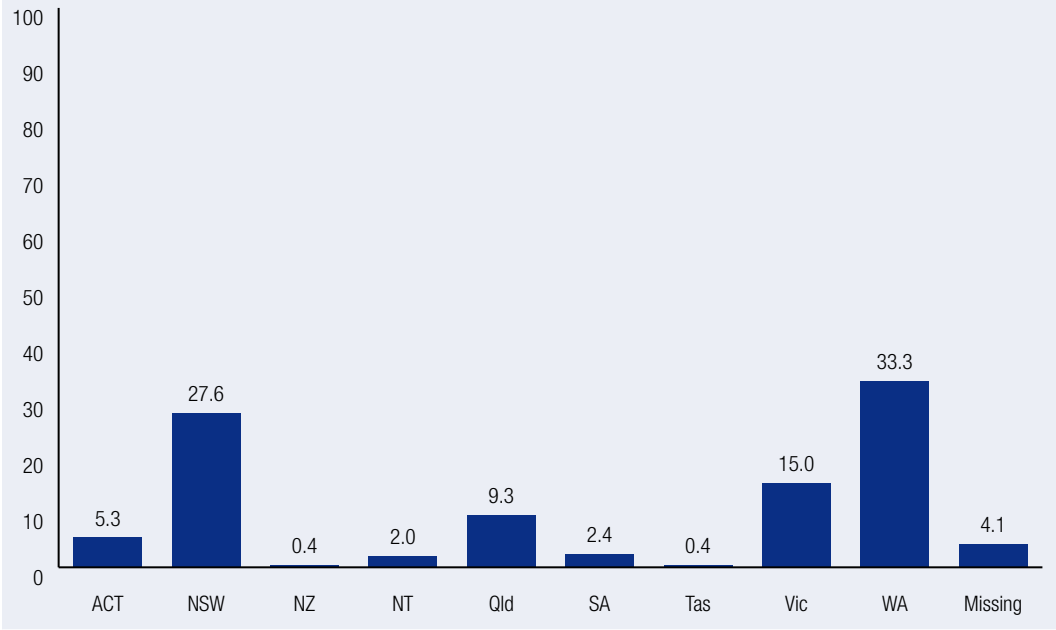
Table 2 shows the breakdown of respondents by age group. Over half of the respondents (55.3%, n=136) were aged over 45 years. Gender was distributed fairly evenly, with 53.7 percent (n=132) of respondents identifying as female and 41.9 percent (n=103) as male; 4.5 percent (n=11) of respondents did not answer this question.

Table 2 Respondents by age, 2010

Age category (yrs)	n	%
17 and under	9	3.7
18–24	22	8.9
25–34	34	13.8
35–44	36	14.6
45–54	71	28.9
55–64	43	17.5
Over 65	22	8.9
Missing	9	3.7
Total	246	100.0

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Figure 1 Respondents by region, 2010 (%)



Note: Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

As shown in Figure 1, the majority of respondents came from Western Australia (33.3%, n=82), New South Wales (27.6%, n=68) and Victoria (15%, n=37). Only one respondent (0.4%) resided in New Zealand. Tasmania (0.4%, n=1), the Northern Territory (2%, n=5) and South Australia (2.4%, n=6) were the least represented states and territories in Australia.

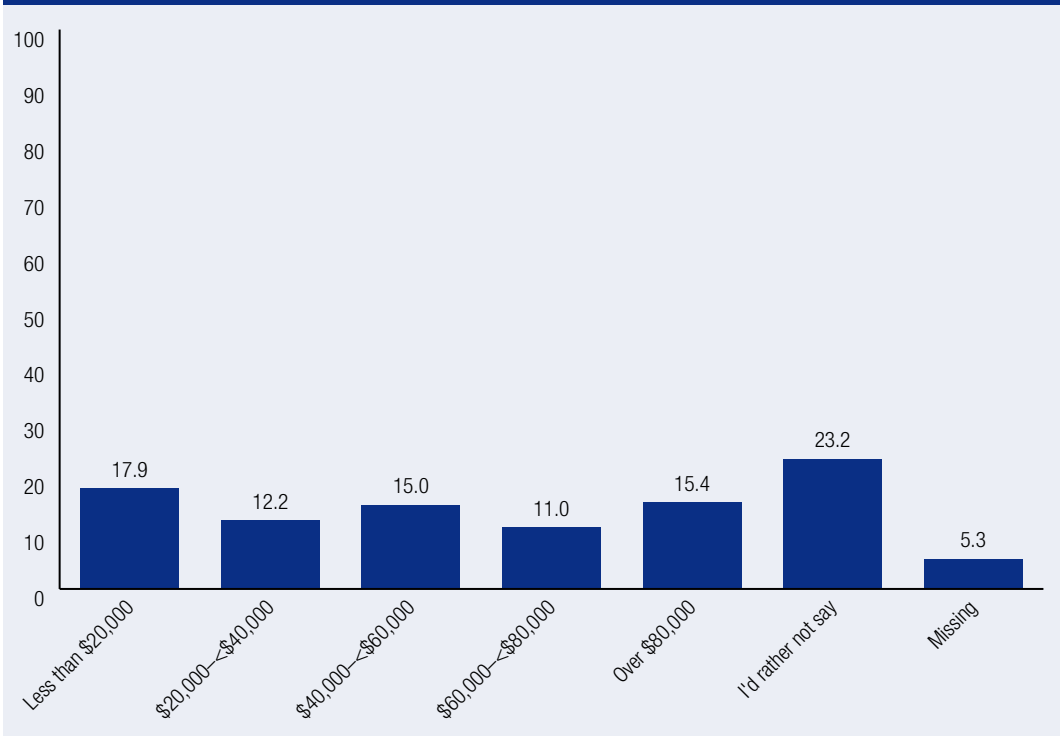
There was a fairly even distribution across the reported annual income levels of respondents, with 17.9% (n=44) of respondents earning less than $20,000 and 15.4% (n=38) of respondents earning more than $80,000 per annum (see Figure 2). Almost one-quarter of respondents (23.2%, n=57) advised that they would rather not disclose their income level, while a further 5.3 percent (n=13) did not respond to this question.

Receiving scams

In 2010, 89 percent (n=219) of survey respondents had received at least one scam invitation in the previous 12 months. Table 3 shows the number and percentage of respondents who received at least one invitation by fraud type. It is noted that respondents may have received invitations for multiple scams. The most commonly received scam types were lottery scams (received by 63% of the sample who received a scam invitation), followed by advance fee frauds (received by 57.5% of the sample who received a scam invitation). The least commonly received scam type was dating scams, received by only 21 percent of the sample who received a scam invitation.

Table 4 shows the number and percentage of respondents by the various types of delivery methods. Email was the most common scam delivery method, with over three-quarters (75.6%) of respondents receiving an invitation via this medium and 84.9 percent of respondents who had received at least one scam invitation solicited this way. Respondents may have received scam invitations through multiple methods of delivery.

Figure 2 Respondents by annual income, 2010 (%)



Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Table 3 Scam invitation received by type, 2010

Scam type	Received scam invitation (n)	Received a scam invitation (%) (n=219)	Total sample (%) (n=246)
Lottery scams	138	63.0	56.1
Advance fee fraud	126	57.5	51.2
Inheritance scams	100	45.7	40.7
Phishing	123	56.2	50.0
Financial advice scams	65	29.7	26.4
Work from home scams	115	52.5	46.8
Dating scams	46	21.0	18.7
Other	88	40.2	35.8

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Table 4 Scams by delivery method, 2010

Method of delivery	Received scam invitation (n)	Received a scam invitation (%) (n=219)	Total sample (%) (n=246)
Mail	44	20.1	17.9
Email	186	84.9	75.6
Phone	36	16.4	14.6
SMS/Mobile	29	13.2	11.8
Internet	27	12.3	11.0
Other	11	5.0	4.5

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Responding to scams

Overall, 72 survey participants responded to a scam during the 12 months prior to the survey, representing 32.9 percent of those who received a scam invitation and 29.3 percent of the total sample. Responding positively included requesting further information, as well as providing personal details or losing money.

Forty-three participants reported that they sent their personal details in response to at least one scam invitation (17.5% of the total sample and 19.6% of the sample who had received a scam invitation), while 27 participants lost money as the result of a scam (11% of the total sample and 12.3% of the sample who had received a scam invitation). Of these, 23 participants had lost money as well as sent their personal details; therefore, 47 participants (19.1% of the total sample and 21.5% of the sample who had received a scam invitation) had suffered a financial loss and/or loss of personal details. Tables 5 and 6 show the number of respondents who provided personal details or lost money to each 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. It is noted that some respondents provided personal details and/or lost money as the result of multiple scams.

Participants were least likely to disclose personal details or lose money as the result of advance fee fraud, inheritance scams or phishing; however, these were reportedly three of the top five scam invitations that respondents reported receiving in the previous 12 months. Dating scams, although the least likely to be received by participants (see Table 3), were among the most likely to lead to the loss of personal details or a financial loss.

Table 5 Loss of personal details by scam type, 2010

Scam type	Provided personal details (n)	Received a scam invitation (%) (n=219)	Total sample (%) (n=246)	Received an invitation to that type of scam (%)
Lottery scams	6	2.7	2.4	4.3
Advance fee fraud	4	1.8	1.6	3.2
Inheritance scams	1	0.5	0.4	1.0
Phishing	4	1.8	1.6	3.3
Financial advice scams	4	1.8	1.6	6.2
Work from home scams	6	2.7	2.4	5.2
Dating scams	9	4.1	3.7	19.6
Other	23	10.5	9.3	26.1

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Table 6 Loss of money by scam type, 2010

Scam type	Suffered a financial loss (n)	Received a scam invitation (%) (n=219)	Total sample (%) (n=246)	Received an invitation to that type of scam (%)
Lottery scams	4	1.8	1.6	2.9
Advance fee fraud	1	0.5	0.4	0.8
Inheritance scams	1	0.5	0.4	1.0
Phishing	1	0.5	0.4	0.8
Financial advice scams	2	0.9	0.8	3.1
Work from home scams	6	2.7	2.4	5.2
Dating scams	6	2.7	2.4	13.0
Other	14	6.4	5.7	15.9

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Of the 27 respondents who had suffered a financial loss as the result of a scam, 26 disclosed the amount. Amounts lost ranged from $92 to $614,200 (mean=$28,849, median=$1,065). The total amount reportedly sent to scammers by the survey participants was $750,074. However, the highest amount sent, $614,200, was sent overseas in response to a request for financial assistance. This example was reported by a male under the age of 18 years, therefore there is concern as to the accuracy of the report. With this outlier removed, the mean financial loss declined from $28,849 to $5,226.

Most participants did not send money or personal details in their first response to the scammer, with 27 of the 53 (50.9%) respondents who answered the question only providing this after being in contact with the scammer between two and 10 times. Three participants (5.6%) were in contact between 11 and 20 times, seven (13.2%) were in contact more than 20 times and three (5.6%) could not recall how many times they had contacted the scammer before providing the personal details or money.

Participants were asked why they did not respond to scam invitations. Their responses are provided in Table 7. As respondents were allowed to select multiple reasons for not responding, the total exceeds 246. While the majority of participants did not respond due to the characteristics of the scam (eg 49.3% thought the offer seemed too good to be true and 51.1% thought something was not quite right with the offer or invitation), 42 percent identified the invitation as a scam due to media or public source information, highlighting the importance of public awareness campaigns in preventing victimisation. Over half of the participants who had received a scam invitation (50.2%) advised that they

Table 7 Reasons for not responding to scams received, 2010

Reason for not responding	n	Received a scam invitation (%) (n=219)	Total sample (%) (n=246)
Seemed too good to be true	108	49.3	43.9
Had received similar offers before and thought they were scams	110	50.2	44.7
Had seen/heard this was a type of scam in the media or a public source	92	42.0	37.4
Was told it was a scam by someone I knew	24	11.0	9.8
Someone I know has been a victim of a scam before	14	6.4	5.7
Wanted to respond but could not afford to participate	11	5.0	4.5
Something was not quite right with the offer or invitation	112	51.1	45.5
Other	44	20.1	17.9

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Table 8 Victims by age, 2010

Age category (yrs)	n	%	Respondents within that age category (%)
17 and under	1	2.1	11.1
18–24	1	2.1	4.5
25–34	6	12.8	17.6
35–44	5	10.6	13.9
45–54	20	42.6	28.2
55–64	10	21.3	23.3
Over 65	2	4.3	9.1
Missing	2	4.3	22.2

Note: Percentages may not total 100 due to rounding.

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

did not respond as they had received similar offers before and thought they were scams. Along with the finding identified above that some of the most commonly received scams are least likely to elicit a response, it appears that internet users are becoming familiar with the most frequently used techniques used by scammers.

Victim demographics

For the purpose of this report, scam victims were defined as those who had provided scammers with their personal details and/or suffered a financial loss as the result of a scam. Of the 47 reported victims, 28 (59.6%) identified themselves as female and 16 (34%) as male. Three (6.4%) victim respondents declined to reveal their gender. Therefore, of the 235 survey respondents who disclosed their gender, 21.2 percent of the females experienced victimisation compared with 15.5 percent of the male respondents.

Table 8 shows the age groups of victims, as well as the percentage of total respondents within that age category who reported victimisation. Respondents between the ages of 45 to 64 years were most likely to report being a victim of a scam, with 28.2 percent of total respondents aged 45 to 54 years and 23.3 percent of total respondents aged 55 to 64 years reporting that they had lost personal details or suffered a financial loss. Of the reported victims, 42.6 percent were in the 45 to 54 year age category.

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

Table 9 Victims by annual income, 2010

Annual income	n	%	Total respondents within that income category (%)
Less than $20,000	6	12.8	13.6
$20,000–<$40,000	12	25.5	40.0
$40,000–<$60,000	7	14.9	18.9
$60,000–<$80,000	7	14.9	25.9
Over $80,000	7	14.9	18.4
I'd rather not say	5	10.6	8.8
Missing	3	6.4	23.1

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Table 10 Victims by region, 2010

Region	n	%	Total respondents within that region (%)
Australian Capital Territory	1	2.1	7.7
New South Wales	10	21.3	14.7
New Zealand	1	2.1	100.0
Northern Territory	1	2.1	20.0
Queensland	6	12.8	26.1
South Australia	3	6.4	50.0
Tasmania	0	0.0	0.0
Victoria	8	17.0	21.6
Western Australia	15	31.9	18.3
Missing	2	4.3	20.0

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Respondents earning between $20,000 and less than $40,000 per annum were most likely to report being a victim of a scam, with 40 percent of total respondents who had that income level losing personal details or suffering a financial loss. Of the reported victims, over one-quarter (25.5%) were in this income category.

Table 10 shows victims by the region in which they resided, as well as the percentage of total respondents within that region who reported victimisation. Nearly one-third (31.9%) of victims resided in Western Australia, with a further 21.3 percent residing in New South Wales. Half (50%) of the six respondents who resided in South Australia reported falling victim to a scam. The one respondent in New Zealand had also provided personal details or suffered a financial loss as the result of a scam, while the respondent from Tasmania had not.

Reporting scams

The majority of those who had received a scam invitation reported it to at least one other person or organisation (n=178, 81.3% of sample who had received a scam invitation and 72.4% of the total sample). Eight respondents (3.3% of the total sample) could not recall whether they had reported a scam invitation(s). Table 11 shows those organisations or persons that scam invitations were reported to, with respondents permitted to select more than one option. Family and friends were most common recipients of scam complaints, with almost half (46.6%) of the sample who had received a scam invitation reporting to this category. Policing agencies were among the least likely to be reported to, with just 13.2 percent of those who had received a scam invitation selecting this category and 3.2 percent selecting the Australian High Tech Crime

Table 11 Reporting of victimisation by agency, 2010

Organisation or person reported to	n	Received a scam invitation (%) (n=219)	Total sample (%) (n=246)
Family/friends	102	46.6	41.5
Police agencies	29	13.2	11.8
Consumer Affairs or Fair Trading agency	75	34.2	30.5
Australian High Tech Crime Centre	7	3.2	2.8
The business represented (eg bank, eBay etc)	54	24.7	22.0
Internet Service Provider	21	9.6	8.5
Legal aid, a lawyer, or a community legal services clinic	4	1.8	1.6
Unable to recall	8	3.7	3.3
Other	41	18.7	16.7

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Table 12 Reporting of financial loss or loss of personal details by agency, 2010

	Reported a financial loss		Reported loss of personal details	
Organisation or person reported to	n	Reported a financial loss (%) (n=27)	n	Reported loss of personal details (%) (n=43)
Family/friends	14	51.9	22	51.2
Police agencies	8	29.6	14	32.6
Consumer Affairs or Fair Trading agency	10	37.0	19	44.2
Australian High Tech Crime Centre	1	3.7	2	4.7
The business represented (eg bank, eBay etc)	10	37.0	12	27.9
Internet Service Provider	4	14.8	5	11.6
Legal aid, a lawyer, or a community legal services clinic	2	7.4	3	7.0
Unable to recall	1	3.7	1	2.3
Other	7	25.9	10	23.3

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Centre (now Australian Federal Police High Tech Crime Operations).

Twenty-four of the 27 respondents who reported a financial loss (88.9%) and 40 of the 43 respondents who reported loss of personal details (93.0%) reported it to at least one other person or organisation. When friends and family were excluded, 20 respondents (74.1%) reported their financial loss and 35 respondents (81.4%) reported loss of personal details to an external agency. Table 12 shows those organisations or persons victimisation was reported to, with respondents permitted to select more than one option. It is noted that policing agencies received reports from less than one-third of victims (29.6% of those who experienced a financial loss and 32.6% of those who lost personal details).

Reasons for not reporting scam invitations were provided by 141 participants (57.3% of the total sample and 64.4% of the sample who received a scam invitation). It is noted that participants may have reported some scams but not others and had multiple reasons for not reporting, therefore, totals do not add to 246. Reasons for not reporting scam invitations are outlined in Table 13.

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 also provided with a *don't know* option and were permitted to select more than one response. The results are outlined in Table 14. While advance fee fraud and phishing scams were most likely to be considered a crime (by 74.4% and 73.2% of the sample respectively), financial advice and work from home scams were more likely to be considered wrong but not a crime, or just something that happens.

The perceptions of scams by respondents who had provided personal details and/or suffered a financial loss that resulted from that particular type of scam were also explored. Again, it is noted that participants could select more than one response. The results are outlined in Table 15. Dating and phishing scams were most likely to be considered a crime by those who had lost money or personal details (90% and 100% respectively). Least likely to be considered a crime by those who had lost finances or personal details were work from home scams (25%).

Table 13 Reasons for not reporting scams, 2010

Reason for not reporting	n	Received a scam invitation (%) (n=219)	Total sample (%) (n=246)
Not worth the effort	55	25.1	22.4
Didn't think it was illegal	9	4.1	3.7
Unsure of which agency to contact	61	27.9	24.8
Feared I would get into trouble	5	2.3	2.0
Didn't think anything would be done	72	32.9	29.3
Other	36	16.4	14.6

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Table 14 Perceptions of scams by scam type, 2010

Scam type	A crime		Wrong but not a crime		Just something that happens		Don't know	
	n	%	n	%	n	%	n	%
Lottery scams	149	60.6	50	20.3	14	5.7	10	4.1
Advance fee fraud	183	74.4	27	11.0	3	1.2	6	2.4
Inheritance scams	139	56.5	47	19.1	16	6.5	15	6.1
Phishing	180	73.2	23	9.3	7	2.8	8	3.3
Financial advice scams	80	32.5	80	32.5	40	16.3	14	5.7
Work from home scams	63	25.6	83	33.7	51	20.7	17	6.9
Dating scams	112	45.5	66	26.8	20	8.1	13	5.3
Other	110	44.7	26	10.6	7	2.8	37	15.0

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

Table 15 Perceptions of scams by respondents who reported victimisation by scam type, 2010

	A crime		Wrong but not a crime		Just something that happens		Don't know	
Scam type	n	%	n	%	n	%	n	%
Lottery scams (n=7)	4	57.1	1	25.0	0	0.0	1	14.3
Advance fee fraud (n=4)	2	50.0	1	25.0	0	0.0	1	25.0
Inheritance scams (n=2)	1	50.0	0	0.0	0	0.0	0	0.0
Phishing (n=5)	5	100.0	0	0.0	0	0.0	0	0.0
Financial advice scams (n=4)	2	50.0	0	0.0	1	25.0	0	0.0
Work from home scams (n=8)	2	25.0	5	62.5	2	25.0	1	12.5
Dating scams (n=10)	9	90.0	1	10.0	0	0.0	0	0.0
Other (n=25)	16	64.0	4	16.0	1	4.0	2	8.0

Source: ACFT Consumer Fraud Survey 2010 [AIC data file]

The 2011 consumer fraud survey results

Scams: It's personal

The ACFT's 2011 annual information campaign ran from 7 to 13 March. The theme of the 2011 campaign was *Scams: It's Personal*, which aimed to raise awareness of the types and impact of consumer fraud experienced by individuals in Australasia (ACCC 2011e).

Sample characteristics

Between 1 January and 31 March 2011, 1,153 people responded to the survey hosted on the AIC's website (www.aic.gov.au). Eight respondents were removed from the sample as they did not reside in Australia or New Zealand, leaving 1,145 responses that formed the sample that was subject to analysis.

Over three-quarters (76.9%, n=880) of respondents reported that they completed the survey as a member of the public and a further 11.8 percent (n=135) of respondents were also retirees. Thirteen respondents (1.1%) were police, 1.7 percent (n=19) were employed by an ACFT government agency, 0.2 percent (n=2) were employed by an ACFT private sector partner and 7.5 percent (n=86) were employed by another government agency.

Websites were the most popular way respondents were directed to the survey, with government websites referring 520 respondents (45.4%) and the SCAMwatch site referring another 287 respondents (25.1%). The media generated 79 responses (6.9%), posters and pamphlets directed nine respondents (0.8%) and 83 respondents (7.3%) were referred to the survey by an agency. A further 62 respondents (5.4%) found out about the survey through word of mouth.

Almost 20 percent (19.6%, n=224) were aware of the ACFT's campaign and 11.3 percent (n=129) were aware of campaigns that had been run in previous years. Thirty-three respondents (2.9%) had completed to the 2010 survey, 14 (1.2%) had completed the 2009 survey, 10 (0.9%) had completed the 2008 survey and eight respondents (0.7%) had previously completed the 2007 survey.

There was an average of 112.2 responses per week in the nine weeks prior to the 2011 campaign (n=1,010); 74 participants completed the survey during the week-long campaign, while the remaining 61 participants completed the survey in the three weeks following the campaign, averaging 20.3 responses per week. Therefore, it appears that in 2011, the media and web presence surrounding the survey had more of an impact on participation rates than the campaign itself.

Table 16 Respondents by age, 2011		
Age category (yrs)	n	%
17 and under	10	0.9
18–24	75	6.6
25–34	197	17.2
35–44	189	16.5
45–54	280	24.5
55–64	239	20.9
Over 65	148	12.9
Missing	7	0.6
Total	1,145	

Note: Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

A new question was included in 2011, asking why respondents chose to complete the survey. Most respondents (n=652, 56.9%) wanted to assist in research to combat scammers. A further 195 participants (17%) completed the survey because they had recently been scammed; 210 respondents (18.3%) had received scams but had not been scammed and 38 respondents (3.3%) wanted to learn more about scams.

When asked about income, most respondents (n=245, 21.4%) responded that they would rather not disclose their income level and a further 1.5 percent (n=17) did not respond to the question. Almost half of respondents (43.8%, n=502) earned an income somewhere in the middle categories provided ($20,000 to $80,000 per annum), while 16.1 percent (n=184) earned less than $20,000 and 17.2 percent (n=197) earned in excess of $80,000 per annum (see Figure 4).

Demographics

Females were overrepresented, comprising 59.3 percent of the sample (n=679) compared with males, who made up 39.6 percent of the sample (n=453). Thirteen respondents (1.1%) did not disclose their gender.

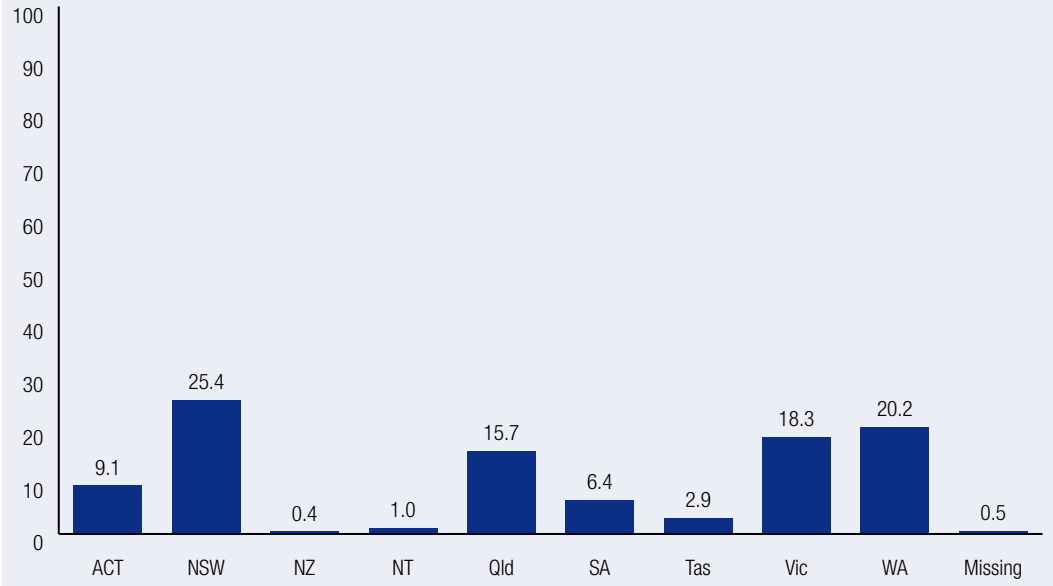
Table 16 shows the breakdown of respondents by age group. Again, those aged over 45 years made up over half (58.3%, n=667) of respondents.

As shown in Figure 3, most respondents resided in New South Wales (25.4%, n=291), Western Australia (20.2%, n=231), Victoria (18.3%, n=210) and Queensland (15.7%, n=180). Five respondents (0.4%) resided in New Zealand. South Australia (6.4%, n=73), Tasmania (2.9%, n=33) and the Northern Territory (1%, n=12) were the least represented states and territories in Australia.

Receiving scams

Of the 1,145 survey participants in 2011, 1,077 (94.1%) had received at least one scam invitation. The number and percentage of respondents who had received at least one scam invitation and the type of invitation received is shown in Table 17. Respondents may have received invitations for more than one scam type. The most common type of scams received, reported by over half (56.6%) of the survey participants, were lottery scams. This was closely followed by 'other' scams (received by 48.6% of survey participants and 51.7% of those who had received a scam invitation). The least likely type of scam invitation reported to have been received remained dating scams, received by 120 of the survey respondents, representing 11.1 percent of the sample who had received a scam invitation and 10.5 percent of the total sample.

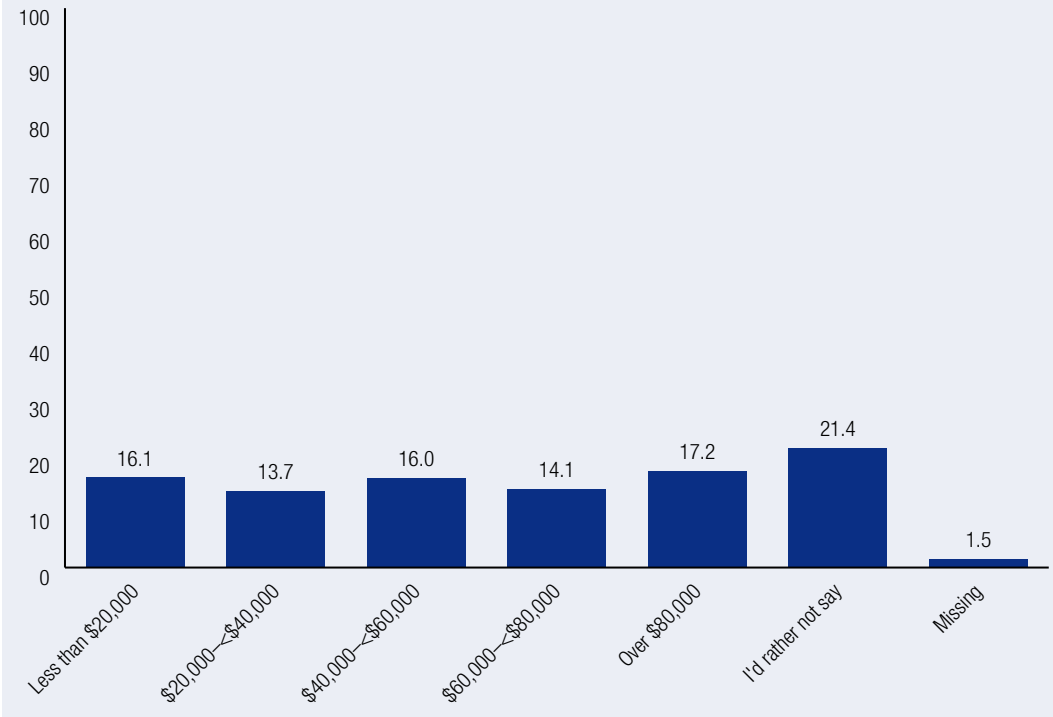
Figure 3 Respondents by region, 2011 (%)



Note: Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Figure 4 Respondents by annual income, 2011 (%)



Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Table 17 Type of scam invitation received, 2011

Scam type	Received a scam invitation (n)	Received a scam invitation (%) (n=1,077)	Total sample (%) (n=1,145)
Lottery scams	648	60.2	56.6
Advance fee fraud	464	43.1	40.5
Inheritance scams	354	32.9	30.9
Phishing	466	43.3	40.7
Financial advice scams	236	21.9	20.6
Work from home scams	469	43.5	41.0
Dating scams	120	11.1	10.5
Other	557	51.7	48.6

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Table 18 Scam delivery method, 2011

Method of delivery	Received a scam invitation (n)	Received a scam invitation (%) (n=1,077)	Total sample (%) (n=1,145)
Mail	215	20.0	18.8
Email	763	70.8	66.6
Telephone	442	41.0	38.6
SMS	168	15.6	14.7
Internet site/social networking	150	13.9	13.1
Other	78	7.2	6.8

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Details of the types of delivery methods by which respondents reported receiving scams are provided in Table 18. It is noted that participants may have received more than one scam invitation, therefore, multiple responses are recorded. Email remained the most popular delivery method, with 70.8 percent of respondents who had received a scam invitation receiving at least one invite this way. However, compared with the previous year's results, the percentage of the total sample who received an invite by email declined from 75.6 percent in 2010 to 66.6 percent in 2011. The percentage of the total sample who received an invitation using the internet or social networking site increased from 11 percent in 2010 to 13.9 percent in 2011. The use of telephone and SMS to deliver scams was captured differently in the 2010 and 2011 surveys, therefore making comparison difficult.

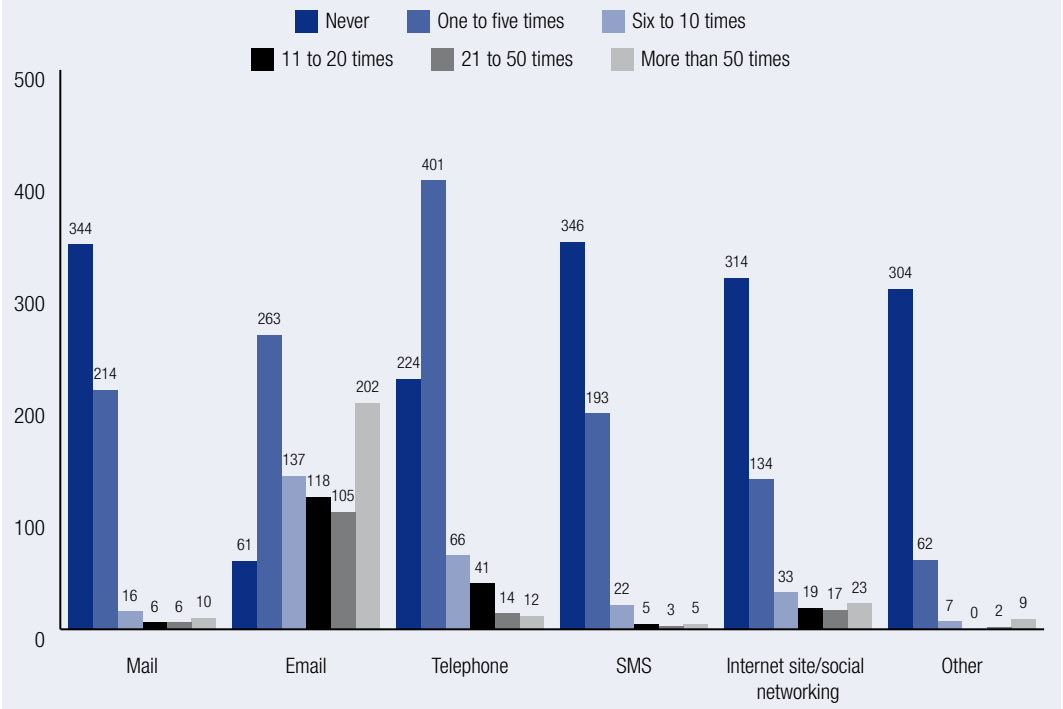
The 2011 survey included a new question asking respondents how many times over the previous 12 months they had received scams by each delivery method (see Figure 5). The results indicate that email is not only the most common scam delivery method, but also that participants received multiple scams in this way.

Responding to scams

During the 12 months prior to the survey, over one-quarter (n=327, 28.6%) of the respondents answered a scam invitation by way of requesting further information, providing personal details or suffering a financial loss. This represented 30.4 percent of those who had received a scam invitation during the 12 month period.

Compared with the results of the 2010 survey, a lower proportion of survey participants were victimised in relation to scams in 2011. Twenty percent of the sample who received an invitation

Figure 5 Scams received by delivery method, 2011 (n)



Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Table 19 Loss of personal details to a scam by scam type, 2011

Scam type	Provided personal details (n)	Received a scam invitation (%) (n=1,077)	Total sample (%) (n=1,145)	Received an invitation to that type of scam (%)
Lottery scams	32	3.0	2.8	4.9
Advance fee fraud	11	1.0	1.0	2.4
Inheritance scams	6	0.6	0.5	1.7
Phishing	24	2.2	2.1	5.2
Financial advice scams	8	0.7	0.7	3.4
Work from home scams	16	1.5	1.4	3.4
Dating scams	17	1.6	1.5	14.2
Other	80	7.4	7.0	14.4

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

sent their personal details, suffered a financial loss or had both occur in response to at least one a scam (n=215, 18.8% of the total sample). By comparison, in 2010, these proportions were 21.5 percent of the sample who had received a scam invitation and 19.1 percent of the total sample. Ninety participants (8.4% of the sample who received a scam invitation and 7.9% of the total sample) sent their personal details only; 51 participants (4.7% of the sample who received a scam invitation and 4.5% of the total sample) suffered a financial loss only and 74 participants (6.9% of the sample who received a scam invitation and 6.5% of the total sample) lost money as well as sent their personal details.

Table 20 Loss of money to a scam by scam type, 2011

Scam type	Suffered a financial loss (n)	Received a scam invitation (%) (n=1,077)	Total sample (%) (n=1,145)	Received an invitation to that type of scam (%)
Lottery scams	17	1.6	1.5	2.6
Advance fee fraud	15	1.4	1.3	3.2
Inheritance scams	6	0.6	0.5	1.7
Phishing	10	0.9	0.9	2.1
Financial advice scams	12	1.1	1.0	5.1
Work from home scams	14	1.3	1.2	3.0
Dating scams	12	1.1	1.0	10.0
Other	70	6.5	6.1	12.6

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

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 19 and 20. 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. Comparing the 2010 survey results to the 2011 responses, it appears that the type of scams that people are likely to fall victim to differs from year to year. For example, 3.4 percent of the sample who received a financial advice or work from home scam invitation sent their personal details in response, while the respective proportions in 2010 were 6.2 percent and 5.2 percent. While victims were less likely to lose personal details in response to financial advice scams in 2011, they were more likely to suffer a financial loss, as reported by 5.1 percent of those who received an invitation for this type of scam in 2011, compared with 3.1 percent in 2010. 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, however this was less pronounced when compared with the 2010 results, with 14.2 percent of the sample who received a dating scam invitation reporting the loss of personal details, compared with 19.6 percent in 2010 and 10 percent reporting a financial loss, compared with 13 percent in 2010.

Of the 125 victims who reported having suffered a financial loss, 117 (93.6%) disclosed the amount. This reportedly ranged from $20 to $200,000,000. With two values removed ($200,000,000 reportedly lost due to a lottery scam and $16,500,000 lost due to a consumer scam by a respondent whose income was less than $20,000 per annum), the reported financial loss totalled $6,999,718, ranging from $20 to $5,000,000 (mean=$60,867.11, median=$700).

Participants were able to select multiple responses when asked why they did not respond to scam invitations. Their responses are provided in Table 21. The most common reasons for not responding to scams included something being not quite right with the offer or invitation (reported by 52% of the total sample), having received similar offers before and thought they were scams, (49.4% of the total sample), or having seen or heard that it was a type of scam in the media or public source (47.5% of the total sample). When compared with the 2010 results, it appears that the role of the media and public source information in creating awareness about scams has improved, with 50.5 percent of the sample who received an invitation realising it was a scam due to the media's influence in 2011, compared with 42 percent in 2010. Only 2.3 percent (n=26) of the sample received a scam that they wanted to respond to but could not afford to participate.

Victim demographics

Of the 215 victims who had lost personal details or suffered a financial loss as the result of the scam, 121 (56.3%) were female and 93 (43.3%) were male; one respondent (0.5%) declined to answer. Therefore, 17.8 percent of the 679 female respondents experienced victimisation, compared with 20.5 percent of the 453 males who participated in the survey and disclosed their gender.

The age of victims, including the percentage of total respondents within that age category who reported being a victim, is displayed in Table 22. Although the small number of respondents (and victims) who completed the 2010 survey makes comparison difficult, it is noted that the 18–24 years and over 65 years age groups reported a substantially higher proportion of victims in 2011 compared with the previous year, while the proportion of victims in the 45–54 year age category dropped from 42.6 percent in 2010 to 27 percent in 2011.

Table 23 shows the annual income levels of victims, as well as the percentage of total respondents within that income category who reported victimisation. Interestingly, the proportion of people reporting victimisation decreased as their income increased, with lower income earners more likely to report victimisation. One-quarter (24.7%, n=53) of victims reportedly earned less than $20,000 per annum. These results differ from the results of the previous

Table 21 Reasons for not responding to scams, 2011

Reason for not responding	n	Received a scam invitation (%) (n=1,077)	Total sample (%) (n=1,145)
Seemed too good to be true	523	48.6	45.7
Had received similar offers before and thought they were scams	566	52.6	49.4
Had seen/heard this was a type of scam in the media or a public source	544	50.5	47.5
Was told it was a scam by someone I knew	148	13.7	12.9
Someone I know has been a victim of a scam before	81	7.5	7.1
Wanted to respond but could not afford to participate	26	2.4	2.3
Something was not quite right with the offer or invitation	595	55.2	52.0
Offer was identified as spam/unsafe by internet filter	271	25.2	23.7
Other	137	12.7	12.0

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Table 22 Victims by age, 2011

Age category (yrs)	n	%	Total respondents within that age category (%)
17 and under	0	0.0	0.0
18–24	17	7.9	22.7
25–34	36	16.7	18.3
35–44	33	15.3	17.5
45–54	58	27.0	20.7
55–64	36	16.7	15.1
Over 65	35	16.3	23.6

Note: Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Table 23 Victims by annual income, 2011

Annual income	n	%	Total respondents within that income category (%)
Less than $20,000	53	24.7	28.8
$20,000–<$40,000	37	17.2	23.6
$40,000–<$60,000	38	17.7	20.8
$60,000–<$80,000	24	11.2	14.8
Over $80,000	29	13.5	14.7
I'd rather not say	31	14.4	12.7
Missing	3	1.4	17.6

Note: Percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Table 24 Victims by region, 2011

Region	n	%	Total respondents within that region (%)
Australian Capital Territory	9	4.2	8.7
New South Wales	56	26.0	19.2
New Zealand	0	0.0	0.0
Northern Territory	3	1.4	25.0
Queensland	40	18.6	22.2
South Australia	14	6.5	19.2
Tasmania	10	4.7	30.3
Victoria	36	16.7	17.1
Western Australia	47	21.9	20.3

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

year. In 2011, the highest proportion of victims earned less than $20,000, while in 2010, this income category had the lowest proportion of victims.

Table 24 shows victims by the region in which they resided, as well as the percentage of total respondents within that region who reported victimisation. Most victims resided in New South Wales (n=56, 26% of the sample who reported victimisation), Western Australia (n=47, 21.9% of the sample who reported victimisation) and Queensland (n=40, 18.6% of the sample who reported victimisation). Although only three victims resided in the Northern Territory (1.4% of the sample who reported victimisation), one-quarter (25%) of the 12 respondents in this jurisdiction provided personal details or suffered a financial loss as the result of a scam. The 10 victims residing in Tasmania only represented 4.7 percent of the total victims, although they made up 30.3 percent of respondents from this state. None of the respondents residing in New Zealand reported victimisation.

Reporting scams

Almost seven out of every 10 respondents who had received a scam invitation reported it to at least one other person or organisation (69.5%, n=749; 65.4% of the total sample). The reporting rate dropped to 52.6 percent of the sample who had received a scam invitation (n=567, 49.5% of the total sample) when friends and family were excluded. The reporting rate for 2011 was lower than that of 2010; however, the response categories differed for the two years, making comparison difficult. Friends and family continued to be the most common recipients of scam complaints; however, the reporting rate for this

Table 25 Reporting of victimisation by agency, 2011

Organisation or person reported to	n	Percentage of sample that received a scam invitation (n=1,077)	Percentage of total sample (n=1,145)
Not reported to anyone	308	28.6	26.9
Family/friends	411	38.2	35.9
Police	115	10.7	10.0
SCAMwatch website (www.scamwatch.gov.au)	193	17.9	16.9
Australian Competition and Consumer Commission	128	11.9	11.2
The business represented (eg bank, eBay etc)	194	18.0	16.9
Internet Service Provider	88	8.2	7.7
Legal aid, a lawyer, or a community legal services clinic	15	1.4	1.3
Unable to recall	15	1.4	1.3
Other	135	12.5	11.8
Missing	101	9.4	8.8

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Table 26 Reporting of scams by agency, 2011

Organisation or person reported to	n	Reported victimisation (%) (n=215)
Not reported to anyone	28	13.0
Family/friends	96	44.7
Police	45	20.9
SCAMwatch website (www.scamwatch.gov.au)	66	30.7
Australian Competition and Consumer Commission	42	19.5
The business represented (eg bank, eBay etc)	64	29.8
Internet Service Provider	22	10.2
Legal aid, a lawyer, or a community legal services clinic	10	4.7
Unable to recall	5	2.3
Other	35	16.3
Missing	5	2.3

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

category dropped from 46.6 percent of those who had received a scam invitation in 2010 to 38.2 percent for participants who had received a scam invitation in 2011. Just 10.7 percent of those who received a scam invitation reported it to the police (a decrease compared with the 2010 survey results), 11.9 percent reported it to the ACCC and 17.9 percent reported it to the SCAMwatch website. Table 25 details who complaints were made to and it is noted that respondents were permitted to select more than one option.

Of the 215 respondents who reported falling victim to a scam, 186 (86.5%) reported scams to at least one other person or organisation. When friends and family were excluded, the reporting rate dropped to 77.2 percent (n=166) of those who reported to an external agency. Table 26 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 (44.7%), the SCAMwatch website (30.7%) and the business represented (29.8%).

Policing agencies received complaints from 20.9 percent of victims and the ACCC received complaints from 19.5 percent.

Included in the 2011 survey was a new question, asking why scam recipients reported to a formal agency (see Table 27). Participants could select more than one reason for reporting scams. The most common reasons for reporting a scam included preventing others from being scammed (44% of sample who received a scam invitation) and knowing it was the right thing to do (32.1% of the sample who received a scam invitation).

Reasons for not reporting scam invitations are outlined in Table 28. The most commonly provided reasons included being unsure of which agency to contact (40.9% of the sample who had received a scam invitation) and not thinking anything would be done (29.1% of the sample who had received a scam invitation). Receiving too many to report was a new response category included in the 2011 survey; 280 (26% of the sample who received a scam invitation) provided this as a reason for not reporting scams. It is noted that participants may have reported some scams but not others and may have had multiple reasons for not reporting.

The 2011 survey included a new question that asked whether respondents had reported scams on behalf of anyone else. Fifty-seven respondents (5%) indicated that they had and 53 indicated on whose behalf they had reported (see Table 29).

Perceptions of scams

Respondents were asked how they perceived each scam type. They were asked to indicate whether they considered each scam type as *a crime*, *wrong but not a crime*, or *just something that happens*. Respondents were permitted to select more than one response (see Table 30). Advance fee fraud and phishing scams continued to be the scams most likely to be considered a crime (by 77.2% and

Table 27 Reasons for reporting scams, 2011

Reason for reporting scam invitation	n	Received a scam invitation (%) (n=1,077)	Total sample (%) (n=1,145)
Desired the apprehension of offender(s)	281	26.1	24.5
Wanted to prevent others from being scammed	474	44.0	41.4
Knew it was the right thing to do	346	32.1	30.2
To assist in the investigation of an offence	289	26.8	25.2
To support your insurance claim	9	0.8	0.8
Other	59	5.5	5.2

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Table 28 Reasons for not reporting scams, 2011

Reason for not reporting	n	Received a scam invitation (%) (n=1,077)	Total sample (%) (n=1,145)
Not worth the effort	285	26.5	24.9
Didn't think it was illegal	40	3.7	3.5
Unsure of which agency to contact	441	40.9	38.5
Feared I would get into trouble	12	1.1	1.0
Didn't think anything would be done	313	29.1	27.3
Receive too many to report	280	26.0	24.5
Other	102	9.5	8.9

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

79.7% of the sample respectively). Compared with the 2010 findings, financial advice scams and work from home scams were more likely to be considered a crime in 2011 (by 43.8% and 65.8% of the sample respectively, compared with 32.5% and 25.6% in 2010).

The perception of scams by respondents who reported victimisation from that scam type was also explored (see Table 31). Again, it is noted that participants could select more than one response. While in 2010 work from home scams were least likely to be considered a crime by those who had lost finances or personal details this way, this scam type was most likely to be considered a crime by victims in 2011.

Table 29 Scams reported on behalf of someone else, 2011

Scam reported on behalf of	n	Total sample (%) (n=1,145)
Child (son or daughter)	2	0.2
Older relative (brother/sister, parent, grandparent, aunt/uncle)	17	1.5
Younger relative (niece/nephew, brother/sister)	1	0.1
A friend	11	1.0
A colleague	2	0.2
A student (if you are a teacher or in some similar capacity)	0	0.0
Other	20	1.8

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Table 30 Perceptions of scams by scam type, 2011

	A crime		Wrong but not a crime		Just something that happens	
Scam type	n	%	n	%	n	%
Lottery scams	669	58.4	308	26.9	82	7.2
Advance fee fraud	884	77.2	126	11.0	37	3.2
Inheritance scams	706	61.7	276	24.1	60	5.2
Phishing	913	79.7	107	9.3	26	2.3
Financial advice scams	501	43.8	400	34.9	132	11.5
Work from home scams	753	65.8	218	19.0	79	6.9
Dating scams	534	46.6	385	33.6	98	8.6
Other	380	33.2	79	6.9	56	4.9

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Table 31 Perceptions of scams by respondents who reported victimisation by scam type, 2011

Scam type	A crime		Wrong but not a crime		Just something that happens	
	n	%	n	%	n	%
Lottery scams (n=40)	31	77.5	4	10.0	2	5.0
Advance fee fraud (n=19)	14	73.7	2	10.5	2	10.5
Inheritance scams (n=10)	4	40.0	4	40.0	2	20.0
Phishing (n=29)	22	75.9	5	17.2	1	3.4
Financial advice scams (n=15)	9	60.0	5	33.3	1	6.7
Work from home scams (n=24)	21	87.5	1	4.2	1	4.2
Dating scams (n=23)	13	56.5	4	17.4	5	21.7
Other (n=110)	57	51.8	7	6.4	7	6.4

Source: ACFT Consumer Fraud Survey 2011 [AIC data file]

Conclusion and policy implications

Findings and discussion

Scams were received by a large proportion of the survey respondents—89 percent in 2010 and 94 percent in 2011. While lottery scams, advance fee frauds, phishing and work from home scams were the most common types of scams received, they were not necessarily the ones that resulted in the highest levels of victimisation. Dating scams, although less prevalent, were the most likely to result in the disclosure of personal details or a financial loss when a respondent was exposed to them. This finding is consistent with scam complaints made to the ACCC (2012a) and indicates that it is not sufficient to just raise awareness about the most commonly received scam invitations, but there must also be a focus on the more obscure scams.

Email was the method by which most scams were received; however, the use of mobile and landline phones, and SMS as scam delivery methods appears to be increasing, which coincides with the functionality and availability of smartphones. As reported by SCAMwatch, potential victims are increasingly being contacted by phone as targets for computer support centre scams (ACCC 2011c). It is anticipated that future scams may become more sophisticated to take advantage of the abilities of communication technologies. One recent example of this is scams that use quick response codes to direct consumers to phishing sites or send premium SMSs without the phone owner's consent.

One of the salient findings from the surveys was the low reporting rate to law enforcement and regulatory agencies. The main reasons provided for not reporting were not thinking anything would be done, being unsure of which agency to contact and perceiving that reporting was not worth the effort. A failure to report scams is problematic, in part because it reduces knowledge and understanding of the nature and extent of scams, not only for creating awareness about current threats, but also in coordinating law enforcement investigations and collecting evidence about small-value, high-volume frauds that may affect a large number of victims. A focus on the reasons why scams were reported, namely preventing others from being scammed, knowing it was the right thing to do and to assist in investigating and apprehending offenders, may be useful in the development of future education campaigns that encourage others to report scams.

Comparison of the 2010 and 2011 survey results

As there were some substantial changes for the 2011 survey compared with the 2010 survey, it was difficult to reliably compare the results of the two. There was a substantial change in the wording, as respondents were asked about 'scams' in 2011 compared with 'unsolicited contacts' in 2010. There

were also some changes and additions to the response categories for several of the forced-choice questions. The low response rate for the 2010 survey also makes it difficult to compare the findings with the survey that was conducted in 2011 (249 respondents in 2010 *c/f* 1,145 respondents in 2011).

Yet respondents to the 2010 and 2011 surveys were comparable in terms of their demographics, with females oversampled in both years and most survey respondents being over 45 years of age. Further, lottery scams were the most common type of scam received in both 2010 and 2011 (although work from home scams replaced advance fee fraud to be the second most received scam in 2011), while phishing remained the third most common scam type in both years.

Trends in scam delivery methods were difficult to capture, as the use of telephone and SMS to deliver scams was explored differently in the 2011 survey compared with the 2010 survey. However, in both years, email was the most common way that scams were received; there was a slight increase in the dissemination of scam invitations using internet and social networking websites in 2011.

Slightly more respondents reported receiving a scam invitation in the 2011 survey; however, the percentage reporting subsequent victimisation was lower in 2011 than in 2010. In both years, the scam type that resulted in the greatest proportion of recipients reporting a financial loss was dating scams. The median financial loss due to scams declined from $1,065 in 2010 to $700 in 2011.

In both the 2010 and 2011 surveys, the top two reasons for not responding to scams was that something was not quite right with the offer or invitation and that they had received similar offers before and thought they were scams. Along with the increased media coverage about the survey in 2011, there was an increase in participants who did not respond to a scam, compared with the 2010 survey, because they had seen or heard that this was a type of scam via the media or a public source.

Victim demographics were markedly different for the 2010 survey compared with the 2011 survey. As a proportion of respondents that disclosed their gender, females were overrepresented as victims in 2010, while males were overrepresented in 2011.

There were also few similarities in respect of the age of victims for the two years. In 2011, the age group who reported the highest level of victimisation (as a proportion of total respondents within that age category) was 18 to 24 years; while in 2010, this age category reported the lowest level of victimisation. Similarly, in 2011, respondents earning less than $20,000 were most likely to report victimisation, while in 2010, respondents within this income category were the least likely to be victimised.

Reporting rates dropped for 2011 compared with 2010, although those most likely to receive a scam complaint were family and friends for both years. While the response categories changed substantially over the two surveys, it was apparent that the agencies or businesses most likely to receive complaints were consumer affairs or fair trading agencies, followed by the business that had been represented in the scam, such as a bank or online auction site. In both years, policing agencies were among the least likely to receive a scam complaint. The top two reasons provided for not reporting were being unsure of which agency to contact and not thinking anything would be done.

Suggestions for future campaigns

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

- developing awareness about 'hidden' frauds. This includes frauds where victims may not realise they have been scammed, such as charity scams;
- new technologies that may be misused by scammers, such as quick response codes;
- developing awareness of the value of personal information and changing the culture in which data are liberally provided to third parties; and
- if a national reporting facility for online crime is implemented in Australia, it is suggested that a future campaign could focus on how to recognise and report scams to appropriate bodies. This could coincide with a message that aims to reduce the stigma associated with falling victim to a scam, as suggested by Budd and Anderson (2011).

References

URLs correct as at July 2012

Australian Bureau of Statistics (ABS) 2012. *Personal fraud, 2010–2011.* cat no. 4528.0. Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4528.0Main+Features12010-2011?OpenDocument

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. *Report a scam to another organisation*. http://www.scamwatch.gov.au/content/index.phtml/itemId/854913

Australian Competition & Consumer Commission (ACCC) 2012c. *Best practice guidelines for dating websites: Protecting consumers from dating scams*. Canberra: ACCC. http://www.accc.gov.au/content/index.phtml/itemId/1032533

Australian Competition & Consumer Commission (ACCC) 2012d. *Report a scam*. https://www.scamwatch.gov.au/content/index.phtml/tag/reportascam/

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

Australian Competition & Consumer Commission (ACCC) 2011b. *Targeting scams: Report of the ACCC on scam activity 2010.* Canberra: ACCC. http://www.accc.gov.au/content/index.phtml/itemId/972476

Australian Competition & Consumer Commission (ACCC) 2011c. *New twist on computer error message/virus scams: Joint warning.* http://www.scamwatch.gov.au/content/index.phtml/itemId/834379

Australian Competition & Consumer Commission (ACCC) 2011d. *ACFT campaign 2010: Online offensive-fighting fraud online!* http://www.scamwatch.gov.au/content/index.phtml/itemId/777456

Australian Competition & Consumer Commission (ACCC) 2011e. *ACFT campaign 2011: Scams—It's personal*. http://www.scamwatch.gov.au/content/index.phtml/itemId/777456

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

Department of the Prime Minister and Cabinet (DPMC) 2011. *Connecting with confidence: Optimising Australia's digital future.* Canberra: DPMC. http://cyberwhitepaper.dpmc.gov.au/white-paper

Levi M & Smith RG 2011. Fraud vulnerabilities and the global financial crisis. *Trends & Issues in Crime and Criminal Justice* no. 422. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/421-440/tandi422.aspx

Ross S & Smith RG 2011. Risk factors for advance fee fraud victimisation. *Trends & Issues in Crime and Criminal Justice* no. 420. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/401-420/tandi420.aspx

Shanklin W 2011. *Quick response codes are being used to spread malware*. http://www.geek.com/articles/mobile/qr-codes-are-being-used-to-spread-malware-20111021/

Smith RG 2008. Coordinating individual and organisational responses to fraud. *Crime, Law and Social Change* 49(5): 379–396

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

Vuong A 2011. *Growing popularity of quick response codes attracts digital scammers.* http://www.denverpost.com/business/ci_19329006

Appendixes

Appendix A

2010 consumer fraud survey

Australasian Consumer Fraud Taskforce Online Survey 2010

The Australasian Consumer Fraud Taskforce (ACFT) was formed in March 2005 and comprises 20 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 you would like to assist us by completing the survey, please click on the proceed button below.

Australasian Consumer Fraud Taskforce Survey 2010

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

a) Having won the 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,

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

h) Some other scam type

R1_1 ☐ Yes

R1_2 ☐ No (Skip to Q12)

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

Type of Scam	Mail	Email	Home/work phone	Mobile phone/ SMS	Internet site/social networking site	Other
Notification of having won the lottery or some other prize	R2_1 ☐	R2_2 ☐	R2_3 ☐	R2_4 ☐	R2_5 ☐	R2_6 ☐
A request for assistance to transfer money out of another country (such as Nigeria)	R3_1 ☐	R3_2 ☐	R3_3 ☐	R3_4 ☐	R3_5 ☐	R3_6 ☐
A notification of an inheritance	R4_1 ☐	R4_2 ☐	R4_3 ☐	R4_4 ☐	R4_5 ☐	R4_6 ☐
A request by a business to confirm your personal details or passwords (phishing scams)	R5_1 ☐	R5_2 ☐	R5_3 ☐	R5_4 ☐	R5_5 ☐	R5_6 ☐
A request to supply you with financial advice	R6_1 ☐	R6_2 ☐	R6_3 ☐	R6_4 ☐	R6_5 ☐	R6_6 ☐
An opportunity to work from home	R7_1 ☐	R7_2 ☐	R7_3 ☐	R7_4 ☐	R7_5 ☐	R7_6 ☐
Pursuing a personal relationship that later turned out to be false	R8_1 ☐	R8_2 ☐	R8_3 ☐	R8_4 ☐	R8_5 ☐	R8_6 ☐
Other type of scam	R9_1 ☐	R9_2 ☐	R9_3 ☐	R9_4 ☐	R9_5 ☐	R9_6 ☐

If 'other' type of scam, please specify what the contact was about (max 250 characters)	R10_1 .....

3 - Over the last 12 months, have you responded positively in any way to these unsolicited contacts? (Select all that apply)

Responding positively 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).

R11_1 ☐ Yes

R11_2 ☐ No (Skip to Q9)

4 - How many times over the last 12 months have you responded positively to each of the following type of unsolicited contact? (Select one response for each type of scam listed)

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

Type of Scam	Never	Once	Twice	Three times	Four times	Five or more times	Other
Notification of having won the lottery or some other prize	R12_1 ☐	R12_2 ☐	R12_3 ☐	R12_4 ☐	R12_5 ☐	R12_6 ☐	R12_7 ☐
A request for assistance to transfer money out of another country (such as Nigeria)	R13_1 ☐	R13_2 ☐	R13_3 ☐	R13_4 ☐	R13_5 ☐	R13_6 ☐	R13_7 ☐
A notification of an inheritance	R14_1 ☐	R14_2 ☐	R14_3 ☐	R14_4 ☐	R14_5 ☐	R14_6 ☐	R14_7 ☐
A request by a business to confirm your personal details or passwords (phishing scams)	R15_1 ☐	R15_2 ☐	R15_3 ☐	R15_4 ☐	R15_5 ☐	R15_6 ☐	R15_7 ☐
A request to supply you with financial advice	R16_1 ☐	R16_2 ☐	R16_3 ☐	R16_4 ☐	R16_5 ☐	R16_6 ☐	R16_7 ☐
An opportunity to work from home	R17_1 ☐	R17_2 ☐	R17_3 ☐	R17_4 ☐	R17_5 ☐	R17_6 ☐	R17_7 ☐
Pursuing a personal relationship that later turned out to be false	R18_1 ☐	R18_2 ☐	R18_3 ☐	R18_4 ☐	R18_5 ☐	R18_6 ☐	R18_7 ☐
Other type of scam	R19_1 ☐	R19_2 ☐	R19_3 ☐	R19_4 ☐	R19_5 ☐	R19_6 ☐	R19_7 ☐

5 - Have you ever sent money as a result of any of these unsolicited contacts? (Select one response for each type of scam listed)

Type of Scam	Yes	No	Dont know/ cant remember
Notification of having won the lottery or some other prize	R20_1 ☐	R20_2 ☐	R20_3 ☐
A request for assistance to transfer money out of another country (such as Nigeria)	R21_1 ☐	R21_2 ☐	R21_3 ☐
A notification of an inheritance	R22_1 ☐	R22_2 ☐	R22_3 ☐
A request by a business to confirm your personal details or passwords (phishing scams)	R23_1 ☐	R23_2 ☐	R23_3 ☐
A request to supply you with financial advice	R24_1 ☐	R24_2 ☐	R24_3 ☐
An opportunity to work from home	R25_1 ☐	R25_2 ☐	R25_3 ☐
Pursuing a personal relationship that later turned out to be false	R26_1 ☐	R26_2 ☐	R26_3 ☐
Other type of scam	R27_1 ☐	R27_2 ☐	R27_3 ☐

6 - If you responded 'yes' to any of the options in Question 5, 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 true.

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.

R28_1 ☐ Don't know/can't remember

R28_2 ☐ I'd rather not say

R28_3 ☐ The amount in the box below

Please indicate the amount in whole dollars.	R29_1 .....

7 - Have you ever disclosed personal details or passwords as a result of these unsolicited contacts? (Select one response for each type of scam listed)

Type of Scam	Yes	No	Dont know/ cant remember
Notification of having won the lottery or some other prize	R30_1 ☐	R30_2 ☐	R30_3 ☐
A request for assistance to transfer money out of another country (such as Nigeria)	R31_1 ☐	R31_2 ☐	R31_3 ☐
A notification of an inheritance	R32_1 ☐	R32_2 ☐	R32_3 ☐
A request by a business to confirm your personal details or passwords (phishing scams)	R33_1 ☐	R33_2 ☐	R33_3 ☐
A request to supply you with financial advice	R34_1 ☐	R34_2 ☐	R34_3 ☐
An opportunity to work from home	R35_1 ☐	R35_2 ☐	R35_3 ☐
Pursuing a personal relationship that later turned out to be false	R36_1 ☐	R36_2 ☐	R36_3 ☐
Other type of scam	R37_1 ☐	R37_2 ☐	R37_3 ☐

8 - How many times were you in contact with the person/s before you sent money or personal information? (Select one option only)

R38_1 ☐	Once only
R38_2 ☐	Between two and ten times
R38_3 ☐	Between eleven and twenty times
R38_4 ☐	More than twenty times
R38_5 ☐	I can't recall

9 - If you received any unsolicited contacts 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	R39_1 ☐
Had received similar offers before and thought they were scams	R40_1 ☐
Had seen/heard this was a type of scam in the media or a public source	R41_1 ☐
Was told it was a scam by someone I knew	R42_1 ☐
Someone I know has been a victim of a scam before	R43_1 ☐
Wanted to respond but could not afford to participate	R44_1 ☐
Something was not quite right with the offer or invitation	R45_1 ☐
Other (please specify below)	R46_1 ☐
	R47_1 .....

10 - Have you reported any of these unsolicited invitations to anyone? (Select all that apply)

Family/friends	R48_1 ☐
Police Agencies	R49_1 ☐
Consumer Affairs or Fair Trading Agency	R50_1 ☐
Australian High Tech Crime Centre	R51_1 ☐
The business represented (e.g bank, ebay etc)	R52_1 ☐
Internet Service Provider	R53_1 ☐
Legal aid, a lawyer, or a community legal services clinic	R54_1 ☐
Unable to recall	R55_1 ☐
Other (please specify below)	R56_1 ☐
	R57_1

	.....

11 - If you received an unsolicited invitation 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	R58_1 ☐
Didn't think it was illegal	R59_1 ☐
Unsure of which agency to contact	R60_1 ☐
Feared I would get into trouble	R61_1 ☐
Didn't think anything would be done	R62_1 ☐
Other (please specify below)	R63_1 ☐
	R64_1 .....

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

Type of Scam	A crime	Wrong but not a crime	Just something that happens	Dont know
Notification of having won the lottery or some other prize	R65_1 ☐	R65_2 ☐	R65_3 ☐	R65_4 ☐
A request for assistance to transfer money out of another country (such as Nigeria)	R66_1 ☐	R66_2 ☐	R66_3 ☐	R66_4 ☐
A notification of an inheritance	R67_1 ☐	R67_2 ☐	R67_3 ☐	R67_4 ☐
A request by a business to confirm your personal details or passwords (phishing scams)	R68_1 ☐	R68_2 ☐	R68_3 ☐	R68_4 ☐
A request to supply you with financial advice	R69_1 ☐	R69_2 ☐	R69_3 ☐	R69_4 ☐
An opportunity to work from home	R70_1 ☐	R70_2 ☐	R70_3 ☐	R70_4 ☐
Pursuing a personal relationship that later turned out to be false	R71_1 ☐	R71_2 ☐	R71_3 ☐	R71_4 ☐
Other type of scam	R72_1 ☐	R72_2 ☐	R72_3 ☐	R72_4 ☐

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

R73_1 ☐	Media Article
R73_2 ☐	A Government website
R73_3 ☐	Scamwatch website
R73_4 ☐	Poster or pamphlet
R73_5 ☐	Referred by other agency
R73_6 ☐	Word of mouth (family, friends etc)
R73_7 ☐	Other
If 'other', please specify	R74_1 .....

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

2009	R75_1 ☐
2008	R76_1 ☐
2007	R77_1 ☐
2006	R78_1 ☐

15 - Are you aware of the 2010 fraud awareness campaign run by the Australasian Consumer Fraud Taskforce?

R79_1 ☐	Yes
R79_2 ☐	No

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

R80_1 ☐	Yes
R80_2 ☐	No

17 - What is your age?

R81_1 ☐	17 and under
R81_2 ☐	18 - 24
R81_3 ☐	25 - 34
R81_4 ☐	35 - 44
R81_5 ☐	45 - 54
R81_6 ☐	55 - 64
R81_7 ☐	65+

18 - What is your gender?

R82_1 ☐	Male
R82_2 ☐	Female

19 - Where do you normally reside?

R83_1 ☐	Australian Capital Territory
R83_2 ☐	New South Wales
R83_3 ☐	New Zealand
R83_4 ☐	Northern Territory
R83_5 ☐	Queensland
R83_6 ☐	South Australia
R83_7 ☐	Tasmania
R83_8 ☐	Victoria
R83_9 ☐	Western Australia
R83_10 ☐	Resident of a country other than Australia or New Zealand (please specify below)

Please specify country R84_1 .....

20 - What is your average yearly income?

R85_1 ☐	Under $20,000
R85_2 ☐	$20,000 - <$40,000
R85_3 ☐	$40,000 - <$60,000
R85_4 ☐	$60,000 - <$80,000
R85_5 ☐	Over $80,000
R85_6 ☐	I'd rather not say

21 - In which capacity did you fill out this survey?

	Member of the public	Member of the police	My employer is a private sector Australasian Consumer Fraud Taskforce member	My employer is a government sector Australasian Consumer Fraud Taskforce member	Other government agency
	○ *(1)* R86_1 Member of the public ○ *(2)* R86_1 Member of the police ○ *(3)* R86_1 My employer is a				

R86_1	private sector Australasian Consumer Fraud Taskforce member ○ *(4)* R86_1 My employer is a government sector Australasian Consumer Fraud Taskforce member ○ *(5)* R86_1 Other government agency

Appendix B

2011 consumer fraud survey

Australasian Consumer Fraud Taskforce Online Survey 2011

The Australasian Consumer Fraud Taskforce (ACFT) was formed in March 2005 and comprises 20 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 you would like to assist us by completing the survey, please click on the proceed button below.

Australasian Consumer Fraud Taskforce Survey 2011

1 - Over the last 12 months, have you been 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) Pursuing a personal relationship that turned out to be false, or

h) Some other scam type

R1_1 ☐ Yes

R1_2 ☐ No (Skip to Q15)

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

Type of Scam	Mail	Email	Telephone (including landlines and moblie phones)	SMS	Internet site/social networking site	Other	N/A
Notification of having won a lottery or some other prize	R2_1 ☐	R2_2 ☐	R2_3 ☐	R2_4 ☐	R2_5 ☐	R2_6 ☐	R2_7 ☐
A request for assistance to transfer money out of another country (such as Nigeria)	R3_1 ☐	R3_2 ☐	R3_3 ☐	R3_4 ☐	R3_5 ☐	R3_6 ☐	R3_7 ☐
A notification of an inheritance	R4_1 ☐	R4_2 ☐	R4_3 ☐	R4_4 ☐	R4_5 ☐	R4_6 ☐	R4_7 ☐
A request by a business to confirm your personal details or passwords (phishing scams)	R5_1 ☐	R5_2 ☐	R5_3 ☐	R5_4 ☐	R5_5 ☐	R5_6 ☐	R5_7 ☐
A request to supply you with financial advice	R6_1 ☐	R6_2 ☐	R6_3 ☐	R6_4 ☐	R6_5 ☐	R6_6 ☐	R6_7 ☐
An opportunity to work from home (a front for money laundering)	R7_1 ☐	R7_2 ☐	R7_3 ☐	R7_4 ☐	R7_5 ☐	R7_6 ☐	R7_7 ☐
Pursuing a personal relationship that later turned out to be	R8_1 ☐	R8_2 ☐	R8_3 ☐	R8_4 ☐	R8_5 ☐	R8_6 ☐	R8_7 ☐

false							
Other type of scam	R9_1 ☐	R9_2 ☐	R9_3 ☐	R9_4 ☐	R9_5 ☐	R9_6 ☐	R9_7 ☐
If 'other', please specify						R10_1	

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

Type of Scam	Never	One to five times	Six to 10 times	11 to 20 times	21 to 50 times	More than 50 times
Mail	R11_1 ☐	R11_2 ☐	R11_3 ☐	R11_4 ☐	R11_5 ☐	R11_6 ☐
Email	R12_1 ☐	R12_2 ☐	R12_3 ☐	R12_4 ☐	R12_5 ☐	R12_6 ☐
Telephone (including landlines and mobile phones)	R13_1 ☐	R13_2 ☐	R13_3 ☐	R13_4 ☐	R13_5 ☐	R13_6 ☐
SMS	R14_1 ☐	R14_2 ☐	R14_3 ☐	R14_4 ☐	R14_5 ☐	R14_6 ☐
Internet site/ social networking	R15_1 ☐	R15_2 ☐	R15_3 ☐	R15_4 ☐	R15_5 ☐	R15_6 ☐
Other	R16_1 ☐	R16_2 ☐	R16_3 ☐	R16_4 ☐	R16_5 ☐	R16_6 ☐
If 'other', please specify					R17_1	

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).

R18_1 ☐ Yes

R18_2 ☐ 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

Type of Scam	Never	Once	Twice	Three times	Four times	Five or more times
Notification of having won the lottery or some other prize	R19_1 ☐	R19_2 ☐	R19_3 ☐	R19_4 ☐	R19_5 ☐	R19_6 ☐
A request for assistance to transfer money out of another country (such as Nigeria)	R20_1 ☐	R20_2 ☐	R20_3 ☐	R20_4 ☐	R20_5 ☐	R20_6 ☐
A notification of an inheritance	R21_1 ☐	R21_2 ☐	R21_3 ☐	R21_4 ☐	R21_5 ☐	R21_6 ☐
A request by a business to confirm your personal details or passwords (phishing scams)	R22_1 ☐	R22_2 ☐	R22_3 ☐	R22_4 ☐	R22_5 ☐	R22_6 ☐
A request to supply you with financial advice	R23_1 ☐	R23_2 ☐	R23_3 ☐	R23_4 ☐	R23_5 ☐	R23_6 ☐
An opportunity to work from home (a front for money laundering)	R24_1 ☐	R24_2 ☐	R24_3 ☐	R24_4 ☐	R24_5 ☐	R24_6 ☐
Pursuing a personal relationship that later turned out to be false	R25_1 ☐	R25_2 ☐	R25_3 ☐	R25_4 ☐	R25_5 ☐	R25_6 ☐
Other type of scam	R26_1 ☐	R26_2 ☐	R26_3 ☐	R26_4 ☐	R26_5 ☐	R26_6 ☐
If 'other', please specify					R27_1	

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	Dont know/ I can't recall
Notification of having won the lottery or some other prize	R28_1 ☐	R28_2 ☐	R28_3 ☐
A request for assistance to transfer money out of another country (such as	R29_1 ☐	R29_2 ☐	R29_3 ☐

Nigeria)			
A notification of an inheritance	R30_1 ☐	R30_2 ☐	R30_3 ☐
A request by a business to confirm your personal details or passwords (phishing scams)	R31_1 ☐	R31_2 ☐	R31_3 ☐
A request to supply you with financial advice	R32_1 ☐	R32_2 ☐	R32_3 ☐
An opportunity to work from home (a front for money laundering)	R33_1 ☐	R33_2 ☐	R33_3 ☐
Pursuing a personal relationship that later turned out to be false	R34_1 ☐	R34_2 ☐	R34_3 ☐
Other type of scam	R35_1 ☐	R35_2 ☐	R35_3 ☐
If 'other', please specify			R36_1 .....

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 Q8, skip to Q10.

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 true.

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.

R37_1 ☐	Don't know/ I can't recall
R37_2 ☐	I'd rather not say
R37_3 ☐	The amount in the box below
Please indicate the amount in whole dollars.	R38_1 .....

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	Dont know/I can't recall
Notification of having won the lottery or some other prize	R39_1 ☐	R39_2 ☐	R39_3 ☐
A request for assistance to transfer money out of another country (such as Nigeria)	R40_1 ☐	R40_2 ☐	R40_3 ☐
A notification of an inheritance	R41_1 ☐	R41_2 ☐	R41_3 ☐
A request by a business to confirm your personal details or passwords (phishing scams)	R42_1 ☐	R42_2 ☐	R42_3 ☐
A request to supply you with financial advice	R43_1 ☐	R43_2 ☐	R43_3 ☐
An opportunity to work from home (a front for money laundering)	R44_1 ☐	R44_2 ☐	R44_3 ☐
Pursuing a personal relationship that later turned out to be false	R45_1 ☐	R45_2 ☐	R45_3 ☐
Other type of scam	R46_1 ☐	R46_2 ☐	R46_3 ☐
If 'other', please specify			R47_1 .....

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

R48_1 ☐	Once only
R48_2 ☐	Two to five times
R48_3 ☐	Six to 10 times
R48_4 ☐	10 to 20 times
R48_5 ☐	More than 20 times
R48_6 ☐	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	R49_1 ☐
Had received similar offers before and thought they were scams	R50_1 ☐

Had seen/heard this was a type of scam in the media or a public source	R51_1 ☐
Was told it was a scam by someone I knew	R52_1 ☐
Someone I know has been a victim of a scam before	R53_1 ☐
Wanted to respond but could not afford to participate	R54_1 ☐
Something was not quite right with the offer or invitation	R55_1 ☐
Offer was identified as spam/ declared unsafe by Internet filter	R56_1 ☐
Other	R57_1 ☐
If 'other', please specify	R58_1 .....

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

Not reported to anyone (Skip to Q13)	R59_1 ☐
Family/ friends	R60_1 ☐
Police	R61_1 ☐
SCAMwatch website (www.scamwatch.gov.au)	R62_1 ☐
Australian Competition and Consumer Commission/ Fair Trading agencies	R63_1 ☐
The business represented (e.g bank, ebay etc)	R64_1 ☐
Internet Service Provider	R65_1 ☐
Legal aid, a lawyer, or a community legal services clinic	R66_1 ☐
Unable to recall	R67_1 ☐
Other	R68_1 ☐
If 'other', please specify	R69_1 .....

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)	R70_1 ☐
Wanted to prevent others from being scammed	R71_1 ☐
Knew it was the right thing to do	R72_1 ☐
To assist in the investigation of an offence	R73_1 ☐
To support your insurance claim	R74_1 ☐
Other	R75_1 ☐
If 'other', please specify	R76_1 .....

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	R77_1 ☐
Didn't think it was illegal	R78_1 ☐
Unsure of which agency to contact	R79_1 ☐
Feared I would get into trouble	R80_1 ☐
Didn't think anything would be done	R81_1 ☐
Receive too many to report	R82_1 ☐
Other	R83_1 ☐
If 'other', please specify	R84_1 .....

14 - Have you reported any scams to those specified in Q11, on behalf of anyone else?

Yes	R85_1 ☐
No	R86_1 ☐

	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 yes, please specify who you reported on behalf of R87_1	○ *(1)* R87_1 Your child (son or daughter) ○ *(2)* R87_1 Your older relative (brother/sister, parent, grandparent, aunt/uncle) ○ *(4)* R87_1 Your younger relative (niece/nephew, brother/sister) ○ *(3)* R87_1 A friend ○ *(5)* R87_1 A colleague ○ *(6)* R87_1 A student (if you are a teacher or in some similar capacity) ○ *(7)* R87_1 Other						

15 - How do you regard each of the following 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 the lottery or some other prize	R88_1 ☐	R88_2 ☐	R88_3 ☐
A request for assistance to transfer money out of another country (such as Nigeria)	R89_1 ☐	R89_2 ☐	R89_3 ☐
A notification of an inheritance	R90_1 ☐	R90_2 ☐	R90_3 ☐
A request by a business to confirm your personal details or passwords (phishing scams)	R91_1 ☐	R91_2 ☐	R91_3 ☐
A request to supply you with financial advice	R92_1 ☐	R92_2 ☐	R92_3 ☐
An opportunity to work from home (a front for money laundering)	R93_1 ☐	R93_2 ☐	R93_3 ☐
Pursuing a personal relationship that later turned out to be false	R94_1 ☐	R94_2 ☐	R94_3 ☐
Other type of scam	R95_1 ☐	R95_2 ☐	R95_3 ☐
If 'other', please specify			R96_1 .....

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

R97_1 ☐	Media article
R97_2 ☐	A Government website
R97_3 ☐	SCAMwatch website (www.scamwatch.gov.au)
R97_4 ☐	Poster or pamphlet
R97_5 ☐	Referred by other agency

R97_6 ☐	Word of mouth (family, friends etc)
R97_7 ☐	Other
If 'other', please specify	R98_1 .....

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

2010	R99_1 ☐
2009	R100_1 ☐
2008	R101_1 ☐
2007	R102_1 ☐

18 - Are you aware of the 2011 fraud awareness campaign run by the Australasian Consumer Fraud Taskforce?

R103_1 ☐	Yes
R103_2 ☐	No

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

R104_1 ☐	Yes
R104_2 ☐	No

20 - Which age group do you belong to?

R105_1 ☐	17 and under
R105_2 ☐	18 - 24
R105_3 ☐	25 - 34
R105_4 ☐	35 - 44
R105_5 ☐	45 - 54
R105_6 ☐	55 - 64
R105_7 ☐	65+

21 - What is your gender?

R106_1 ☐	Male
R106_2 ☐	Female

22 - Where do you normally reside?

R107_1 ☐	Australian Capital Territory
R107_2 ☐	New South Wales
R107_3 ☐	Northern Territory
R107_4 ☐	Queensland
R107_5 ☐	South Australia
R107_6 ☐	Tasmania
R107_7 ☐	Victoria
R107_8 ☐	Western Australia
R107_9 ☐	New Zealand
R107_10 ☐	Resident of a country other than Australia or New Zealand (please specify below)
Please specify country	R108_1 .....

23 - What was your gross income from all sources for the year 2009-10 (i.e. before tax deductions)?

R109_1 ☐	Under $20,000
R109_2 ☐	$20,000 - <$40,000
R109_3 ☐	$40,000 - <$60,000

R109_4 ☐	$60,000 - <$80,000
R109_5 ☐	Over $80,000
R109_6 ☐	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
R110_1	○ *(1)* R110_1 Recently been scammed ○ *(2)* R110_1 Receive scams but have not been scammed ○ *(3)* R110_1 Want to assist in research to combat scammers ○ *(4)* R110_1 To learn more about scams ○ *(5)* R110_1 Other				
If 'other', please specify					R111_1 .....

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
R112_1	○ *(1)* R112_1 Member of the public ○ *(2)* R112_1 Retiree ○ *(3)* R112_1 Member of the police ○ *(4)* R112_1 My employer is an Australasian Consumer Fraud Taskforce Government member ○ *(5)* R112_1 My employer is an Australasian					

	Consumer Fraud Taskforce private sector partner ○ *(6)* R112_1 Other Government agency

Appendix C

Newspaper articles relating to consumer fraud published 1 to 7 March 2010

Bain D 2010. Scammers on the rise. *The World Today* 1 March

Brisbane MX 2010. Scam alerts on the rise. *Brisbane MX* 1 March

Caton P 2010. Internet scams cost us $70m pa. *Tweed Daily News* 2 March

Clark N 2010. Warning over net scams Tassie buyers alerted. *The Mercury* 5 March

Davies J 2010. How to avoid online scams. *Sunday Herald-Sun* 7 March

Davies J 2010. Money talk: How to avoid online scams. *Sunday Mail* 7 March

Davies J 2010. How to avoid online scams. *Sunday Mail* 7 March

Davies J 2010. How to avoid online scams. *Sunday Telegraph* 7 March

Fraser Coast Chronicle 2010. Keep clear of phishing and smishing scams. *Fraser Coast Chronicle* 3 March

Geelong Advertiser 2010. In brief. *Geelong Advertiser* 2 March

Gilbert J 2010. Web scam hits Sounds Resort. *The Marlborough Express* 3 March

Harmer W 2010. In cyberspace no one can hear you scream. *Sunday Telegraph* 7 March

Jacques O 2010. How staying in touch makes you a target for theft by Twitter. *Sunshine Coast Daily* 5 March

Johnston J 2010. Bungle fuels fraud fears. *The Gold Coast Bulletin* 4 March

Kalgoorlie Miner 2010. Tackling online fraudsters. *Kalgoorlie Miner* 3 March

Lohman T 2010. Online fraud victims too embarrassed to report being scammed. *Computerworld* 2 March

Rochfot S 2010. CBD. *Sydney Morning Herald* 2 March

Sun M 2010. Online rip-offs surge—New figures 'tip of the iceberg'. *Sydney MX* 4 March

Sun M & Munro O'Brien J 2010. Surge in online rip-offs—New figures 'tip of iceberg'. *Brisbane MX* 4 March

The Daily Telegraph 2010. $70m lost in scams. *The Daily Telegraph* 2 March

The Gympie Times 2010. Public warn to be vigilant against investment scams. *The Gympie Times* 6 March

The Herbert River Express 2010. Fraud Week warning on scams. *The Herbert River Express* 4 March

The Northern Territory News 2010. ATO fraud warning. *The Northern Territory News* 2 March

The Northern Territory News 2010. Scams catching Aussies out online. *The Northern Territory News* 2 March

The Northern Times 2010. Crime stoppers. *The Northern Times* 5 March

The Queensland Times 2010. Look after personal details. *The Queensland Times* 2 March

The Queensland Times 2010. Beware of scammers. *The Queensland Times* 1 March

Thom G 2010. Cyber fraud soaring. *Herald Sun* 3 March

Walsh L 2010. Online fraud increases as complaints reach a new high. *The Courier-Mail* 2 March

Walsh L 2010. Web scam claims skyrocket. *The Mercury* 2 March

Walsh N 2010. Online fraudsters net millions. *ABC Premium News* 1 March

Warwick Daily News 2010. Fraud Week warning on scams. *Warwick Daily News* 2 March

Warwick Daily News 2010. Readers urged to protect ID. *Warwick Daily News* 6 March

Appendix D

Newspaper articles relating to consumer fraud published 7 to 13 March 2011

ABC Premium News 2011. Internet scam victims open to prosecution. *ABC Premium News* 8 March

Adlam N 2011. Scammers getting personal. *The Northern Territory News* 8 March

Advocate 2011. Briefly. *Advocate* 9 March

Ayr Advocate 2011. Fraud message promoted. *Ayr Advocate* 11 March

Bita N 2011. Online cash scams double in a year. *The Australian* 7 March

Bowen Independent 2011. Scammer warning. *Bowen Independent* 9 March

Bowen Independent 2011. Stay alert call for mobile scams. *Bowen Independent* 11 March

Brown D 2011. Scams impact hitting home. *The Mercury* 7 March

Eastern Suburbs Reporter 2011. Sellers beware of internet scammers. *Eastern Suburbs Reporter* 8 March

Harper J 2011. Quiz to help avoid scams. *Geelong Advertiser* 8 March

Hervey Bay Observer 2011. Too good to be true? Then it usually is. *Hervey Bay Observer* 11 March

Hills Gazette 2011. If you are trying to sell your home via the internet, be warned about scammers who are targeting private property sellers online. *Hills Gazette* 11 March

Kalgoorlie Miner 2011. Beware scams. *Kalgoorlie Miner* 9 March

Larkin N 2011. Frauds running riot. *The Advertiser* 7 March

Larkin N 2011. Yourmoney.com.au: Fraud running riot. *The Cairns Post* 7 March

Larkin N 2011. Fraud running riot. *The Courier-Mail* 7 March

Larkin N 2011. Fraud running riot. *The Daily Telegraph* 7 March

Larkin N 2011. Fraudsters run amok on internet. *Townsville Bulletin* 7 March

Larkin N 2011. Fraud running riot. *Herald Sun* 7 March

Miller T 2011. Gen Y's scam shame. *Brisbane MX* 8 March

Miletic D 2011. Scammers double the dupe rate. *The Age* 7 March

Niletic D 2011. Scam warning, victims lose $63m. *Canberra Times* 7 March

O'Loan J 2011. Scams on the rise, but we're not too gullible. *The Courier-Mail* 10 March

Pape S 2011. How to avoid being victim of scammers. *The Advertiser* 12 March

Pape S 2011. National Consumer Fraud Week tips. *The Courier-Mail* 12 March

Pape S 2011. Shell out cash wisely. *The Courier-Mail* 12 March

Pape S 2011. There's plenty of lessons we can learn from an 'accidental' conman. *Herald Sun* 12 March

Pape S 2011. Sniffing out a scam artist. *The Mercury* 12 March

Pape S 2011. Good deal or real deal. *The Sunday Times* 13 March

Rosenberg J 2011. Twice as many fall prey to scammers. *Sydney Morning Herald* 7 March

Rosenberg J 2011. Hoaxes double. *Newcastle Herald* 7 March

Smart Company 2011. Scam complaints double as shonks target domain names, directories and franchising. *Smart Company* 7 March

The Cairns Post 2011. Want to lose cash fast? Respond to scams. *The Cairns Post* 9 March

The Daily Mercury 2011. Phone scams. *The Daily Mercury* 12 March

The Daily Telegraph 2011. Scammers net $1b. *The Daily Telegraph* 9 March

The Gold Coast Bulletin 2011. Scams rampant. *The Gold Coast Bulletin* 9 March

The Gympie Times 2011. Fraud is personal. *The Gympie Times* 9 March

The Morning Bulletin 2011. Briefs. *The Morning Bulletin* 9 March

The Northern Territory News 2011. Cyber criminals target smartphones. *The Northern Territory News* 10 March

The Queensland Times 2011. Internet scams doubled in year. *The Queensland Times* 12 March

The Queensland Times 2011. Watch out for scams. *The Queensland Times* 8 March

The Redcliffe & Bayside Herald 2011. Crime Stoppers. *The Redcliffe & Bayside Herald* 9 March

The West Australian 2011. Con artists make online Aussies pay. *The West Australian* 7 March

Thom G 2011. Aussies lose $63m to scammers. Net rip-offs trap 1000s. *Herald Sun* 7 March

Townsville Bulletin 2011. Scams still trap Aussies. *Townsville Bulletin* 9 March

Turnbull J 2011. Online scammers reap $1bn. *The Advertiser* 9 March