Australian Government
Australian Institute of Criminology

Consumer fraud in Australasia: Results of the Australasian Consumer Fraud Taskforce online Australia surveys 2008 and 2009

Carolyn Budd
Jessica Anderson

AIC Reports
Technical and Background Paper 43

Consumer fraud in Australasia: Results of the Australasian Consumer Fraud Taskforce online Australia surveys 2008 and 2009

Carolyn Budd
Jessica Anderson

AIC Reports
Technical and
Background Paper
43

www.aic.gov.au

ISSN 1836-2052
ISBN 978 1 921532 77 1

Project no. 0132
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

Those who perpetrate consumer scams use a wide range of deceptive practices and methods of communication. However, all aim to trick unsuspecting consumers into parting with money or information, often to criminals located overseas. Phishing attacks, lottery and prize scams, financial investment scams and advanced fee fraud are just a few of the more common scam varieties that are used in an attempt to gain either money or personal details that will eventually be used for financial gain by offenders. The increased use of electronic forms of communication and the ease of sending mass scam invitations via the Internet has also resulted in an increase in the number of scam requests disseminated globally.

Scam invitations may appear benign to those who receive them and choose not to respond. This form of spam may be seen as an unfortunate consequence of using the Internet, however, scams can cause serious financial and other harms to those who are victimised, as well as to the wider community. Consumer fraud has been estimated to cost Australia almost $1b annually, although the full extent of the losses is unknown as many choose not to report their experiences officially. Although victims of scams can lose as little as $1, some send substantial amounts to criminals, occasionally exceeding many hundreds of thousands of dollars. Those who send such large amounts frequently feel ashamed of what they have done, or apprehensive that they might have acted illegally. Victims may also receive little sympathy for having being victimised and may be blamed for being gullible. These factors act to deter victims from formally reporting the scam to police. When the full circumstances of cases are known, however, the sophistication of the deception makes it clear that victims have been enticed by a serious and concerted campaign of trickery which preys on their weaknesses and vulnerabilities.

The Australasian Consumer Fraud Taskforce (ACFT) includes 20 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 their impact, to determine how victims respond and to identify any emerging typologies and issues.

This report presents the results of surveys conducted in conjunction with the 2008 campaign that focused on *Seduction and Deception Scams* and the 2009 campaign that focused on sending the message—*Scams Target You: Protect Yourself, Don't Be a Victim of Scammers* and *Fight the Scammers. Don't Respond*. Overall, both surveys found that despite most respondents indicating that they had received a scam invitation over the specified 12 month period, the majority did not respond. Invitations sent by email remained the most common method of receiving an invitation, with lottery scams attracting the highest number of victims in 2008 whereas in 2009, work from home scams were the most common way respondents were scammed.

Although the survey relies on self-reported data, it still provides a useful means of identifying the nature of victimisation and for identifying areas for further research into consumer fraud. The links identified between scam victimisation and factors such as age, income, reporting and jurisdiction could be used to develop more strategic consumer fraud awareness campaigns that focus on the groups more vulnerable to scam victimisation. The relationships between these variables and victimisation could then be explored more fully using representative samples of the population, or in-depth data collection techniques such as interviewing of those who have been defrauded. With a more extensive understanding of who is victimised and why, more effective scam prevention measures can be enacted.

Adam Tomison
Director

Contents

Figures

Tables

Acknowledgements

This paper makes use of information provided by members of the Australasian Consumer Fraud Taskforce (ACFT). 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. We are grateful to all those who took the time to complete the ACFT survey in 2008 and 2009.

Acronyms

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACFT	Australasian Consumer Fraud Taskforce
AFF	Advance fee fraud
AIC	Australian Institute of Criminology
UKOFT	UK Office of Fair Trading

Executive summary

Consumer fraud is not a new phenomenon, however, the expansion of the Internet and the increased capacity for spam email has seen a rise in the number of fraudulent requests sent to internet users across the globe. *Spam* is the electronic equivalent of paper 'junk' mail, in which unsolicited, bulk transmission emails are sent to email account holders (AIC 2006). The primary motivation for sending spam emails is the lure of obtaining financial returns far in excess of the sender's outlays. Nowadays, however, spam can be sent simultaneously to millions of potential victims in just seconds and at negligible cost.

Unsolicited spam emails comprise a major component of how consumer scams are sent to potential victims. The Australian Bureau of Statistics (ABS) (2008: 5) defined consumer scams as

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

Consumer fraud can incorporate, among other things, fraudsters selling a non-existent item that requires an advanced payment (known as advance fee, or AFF schemes), persuading consumers to buy an unwanted product through deceptive marketing techniques and using someone else's personal details for their own benefit (see Smith 2007). Common scam types in Australasia include:

- AFF (such as Nigerian or 419 scams);
- phishing;
- lottery and prize scams;
- inheritance scams;
- financial investment scams;
- work from home scams; and
- dating/relationships scams.

Since 2006, the Australasian Consumer Fraud Taskforce (ACFT) has participated in the fraud prevention and awareness-raising activities undertaken each year by members of the International Consumer Protection and Enforcement Network. An annual awareness campaign has been conducted in Australia and in New Zealand since 2007. In 2008, the campaign ran for a fortnight under the title *Fraud Fortnight*, with the theme *Seduction and Deception Scams*. By comparison, the 2009 campaign lasted only one week and was called the *National Consumer Fraud Week*. Key phrases used in the 2009 promotional material were *Scams Target You: Protect Yourself, Don't Be a Victim of Scammers* and *Fight the Scammers. Don't Respond*.

The campaign has been reduced from one month in 2007 to one week in 2009. The aim in reducing the length of the campaign was to deliver a more focused, compact message that would raise awareness more forcefully than could be managed over a longer period. Since 2007, the Australian Institute of Criminology (AIC) has hosted the ACFT online Consumer Fraud Surveys. These surveys were designed to examine the types of consumer frauds that respondents were exposed to during the previous 12 months. The surveys sought to identify:

- the extent of consumer scams;
- the types of frauds or scams that attracted the most victims;
- the factors that influence becoming a victim of scams; and
- what affects reporting of scams.

An anonymous online survey was used to collect data between 1 January and 31 March of each year. This timeframe was chosen to enable responses to be collected during the ACFT fraud awareness campaign each year, which ran from 24 February to

9 March in 2008 and from 1 March to 8 March in 2009, as well as gathering responses shortly prior to, and following, the campaign period. This was done in order to gauge the effect of the campaign on survey response rates. The surveys contained a mixture of forced-choice responses and open-ended questions about respondents' exposure to, and victimisation from, consumer scams (see *Appendix 1* and *Appendix 2*).

In 2008, information was sought on four specific consumer scams types:

- lottery and prize scams;
- AFF scams;
- phishing; and
- financial advice scams.

An 'other' category was also included to capture any scams outside of these categories.

While the 2009 survey instrument was based on the format used in previous years, the questions were updated to include new fraud categories, including new questions on identity fraud and loss of personal information. In addition, respondents' motivations for not responding to scams were also investigated. In 2009, three new scam categories were added to the list above. These were:

- inheritance scams;
- work from home scams; and
- dating/romance scams.

Survey limitations

Collecting data on the nature and extent of fraud is notoriously difficult, as victimisation is often under-reported and the methods used to deceive people are complex. Under-reporting occurs for a number of reasons. In some cases, it is because the victim is unaware that the incident actually involves fraud. In addition, as this survey used self-reported data on victimisation, it is possible that some respondents may have reported incidents in which they felt they had been exploited, but which were not actually illegal.

The findings from the surveys can be used to provide insight to the experiences of individuals in relation to their exposure to, victimisation from, and reporting of consumer fraud scams in each year and can highlight any emerging scam types that authorities and individuals should be aware of. However, due to limitations such as self-selection bias among respondents, different timeframes for the two surveys and changes in questions between the 2008 and 2009 ACFT surveys, the results cannot provide a robust measurement of consumer fraud victimisation rates in Australasia, nor measure the success of the entire 2008 Fraud Fortnight campaign or 2009 Fraud Awareness Week. The results are also insufficient to determine whether the two campaigns increased people's awareness of consumer frauds and scams or accurately measured trends over time. Therefore, the findings from this survey should be interpreted and used with these limitations in mind.

In both the 2008 and 2009 Consumer Fraud Surveys, it was found that the majority of people who received a scam invitation did not respond. This result was not unexpected, as similar findings have arisen both in previous ACFT consumer fraud surveys and in other studies conducted on fraud both nationally and internationally. Despite this, consumer fraud remains a concern because of the large number of attempts to perpetrate fraud, the serious financial losses that successful frauds involve and the pain and humiliation that the fraud can inflict on victims.

Results

In 2008, 919 people responded to the Consumer Fraud Survey and in 2009, there were 708 respondents. The results were not combined in the analyses conducted in this report, as the surveys used different sampling frames and the questions were altered slightly which made direct comparisons between questions difficult. In both the 2008 and 2009 Consumer Fraud Surveys, the majority of people who received a scam invitation did not respond and the main method of receiving a scam invitation was via email.

In 2009, the types of scams affecting respondents differed from previous years, with work from home scams attracting the most victims, compared with previous years where the lottery scam attracted the most victims. This is possibly due to the evolution of scam invitations, but may also be a result of the inclusion of the new scam categories included in the 2009 survey.

A potential problem when collecting self-report data on victimisation is that it is often difficult to determine the difference between legal and illegal invitations. For example, in the case of premium SMS services, it is difficult to determine the legitimacy of text messages as respondents, who may have willingly signed up to a legitimate premium SMS service (such as a ringtone subscription), but may not have read the terms and conditions detailing the relatively high cost of some services and mistakenly attributed the high cost as evidence of scam, even though it is not one. Therefore, there was a risk in the ACFT surveys that legal invitations were included by respondents due to their ambiguous nature, which may artificially inflate reported figures.

In the 2008 survey, and to a lesser extent the 2009 survey, many of the 'other' responses belonged in one of the four specified scam categories. This indicates that some respondents may have been unclear about what constituted a particular type of scam according to the definitions provided. This reflects the constantly changing nature of scams, which scammers must refine in order to acquire new victims. It also demonstrates the difficulty in defining scam types because of their evolving nature. The inclusion of new categories may also affect the rates of victimisation for each scam type each year, making it difficult, if not impossible, to compare the yearly rates for each category with any accuracy.

The study by Titus, Heinzelmann & Boyle (1995) found that fraud attempts were less likely to be successful if the target had previously heard of the fraud type. This supports the current survey results that found that people appear to be more vulnerable to new scam types. It also reinforces the importance of the ACFT annual awareness campaign in drawing consumer fraud to the public's attention and in particular, emerging scams.

The reported victimisation rates in both the 2008 (18%) and 2009 (17%) surveys were higher than those found in similar surveys, such as the *Personal Fraud Survey* conducted by the ABS (2008), which obtained a random sample of individuals from the population as part of the 2007–08 ABS *Multi-Purpose Household Survey*. In the ABS survey, 38.5 percent of the sample had been exposed to a scam and five percent were a victim of personal fraud. The difference in reported rates of victimisation between ACFT and ABS respondents is likely due to a self-selection bias among respondents in the ACFT surveys (often seen in this type of voluntary survey), where those with a pre-existing interest in the topic, or personal experience of victimisation, are more likely to respond.

In 2009, the survey drew a distinction between money lost to scams and personal information lost to scams. One finding highlighted the large difference between victims of lottery scams who reported a financial loss (5%) compared with those who reported a loss of personal information (14%). A similar difference was seen with 'phishing' scams, where a perpetrator copies electronic communication from a legitimate business (eg masquerades as a bank) to try to access a victim's legitimate confidential information. In phishing scams, just 0.8 percent of phishing victims lost money to the scam, but 7.4 percent lost personal information. These results suggest that, like phishing attacks, the lottery scams reported by victims in the sample initially targeted personal information rather than requesting upfront payments.

As supported by previous research, it appears that prior knowledge of a scam (such as receiving similar offers in the past or being made aware of the scam via the media or other public source) was a key factor in choosing not to respond.

In the 2009 survey, there were differences in whether respondents viewed different scam types as offences. Work from home scams and scams in the 'other' category had the fewest number of respondents who considered them to be a crime despite them being the scam types that elicited the highest numbers of victims. It is important to increase the level of awareness that scams are illegal and should be reported just as any other crime would be.

In addition to the findings above, the relationships between the following variables were found to be statistically significant through chi-square analysis. In 2008, only victimisation, age and sex were analysed, however, in 2009, the focus of further analysis included income, victimisation, sex and reporting. These results reflect the sample population of these particular surveys only and should not be extrapolated to the general population.

2008

There was a statistically significant relationship between age and positive response to scams in general:

- the 45–54 year age group was less likely than expected to respond to a scam; and
- the 55–64 year age group was more likely than expected to respond to a scam.

There was also a statistically significant relationship between age and positive response to specific scam types:

- the 55–64 and 65+ year age groups were more likely than expected to respond positively to lottery scams; and
- the 55–64 year age group was more likely than expected to respond positively to AFF and personal information (phishing) scams.

2009

There was a statistically significant relationship between sending/losing money in a scam and losing personal information.

- those earning less than $20,000 per annum were more likely than expected to send personal information to a scam; and
- those earning more than $80,000 per annum were less likely than expected to send personal information to a scam.

Income and reporting a scam also had a significant relationship:

- those earning over $80,000 per annum were less likely to report a scam to family and friends than those earning less; and
- those earning less than $20,000 a year were more likely than respondents from other income brackets to report a scam to a formal agency (eg police, Australasian Competition and Consumer Commission (ACCC)).

Victimisation and reporting

Findings include:

- Being the victim of a scam increased the likelihood of reporting a scam to a formal agency.
- Those who sent money were more likely than those who did not send money to report a scam to:
  - a formal agency (eg ACCC, police, Consumer Affairs etc); and
  - family and friends (informal reporting).
- Those who sent personal information were more likely than those who did not send personal information to report the scam to a formal agency.
- Those who sent personal information were more likely than those who did not send personal information to report to the scam in general (ie either family and friends or a formal agency).

There was a statistically significant relationship between age and reporting:

- the 25–34 year age group was less likely than expected to report a scam to either a formal agency or family and friends; and
- the 55–64 year age group was more likely than expected to report a scam to either a formal agency or family and friends.

Victimisation and region

Findings include:

- respondents from Western Australia were less likely to respond positively to a scam; and
- respondents from Tasmania were more likely to respond positively to a scam.

Victimisation and perception of crime

Findings include:

- being a victim significantly increased a respondent's perception that all scams are criminal offences; and
- victims were more likely to consider work from home scams as a crime.

Region and reporting

Findings include:

- respondents from New South Wales were more likely to report a scam; and
- respondents from Western Australia were less likely to report a scam.

The sex of the individual was not a significant factor for victimisation in either the 2008 or 2009 surveys.

Whereas the findings listed above were statistically significant, it is important to note that the strength of most of these relationships was only moderate and in some cases, the relationship was relatively weak. This indicates that other factors may be involved in the findings and caution should be exercised when interpreting the results. As such, further investigation into these relationships and other factors that may influence victimisation and reporting may facilitate more beneficial public education campaigns. For example, it may be more beneficial to target older rather than younger age groups about lottery scams and managing requests for personal details. However, further research is needed to determine whether the findings from these surveys can be generalised to the broader population.

Suggestions for future campaigns

Besides general information collected on scams, the ACFT survey could be well-placed to identify emerging trends in scam typologies and collect annual data on victimisation, although due to the evolving nature of scams, it would be difficult to map some trends over time. Some suggestions include:

- A survey addendum be included each year that focuses on a particular theme or victim group. As each year of the ACFT awareness campaign usually has a thematic focus—such as the 2008 *Seduction and Deception Scams*—the addendum could be developed to tie in with the theme of each campaign. This would allow a focus on any newly emerging or increasingly prevalent scam types identified in the previous year's campaign.
- The findings from the survey regarding the different rates and types of victimisation by age group and income need to be researched further to determine if these differences can be used to more efficiently target campaign messages to the most appropriate audience.
- The need to encourage reporting of scams was also evident in the findings, as the stigma and embarrassment associated with being scammed may be responsible for the low reporting rates. It may be useful in future campaigns to attempt to change public attitudes about scam victims, thereby potentially increasing reporting rates.
- The results from the 2009 survey shows that having been previously exposed to a recognised scam type, either by receiving an invitation or seeing information in the media or via some other public source, is a factor in preventing people being victimised. Therefore, raising awareness of scam types may be an effective way in which to reduce victimisation and lends support to the overarching ACFT approach of a wide-reaching media campaign on fraud awareness.

Introduction

What is fraud?

Fraud, although not a specific offence type in most Australian legislation, is a generic term used to describe a category that contains a diverse and varied list of offences. All fraud-related offences do, however, possess the common features of obtaining a benefit through the use of deception or dishonesty (see ABS 2008; Hayes & Prenzler 2003; Levi & Burrows 2008). Fraud has also been described as being 'highly rationalised and [involving] intentional deception' (Hayes & Prenzler 2003: 3). Similarly, the victims of fraud are diverse and may include businesses, corporations, or individuals at a professional or consumer level.

The problems associated with measuring the extent of fraud are well-documented. While attempting to measure the impact of fraud in the United Kingdom, Levi and Burrows (2008) found limitations caused by the disparity in definitions of fraud, varying levels of willingness by companies or individuals to divulge losses, time lags in the reporting and detection of fraud and difficulty in determining the geographical location of the perpetrators. Under-reporting is one of the main challenges to measuring the extent of fraud. Rollings (2008) estimated that only 25 percent of fraud is reported to an agency such as the police.

Measuring fraud is further complicated by three factors described by Mayhew (2003). The first is the wide range of fraud types. From small-scale credit card fraud through to major corporate crime costing millions of dollars in one transaction, the numerous methods used by perpetrators make obtaining accurate data across the spectrum of fraud types difficult. The second complicating factor in measuring fraud is that the costs of detected fraud are not always known, as victims might not be able to accurately estimate their losses (Mayhew 2003). The third is the volume of 'hidden' fraud, which is fraud that does not become known to police, consumer agencies, or even to the individual or organisations involved. Unlike more common crimes such as car theft, where the victim is aware the crime has taken place (even if they do not report it), some victims of fraud are not even aware they are victims. As Levi and Burrows (2008) highlight, because part of the intention of the fraudster is to deceive the target and make them believe a transaction is legitimate, the fraud incident may not be recognised by the victim as an offence. Some examples of areas where hidden fraud is likely to occur include taxation, benefits and insurance. However, hidden fraud may also work in reverse, where individuals incorrectly identify themselves as victims when they are not actually the target of a crime; rather, they participated in a poor investment.

Despite these limitations, considerable work has been undertaken to estimate the extent and cost of fraud in Australia and overseas. In Australia, Stamp and Walker (2007) estimated that fraud generated $3.16b in proceeds annually. Rollings (2008) estimated that in 2005, the cost of fraud (as opposed to Stamp and Walker's estimates of proceeds) was $8.5b, making it the most costly of all crime types. Overseas, the total estimate of fraud in the United Kingdom in 2008 was £30.5b, with the bulk of this loss coming from the public sector (NFA 2010). Recent estimates of the cost of public sector fraud in the United Kingdom was considered to be at least £25b a year, which includes £18b of lost taxes and £7b against public expenditure (NFA 2010). In 2005, fraud against private individuals in the United Kingdom was estimated at £2.75b (Levi et al. 2007).

In regards to corporate rather than individual victimisation, a survey conducted by KPMG in 2008 reported that 45 percent of private and public sector organisations had experienced at least one incident of fraud between February 2006 and January 2008 (KPMG 2009). The fourth biennial *Global Economic Crime Survey* conducted by PricewaterhouseCoopers (2007) found half of all Australian businesses reported that they had experienced 'economic crime' within the past two years, compared with 39 percent in the Asia–Pacific region and 43 percent globally. Kroll's *Global Fraud Report* (2009) reported from a survey of almost 900 senior executives worldwide that in the past three years, 85 percent of firms had suffered some form of corporate fraud. More specifically, fraud perpetrated in the 2008–09 financial year on Australian-issued payment instruments totalled 446,713 transactions with a value of $173,691,179. The total number of credit card frauds perpetrated in Australia was 173,592 with a value of $63,892,492 (APCA 2009).

Defining consumer fraud

Fraud can be targeted at a range of entities, including businesses and governments, as well as at individuals and consumers. The focus of this report is consumer fraud, also known as personal fraud. Consumer fraud is not a new phenomenon, however, the expansion of the internet and an increased capacity to send spam email has led to an increase in the number of fraudulent requests sent to internet users. *Spam* is the electronic equivalent of junk mail, where unsolicited, bulk transmissions of emails are sent to email account holders (AIC 2006), therefore, increasing the speed and amount of fraudulent invitations that can be sent. This is done at a negligible cost to the 'spammer' or person sending the emails.

Unsolicited scam emails comprise the majority of consumer frauds. The ABS (2008: 5) defined a consumer scam as

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

This follows an earlier definition by Titus (1999: 2), in which personal fraud was described as

> a type of fraud that involves some form of communication between victim and offender, and the deliberate deception of the victim with the promise of goods, services or other benefits that are nonexistent, unnecessary, were never intended to be provided, or were grossly misrepresented.

Consumer fraud can be classified into four main categories, based on the methods of deception involved (see Smith 2007):

- *AFF schemes*—the offender pretends to sell something that does not exist while taking money in advance, or offers a large reward for which an upfront fee must be paid;
- *non-delivery and defective products and services*—the offender seeks to supply goods or services of a lower quality than the goods or services paid for, or fails to supply the goods and services at all;
- *unsolicited and unwanted goods and services*—the offender persuades customers, through deceptive marketing techniques, to buy something they do not really want; and
- *identity fraud*—a benefit is gained, or obligations avoided, through the use of a fabricated, manipulated, or stolen/assumed identity.

Consumer scams (herein referred to as 'scams' unless otherwise specified) usually involve elements of AFF or identity fraud and sometimes both. The invitations require the intended victim to pay an

upfront fee, or they require the intended victim's personal details (such as bank or credit card details) to participate. Scam invitations can be delivered through any medium including mail, email, telephone and the internet (through methods such as provision of internet services, bait advertising and via online auctions). Scams primarily utilise one form of communication, however, they can be adapted to any of the delivery methods listed above.

Identity fraud

The ABS (2008: 5) defined identity fraud as

> the theft of a pre-existing identity without a person's consent, where the person's name, date of birth, address or other personal details are used to engage in fraudulent activities.

While consumer fraud is invariably about obtaining money, these schemes often seek to obtain personal information from victims which can then be used for a variety of identity-related crimes. Financial gain is, however, almost always the eventual goal, although as highlighted earlier, identity fraud can also be used for other purposes such as avoiding obligations (eg taxation). In Australia alone, identity fraud has been estimated to affect three percent of the population—or nearly half a million victims (n=499,500) annually (ABS 2008).

Identity fraud is often considered to be increasing (Doig 2006) and, undoubtedly, advancing technologies make creating false identity documents easier and have increased the ease with which stolen identities can be used. Fear of identity fraud is high, with a 2007 survey finding that over 40 percent of respondents were concerned about the likelihood of having their identity stolen via the internet, over 45 percent that their credit card would be stolen and over 50 percent that their credit card details would be used illegally on the internet (Roberts & Indermaur 2009). Respondents to the survey were more concerned about the likelihood of victimisation from these identity crimes than of physical and sexual assault (Roberts & Indermaur 2009).

In 2008, the ABS (2008) reported five percent of Australians (n=806,000) were victims of personal fraud in the previous 12 months. Of these, almost half a million victims lost money (n=453,100) with a combined financial loss of almost $1b ($977m). On a global scale, van Dijk, van Kesteren and Smit (2008) found one in 10 people had been a victim of consumer fraud in any given 12 month period during which the surveys were conducted. Concerns also were raised that internet-based and credit card fraud may overtake traditional forms of property crime such as pickpocketing to become the most common type of property crime (van Dijk, van Kesteren & Smit 2008).

How scams target potential victims

Consumer scams target potential victims in any of the following three ways—syntactic, semantic and blended methods (Smith 2008). *Syntactic attacks* involve exploitation of technical vulnerabilities such as the use of malicious computer code transmitted via email; *semantic attacks* involve the use of social engineering or the exploitation human vulnerabilities for deception; while *blended attacks* entail the use of technical vulnerabilities to facilitate social engineering. Avoiding syntactic attacks, such as through the use of malware (malicious software), requires continuous and regularly upgraded protection against constantly updated malicious software; while avoiding victimisation through semantic methods requires knowledge of the possibility of fraud on behalf of the victim and a willingness to avoid it (Smith 2008).

Scams are constantly changing by either advancing earlier scams or modelling legitimate offers (UKOFT 2009). As such, new scam offers are likely to be disproportionately successful when compared with more well-known scam types because they are less likely to be recognised as a scam (Titus, Heinzelmann & Boyle 1995; UKOFT 2009). In addition, while they are illegal, scams are usually marketed in the same way as genuine products. Scamming techniques include the use of all elements of the 'marketing mix' (ie product, price, place and promotion) and build a relationship between the scammer and the victim to increase the likelihood of success (UKOFT 2009).

Consumer affairs agencies are reporting increases in the number of complaints about scams. In South Australia, the Office of Consumer and Business Affairs reported that scams were the most commonly

complained about issue in 2007–08, comprising 1,217 complaints out of a total of 5,410 complaints (22.5%). Of the 1,217 complaints, 1,000 concerned Nigerian-type scams (AFF) and 217 concerned 'get-rich-quick' schemes (OCBA 2008). The Australian Competition and Consumer Commission's (ACCC) SCAMwatch initiative also received 1,875 calls and 6,933 complaint emails in 2007–08 (ACCC 2008a). In 2008, the ABS found that two percent (n=329,000) of the population in Australia had been a victim of a scam in the previous 12 months. Recently in the United Kingdom, the UK Office of Fair Trading (UKOFT) estimated that 3.2 million adults in the United Kingdom fall victim to consumer scams, losing £3.5b (UKOFT 2009).

Types of consumer scams

The following section details the more common types of consumer scams. The list is not exhaustive and many scams may include a combination of more than one type of scam. More details on these can be found in the 2008 edition of *The Little Black Book of Scams*, a publication produced by the ACCC that outlines most types of consumer scams that have been identified in Australia.

Advance fee fraud (Nigerian/419 scams)

AFFs, more commonly known as 'Nigerian' or '419' scams (based on the legislative section number that refers to the scam in Nigeria), are some of the most common and most often complained about scams in Australia (ACCC 2008b). While these types of schemes have been used for centuries, AFF in the format in which it exists today has been seen since the late twentieth century when letters were sent to individuals asking for assistance in transferring money out of Nigeria in return for a sizeable financial reward (Smith, Holmes & Kaufmann 1999). Widespread use of the internet since the late 1990s has enabled this type of fraud to flourish due to the ease with which invitations can be sent via email (Holt & Graves 2007). The format of AFF and the content used in invitations has changed over recent years, but the scam invitations continue to utilise a basic format that involves providing an upfront payment in order to receive a later, much larger, payment in return.

Common methods used in AFF include, for example, a wealthy diplomat who needs assistance transferring a large sum of money (often several million dollars) out of their country, of which an individual can receive a cut if that individual pays upfront fees relating to the transfer. Similarly, some requests involve a story about 'black cash' where bank notes are painted in a black liquid to disguise them while smuggling them out of the country and victims are told that the notes can be washed clean afterwards. The advance payment is for solvent needed to clean the black from the paper. However, upon receipt of any 'cash' it becomes apparent they are nothing more than blank pieces of paper. Other more apparently altruistic scams involve a request to assist a dying person distribute their money to various charities and the intended victim is offered a percentage of the sum as payment.

Another variation to the AFF format is the overpayment scam. This scam involves the fraudster purchasing goods and sending a cheque as payment that is more than the advertised price. Once the cheque is banked, the victim is asked to refund the extra money through a transfer, however, it then becomes apparent that the original cheque has bounced and the victim has lost the transferred money.

A recent variant entails the use of online motor vehicle sales in which unsuspecting sellers are asked by prospective buyers to send money to facilitate the removal of the vehicle overseas, to cover so-called government fees, or other expenses associated with the sale. Similar scams involve fraudulent sellers who trick unsuspecting online buyers into parting with funds before their car is received. In reality, the vehicle never existed and the purchaser loses the fee paid.

There are many other scams that also contain upfront payments and which can be considered subcategories of AFF, however, due to the prevalence of certain types of these scams they have been discussed below as separate scam categories.

Phishing

Phishing is a form of social engineering in which the perpetrator, or 'phisher', attempts to fraudulently retrieve legitimate confidential information, such as bank account details, by mimicking electronic communications from a trustworthy public organisation. This is done in an automated fashion, most often via email (Meyers 2007). Since phishing attacks emerged in the 1990s—when phishers would steal the legitimate account details of AOL users in the United States by imitating AOL employees and coercing users into giving out passwords—there has been a dramatic increase in the number and sophistication of these attacks (Meyers 2007).

Phishing attacks will often involve contact from a victim's bank, or another trusted source, asking for personal account information to be verified through a linked website, which is then used to steal the information. More recently, phishing attacks have spread to involve SMiShing, a phishing attack via fraudulent SMS invitations and spear-phishing, a more targeted version of phishing (OECD 2008). In addition, phishing attacks can also involve the use of malware to assist the phisher and make fraudulent invitations seem legitimate. Malware, or malicious software, is installed on a computer with the intention of harming that computer or others. Malware can be installed on computers through phishing invitations and can be used to redirect users from a legitimate URL to a false website in a process known as *pharming* (OECD 2008).

Lottery and prize scams

Lottery and prize scams involve a notification of winning, or an invitation to participate in, a lottery or competition. Victims are told they have won either money or a prize, however, an advance payment of a specified amount or personal information and banking details must be sent to cover administration fees before the winnings can be collected (ACCC 2008b). Once sent, the money and the perpetrator disappear.

Inheritance scams

Inheritance scams involve a notification by a purported foreign lawyer of a deceased estate from which the victim can claim a substantial amount of money. These scams can be delivered on the premise that the deceased is a distant relative and that the victim is entitled to the inheritance, or that the deceased has the same name as the victim and the lawyer will fraudulently claim the inheritance using the victim's name. In both cases, the victim is told that payment will be required to cover the upfront fees associated with the inheritance with the false promise of later reimbursement from the inheritance money (ACCC 2008b).

Financial investment scams

Investment scams involve invitations to invest in shares, a company, product or other financial opportunity with the promise of large returns. These financial scams often involve investing in pyramid schemes. Pyramid schemes operate with the primary purpose of recruiting further participants. Individuals are solicited to join and pay entry fees, and are given payments for each new subscriber they recruit. Income is generated only from the new subscription fees, which are used to make payments to the existing participants. When the scheme reaches a level where there are not enough new subscriptions to pay the existing participants the scheme falls apart. Pyramid schemes are also sometimes known as 'Ponzi' schemes (Grabosky, Smith & Dempsey 2001).

Work from home scams

Fraudulent offers to work from home can operate in two ways—they can be a subcategory of AFF or they can be an invitation to become a money mule. Where the scam operates as a subset of AFF, the jobseeker will be offered a job, but they are asked to provide upfront payments for fees or expenses relating to their employment. Once the money is paid, the job offer will disappear.

The other purpose of a work from home scam is to recruit money mules. A money mule works to facilitate money laundering by passing funds through nominated bank accounts that are designed to disguise the illicit origins of the funds. A money mule is a person unrelated to the original criminal act but through the process of money laundering, even when done unwittingly, they become an integral part of the criminal activity.

The basic process of money muling through work from home scams is outlined below:

- job advertisement offers work as a 'financial agent' or similar;
- jobseeker signs up and opens, or allows access to, a domestic bank account;
- fraudsters transfer money from scam victim's to jobseeker's [now money mule's] account;
- jobseeker transfers money to fraudster overseas;
- jobseeker receives 'commission';
- job seeker is open to prosecution by domestic authorities for money laundering (AIC 2007: np).

Becoming involved in these types of scams is particularly risky as while it is possible that those who participate in these schemes are unaware of the true nature of their employment, the practice is illegal and therefore anyone involved in these operations risks prosecution.

Dating/romance scams

Dating and romance scams involve initiating a false relationship through dating websites, social networking or via email with the intention of later defrauding the victim. These relationships are often initiated online by scammers using false profiles on legitimate dating websites. After a period of communication and when the scammer has obtained the victim's trust, an 'emergency' arises and the victim is asked to send money overseas to assist the scammer in various ways, including to pay medical bills, fees or to purchase a plane ticket to visit the victim (ACCC 2008b).

Victims of consumer fraud

Much criminological research focuses on violent and property crime, however, the effects of fraud victimisation can arguably be more devastating to victims. The debt from unmet financial responsibilities as a result of fraud can escalate (Shoepfer & Piquero 2009) and victimisation is usually a violation of trust that is not often associated with street crime victimisation (Titus & Gover 2001). Several studies have examined the relationships between demographic factors and victimisation, however, victim age is the only factor that has been consistently found to be significant by researchers. Interestingly, the age group found to be most at risk varies across studies (see Smith & Budd 2009; Titus, Heinzelmann & Boyle 1995; van Wyk & Benson 1997; van Wyk & Mason 2001). This indicates that demographic factors alone are not an adequate predictor of potential victimisation.

Fraud, unlike traditional conceptions of theft, generally assumes a relationship between the victim and the offender (Doig 2006). This is often the case with consumer scams, where the victim cooperates or acts in some way that facilitates their victimisation. Titus and Gover (2001) explain 'victim cooperation' in consumer fraud as operating on a continuum from no involvement to a considerable amount of participation. Three examples are given (Titus 1999: 2):

- *No facilitation*—despite having followed all the recommended precautions, a woman discovers in her credit card statement that she has been the victim of an identity fraud.
- *Some facilitation*—A man responds to a 'cold' phone call and contributes to a charity without investigating and learning that it was a phony.
- *Considerable facilitation*—Having responded to an ad for a [seemingly highly profitable] investment opportunity [that subsequently led to becoming a victim of] a Ponzi scam, a man is burned again in a 'recovery scam.' [In another scenario], over a period of years a woman loses many thousands of dollars in a series of one-in-five scams but continues to participate.

A recovery scam is 'an offer to assist the victim to recover his/her money' (Titus 1999: 8). The UKOFT (2009: 6) suggests that victimisation involves an error of judgement on behalf of the victim and sought to identify the categories of decision error and the psychology of persuasion in victimisation. Scams include:

- 'appeals to trust and authority';
- visceral triggers which 'exploit basic human desires and needs—such as greed, fear, avoidance of physical pain, or the desire to be liked—in order to provoke intuitive reactions and reduce the motivation of people to process the content of the scam more deeply';

- invitations personalised to the victim and an emphasis on the urgency and scarcity of the offer; and
- a disproportionate relation between the size of the reward and the cost of trying to obtain it, therefore making the risks seem worth the reward.

Another important element in scam victimisation is that a scammer's participation often occurs gradually. Scammers often ask for small steps of compliance from the victim to draw them in and make them feel committed to continuing to send money (UKOFT 2009).

Counterintuitively, some types of scam victims have been found to have better than average knowledge in the area they were victimised (UKOFT 2009). For example, one study found that people who play the lottery legitimately were more likely to fall victim to a lottery scam (UKOFT 2009). For these victims, the prior knowledge of the lottery system increased rather than decreased the risk of victimisation as would otherwise be expected. A possible explanation for this anomaly may be that regularly playing lotteries has normalised the activity for these individuals, however, this should be researched further.

Conversely, research shows that there are factors that can play a role in reducing the likelihood of victimisation. The following influences were considered significant in reducing the likelihood of a successful fraud attempt (Titus, Heinzelmann & Boyle 1995):

- the offender was a stranger;
- the initial contact was by telephone or mail;
- the potential victim had previous knowledge of the fraud; and
- the potential victim attempted to investigate the proposition before responding.

Having previous knowledge about fraud is a significant factor in reducing victimisation and is of particular interest in this current report, in light of the ongoing ACFT fraud awareness campaigns.

Victims of consumer fraud can sometimes be viewed harshly in light of this perceived contribution they make to their victimisation and are often labelled as greedy or gullible (UKOFT 2009) or are seen to have violated rules of preventative behaviour by failing to take enough precautions against victimisation (Walsh & Schram 1980). However, these labels fail to recognise the complexity of victimisation. This perception of fraud victims can also have a negative effect on the reporting behaviours of fraud victims. Victims may not report their experience because of feelings of guilt surrounding their victimisation, or if they perceive their losses are not as worthy as other causes pursued in the criminal justice system (Walsh & Schram 1980).

Fraud and cybercrime

While fraud does not necessarily involve the use of the internet or computers, and cybercrimes do not necessarily involve elements of fraud, an undeniable relationship exists between them. The internet has increased access to material used for criminal purposes, improved the ease of creating fraudulent documents and increased the number of jurisdictions from and into which crimes can be committed (Doig 2006). The numbers of bulk spam emails containing fraudulent invitations have increased as advances in technology have made their dissemination easier. Increasing transfer of everyday activities to the internet, such as banking and shopping, also creates further opportunities to commit fraud. In addition to the threat from AFF and phishing, online auction sites have been identified as an area where fraud is likely to increase alongside growing sophistication of technology (Choo, Smith & McCusker 2007).

Fraud awareness and prevention: The Australasian Consumer Fraud Taskforce

Since 2006, the ACFT has participated in the fraud prevention and awareness-raising activities undertaken each year by members of the International Consumer Protection and Enforcement Network. As part of this, an annual awareness campaign has been run in Australia and in New Zealand since 2007. The mission of the ACFT is to increase enforcement activity around frauds and scams; raise awareness though annual campaigns for consumers;

engage private sector and community groups to participate in the campaign and share information on fraud and scams; and to generate interest in research for the area (see www.SCAMwatch.gov.au for more information). In both 2008 and 2009, the ACFT included 19 government regulatory agencies and departments, alongside private sector, community and non-government partners.

Members of the taskforce include:

Australian Government

- Attorney General's Department;
- ABS;
- Australian Communication and Media Authority;
- ACCC;
- AIC;
- Australian Securities and Investments Commission;
- Australian Federal Police; and
- Department of Broadband, Communications and the Digital Economy.

State and territory governments

- Australian Capital Territory Office of Fair Trading;
- Consumer Affairs Victoria;
- New South Wales Office of Fair Trading;
- Northern Territory Department of Justice;
- Queensland Department of Fair Trading, Tourism and Wine Industry Development;
- South Australian Office of Consumer and Business Affairs;
- Tasmanian Office of Consumer Affairs and Fair Trading; and
- Western Australian Department of Consumer and Employment Protection.

New Zealand Government

- New Zealand Commerce Commission and SCAMwatch New Zealand (New Zealand Ministry of Consumer Affairs).

In 2008, the annual awareness campaign in Australia and New Zealand ran for two weeks under the title *Fraud Fortnight*, with the theme *Seduction and Deception Scams*. By comparison, the 2009 campaign ran for one week and was called the *National Consumer Fraud Week*. In 2009, key phrases used in the promotional material were *Scams Target You: Protect Yourself, Don't Be a Victim of Scammers* and *Fight the Scammers. Don't Respond*. Since 2007, the campaign has reduced from one month to one week. The shorter duration aimed to reduce potential campaign 'fatigue' from diluting the messages of the ACFT (see Smith & Akman 2008).

As with the previous campaigns, an anonymous online survey was conducted by the AIC to obtain an indication of the exposure and victimisation of respondents to scams. The survey was developed with input from ACFT members and was open to the public and all ACFT members. Questions were asked about the types of scams individuals encounter, whether they respond to the scams, how much money is lost, and their perception of scams in general. The 2008 and 2009 survey results form the basis of this report.

Method

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

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

Each year, an anonymous online survey hosted by the AIC has been used to collect data between 1 January and 31 March. This timeframe was chosen to correspond with the ACFT fraud awareness campaign of each year, which ran from 24 February to 9 March in 2008 and from 1 March to 8 March 2009, as well as collecting 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 in which 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 experiences and possible victimisation.

Links to the survey were available on the AIC website and other ACFT member websites, and the survey was highlighted in ACFT media releases throughout Fraud Fortnight in 2008 and the Fraud Awareness Week in 2009. 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.

The surveys contained a mixture of forced-choice responses and open-ended, qualitative questions about respondent's exposure to, and victimisation from, consumer scams (see *Appendix 1* and *Appendix 2*). These questions were developed in consultation with the ACFT committee members. In 2008, information was sought on four identified consumer scams:

- lottery and prize scams;
- AFF scams;
- phishing; and
- financial advice scams.

An 'other' category was also included to capture any scams outside of these categories. In 2009, three new scam categories were included. These were:

- inheritance scams;
- work from home scams; and
- dating scams.

While the 2009 survey instrument is based on the format used in previous years, the questions were updated to include new fraud categories and questions on identity fraud and loss of personal information. Based on observations of how people interpreted the questions over the past few years, all but two questions were re-worded to improve clarity and comprehension of the survey.

After the 2008 survey concluded, it was suggested that another worthwhile addition to the survey would be to include questions to determine how people identified a request as a scam. This was absent from the ACFT survey and is often missing from consumer fraud literature. A greater understanding of the decision-making process involved in identifying a scam and what resources they use to assist them make this decision (eg the media, word of mouth, own judgement) was considered beneficial on at least two levels—it would provide a greater understanding of why people respond to scams and the findings could help direct scam prevention efforts by increasing the amount of available information about scams in the areas that people get their information from. For example, if people use the internet to check if a request is fraudulent, then promoting scam warning information on websites will be valuable. Similarly, if most people get their information by word of mouth, then generating discussion about fraud among people in the community will need to be a priority of any future campaigns. As such, a question was included in the 2009 survey to try to explore this issue. Knowledge about how to prevent victimisation will be used to help determine what should be included in future awareness and prevention campaigns.

Limitations of the surveys

The 2008 and 2009 AIC surveys experienced the same methodological constraints as those identified in 2007 (see Smith & Akman 2008). Limitations associated with the relatively small sample size and the self-selection bias of the sample make generalising the findings to the wider population problematic. Directly completing the survey was also limited to those who had computer access, however, this was not considered overly restrictive, as SCAMwatch employees were able to fill out surveys over the phone on the client'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 due to the time lapse between when they are received or carried out, identified by the victim and then reported (if indeed they are; Levi & Burrows 2008). The timeframe in the 2008 and 2009 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 their exposure to, victimisation from, and reporting of, consumer fraud scams, identifying reliable trends over time cannot be confidently reported on the survey data. There are two reasons for this. First, Fraud Fortnight and Fraud awareness week timeframes are not the same (2 weeks in 2008 compared with 1 week in 2009); and second, the 2009 survey format and questions were different from the 2008 survey. As a result, the survey results cannot provide a robust measurement of consumer fraud victimisation rates in Australasia, or of the success of the entire 2008 Fraud Fortnight campaign or 2009 Fraud Awareness Week. The results are also unable to identify whether the two campaigns increased people's awareness of consumer frauds and 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. However, when cell sizes were of sufficient magnitude, additional statistical testing was performed to look for relationships and/or for differences between selected variables. In 2008, age and sex were the focus of such testing. In 2009, income, victimisation, sex and reporting behaviours were explored. Due to the non-parametric nature of the data, chi-square statistics were used to test for the statistical significance of relationships between variables, with $p<.05$ set as the threshold for determining statistical significance. In the 2008 survey, Cramér's V statistic was used to estimate

correlations between the categorical variables (de Vaus 1995). The chi-square test was performed if the expected counts were equal or greater than five in 80 percent of cells (Yates, Moore & McCabe 1999). The strength of the association between the variables was interpreted based on a scale adopted by Tomison (1999: np):

- 0.0–0.1=weak or very weak association;
- >0.1–0.2=mild association;
- >0.2–0.3=moderate association;
- >0.3–0.5=strong association; and
- >0.5–1.0=very strong association.

It should be noted that associations were reported to four decimal places and were not rounded.

Throughout the analysis, the 2008 survey results were often compared with the 2007 results. Some of the 2007 calculations may be slightly different to the results reported previously, as some questions were re-coded and re-analysed to be consistent with the 2008 calculations (as seen in Smith & Akman 2008). If responses have been recalculated, it is highlighted in the Table notes.

In 2009, direct comparisons were not made with the 2008 data (with the exception of a few questions), for a number of reasons:

- the 2008 campaign included respondents who resided outside Australia or New Zealand. In 2009, only respondents who indicated they resided inside Australia or New Zealand were used in the sample;
- both campaigns had different campaign timeframes—in 2008, the campaign ran for a fortnight, whereas in 2009, the campaign lasted one week; and
- all but two questions in the 2009 survey had either additional variables included or were worded differently to the 2008 survey.

These variations, although subtle, meant that most of the survey questions in 2008 and 2009 were not comparable. As such, the two campaigns are reported separately in this report.

The 2008 consumer fraud survey results

2008 consumer fraud awareness fortnight

The theme of the 2008 ACFT consumer fraud awareness fortnight was *Seduction and Deception Scams*, including online dating/romance scams. This was intended to address the perceived increase in prevalence of these types of scams in Australasia based on the observations of ACFT members. The ACFT engaged in a broad awareness campaign during the fortnight in both Australia and New Zealand, which was similar to the one conducted in 2007.

Responses to the Australasian Consumer Fraud Taskforce survey

Survey respondents

In 2008, 919 respondents completed the survey and all responses were used in the analysis. This was an increase of 78 responses from the 841 received in 2007. Awareness of previous campaigns was low, with only 91 respondents (10%) indicating an awareness of previous campaigns and only 13 of these (1%) indicating they had completed the survey in previous years.

Response timeframes

Of the 919 responses, 398 (43%) were completed prior to Fraud Fortnight (1 Jan–23 Feb), 331 (36%) during Fraud Fortnight (24 Feb–9 March) and 190 (21%) after Fraud Fortnight (10 March–31 March). Week to week, the highest number of responses were seen during Fraud Fortnight with 162 and 163 responses received in the respective weeks of the campaign. There was also a spike in responses during the week beginning 10 February 2008, with 129 responses in that period. Prior to this, there was a slow increase in responses leading to Fraud Fortnight, then a steady decline in the subsequent weeks.

Characteristics of the respondents

The overwhelming majority of survey participants came from the general public (78%; n=717). Just over three percent (n=32) came from an unidentified source and the rest of the respondents were affiliated with ACFT agencies. Respondents were asked if they belonged to any ACFT partner agencies so the researchers could identify if the results had been dominated by these agencies which potentially skews the results. It was found that 22 percent (n=170) were affiliated with ACFT agencies, however, this was not considered a large enough proportion to affect the results, particularly

as not all the ACFT partner-affiliated respondents are part of the taskforce, nor participated directly with Fraud Fortnight.

Most respondents were from Victoria (31%), New South Wales (24%) and Queensland (19%), with only 17 respondents (2%) reporting that they were from New Zealand. Because of the low rate of participation from New Zealand, the survey findings cannot confidently be considered relevant to New Zealand.

Table 1 shows the age and sex of respondents. Respondents were fairly evenly distributed between male (47%; n=429) and female (53%; n=487), which is similar to the 2007 results (male=49%, female=51%). Figure 1 shows a comparison of the age characteristics of respondents between 2007 and 2008. The largest single age group represented in the sample were the 25–34 year olds (25%), however, the 45–54 year old group and the 35–44 year old group (24% and 22% respectively) had

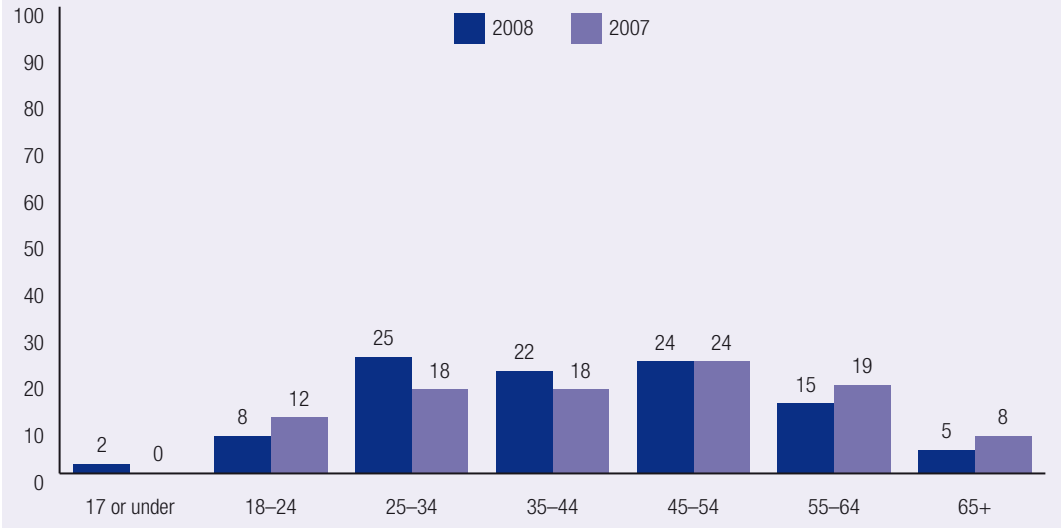
Table 1 Respondents by age in years and sex, 2008

	Respondents by sex (n)				
Age in years	Male	Female	Missing	Total respondents (n)	Total sample (%)[a]
17 or below	9	7	0	16	2
18–24	29	41	0	70	8
25–34	94	135	1	230	25
35–44	101	101	1	203	22
45–54	97	119	0	216	24
55–64	66	68	0	134	15
65+	32	14	0	46	5
Missing	1	2	1	4	<1%
Total	429	487	3	919	

a: percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2008 [AIC data file]

Figure 1 Age in years of respondents, 2007 and 2008 (%)



Source: ACFT Consumer Fraud Survey 2007 and 2008 [AIC data file]

similar respondent numbers. The same three categories comprised the most common age groups in the 2007 sample, albeit in a different order. The largest age category in 2007 was 45–54 year olds (24%), closely followed by 55–64 (19%) year olds and then the 35–44 and 25–34 year old age groups (18%).

Scam invitations

People who received scam invitations

In both 2007 and 2008, an overwhelming majority of respondents indicated that they had been contacted in relation to a scam in the last 12 months. In 2008, 90 percent of survey respondents (n=824) received a scam invitation, compared with 86 percent of the 2007 sample (n=724). In addition, in 2008 over 70 percent of those contacted indicated they received more than one scam invitation.

Table 2 compares the number of scam invitations received by scam type across the two years. There was little difference between the three most commonly received scam invitations. The most common scam was the lottery scam, with 55 percent of the total sample receiving a lottery scam invitation in 2008, similar to 2007 (56%). In 2008, lottery scams were only fractionally more common than requests for personal information (54%) and AFF requests (53%), followed by offers of financial advice at 35 percent and 'other' at 33 percent. This was a similar pattern to 2007.

Upon analysing the responses it was found that many of the answers in the 'other' category of scams actually related to scams in the four categories above. If these 'other' responses were found to match descriptions already used in the survey, they were re-coded into the corresponding category. If a new type/version of a scam was described a number of times in the 'other' category, new categories were created to highlight the emerging scam types. Thus, the 'other' category included scams such as the inheritance scam (n=38) and the work from home (n=47) scams (see Table 3). While these could be included as AFF scams, it was concluded that the typology was distinct enough to be treated as an individual category.

Other emerging scams identified in the 'other' category (see Table 3) included scams targeted at small business for advertisements, subscriptions to publications and domain names (n=23), dating and romance scams (n=14) and one account of the 'assassin' scam, where the scammer reports that he/she has been paid to assassinate the individual, but will not perform the 'hit' if the intended victim pays the scammer a sum of money. Due to the nature of consumer scams, there was some overlap with methods of delivery and scam type. As well as the scenario with AFF scams, there were also some identified mobile ringtone scams. These scams specifically target mobile phone users and involve a failure to deliver the ringtone to the phone after it is paid for. Alongside this, the mobile phone can be used as a method of delivery for lottery and prize scams. Where this occurred, any ringtone scams

Table 2 Type of scam invitation received in 2008 compared with 2007

	2008			2007[a]		
Scam invitation type[b]	Received a scam invitation (n=824)	Percentage of those who received a scam invitation (n=824)	Percentage of total sample (n=919)	Received a scam invitation (n=724)	Percentage of those who received a scam invitation (n=724)	Percentage of total sample (n=841)
Lottery	506	61	55	475	66	56
Personal information	497	60	54	461	64	55
Money transfer	487	59	53	438	60	52
Financial advice	325	39	35	302	42	36
Other	301	37	33	260	36	31

a: 2007 results recalculated to match 2008 classifications

b: respondents could respond to more than 1 category

Source: ACFT Consumer Fraud Survey 2007 and 2008 [AIC data file]

were left in the 'other' category as a distinct type of scam, whereas lottery scams via mobile phones were coded back into the lottery category with 'phone' identified as the method of invitation.

Similar classification issues were also identified with possible phishing responses. For example, the survey asked if anyone had requested personal details from them, such as a bank. Because of this specific reference to banks, it was decided that only phishing scams described in the 'other' category that involved divulging information to a fake bank request would be recoded as a phishing request. All other similar scenarios such as fake website descriptions were left as 'other' scam types.

How people receive scam invitations

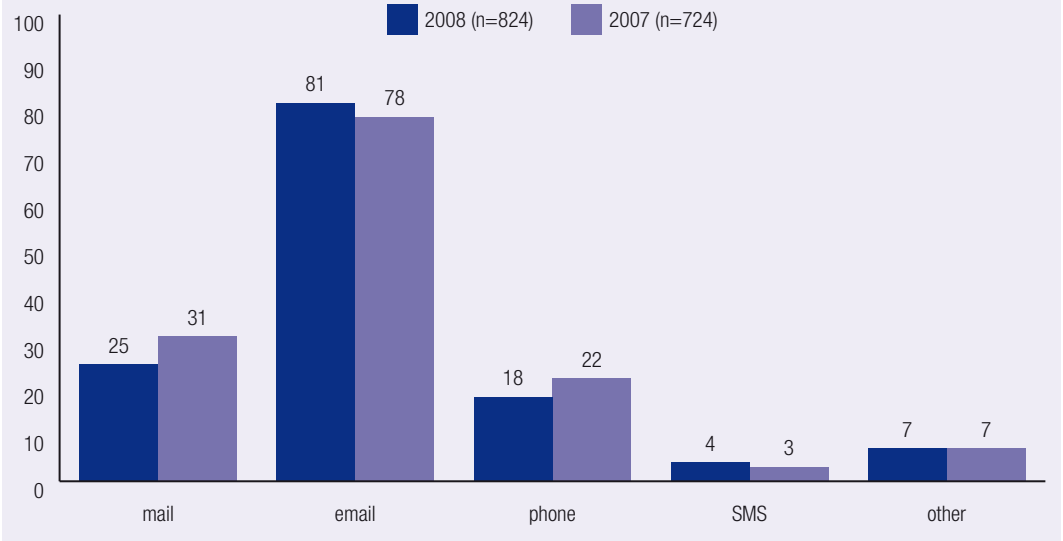
The majority of respondents (n=763; 81%) had received at least one scam invitation sent via email. This was similar to the 2007 survey where 78 percent of respondents had received a scam invitation by email. Although it was the second most common method, invitation via mail occurred for fewer than 25 percent of scams received (see Figure 2). This was followed by invitation via the phone (18%), unspecified 'other' methods (7%) and SMS (4%). These figures were almost identical to the 2007 results (see Figure 2).

Table 3 Scams invitations in the 'other' category, 2008 (n)

Scam	n
Inheritance	38
Work from home	47
Scams targeted at small business for ads, subscriptions to publications and domain names	23
Chain letters and pyramid scams	14
Dating scams	14
Phone scams (eg ringtones or unsolicited chargeable sms)	14
Assassin scam	1

Source: ACFT Consumer Fraud Survey 2008 [AIC data file]

Figure 2 Method of receiving scam invitation, 2007 and 2008 (%)



Note: respondents could be contacted via more than 1 method

Source: ACFT Consumer Fraud Survey 2007 and 2008 [AIC data file]

Consumer fraud victimisation

Responding to scams

People were considered to have responded positively to a scam if they communicated with the scammer in any way that was intended as a potential response to the request. This included communication ranging from an email enquiry through to sending money or personal details, but excluded requests to be left alone or to engage in 'scam baiting'—a process in which a person deliberately leads a scammer on with no intention to follow through with the deal. Respondents did not necessarily have to lose money to be considered to have responded positively to the scam.

In the 2008 survey, 90 percent (n=824) of respondents received some type of scam invitation, a slight increase compared with 86 percent (n=724) in 2007. Of those who received a scam invitation, approximately 20 percent (n=168) in 2008 had responded positively to a scam, compared with almost 15 percent (n=108) in 2007. Of the total sample, 18 percent (n=168) indicated in the 2008 survey that they had responded positively and 13 percent (n=108) from the 2007 survey indicated they had responded positively. Slightly more males (20%) responded positively to scams than females (17%; see Table 4). A chi-square estimate performed on the data indicated that the difference between males and females who responded positively to scams was not statistically significant.

Further tests identified a statistically significant relationship between age and the propensity of an individual to respond positively to a scam (χ^2 (6)=17.0; p<0.01), along with a mild correlation between the two categories (Cramér's V=0.1451). While there were no statistically significant differences between actual and expected incidences in responding positively to a scam for the younger age groups (17 or below, 18–24, 25–34, 35–44 year age groups), there were statistically significant differences for the older age groups. Those aged 45–54 years were less likely to respond to a scam than expected. In contrast, those in the 55–64 and 65+ year age categories were more likely to positively respond to a scam than expected. When interpreting these results, it is important to note that tests for expected frequencies only looked for differences *within* groups, not *between* them. For example, it cannot be said that the 55–64 year age group is more likely than other age groups to respond positively to scams. Instead, it indicates that the number of 55–64 year olds who responded positively was higher than expected. However, these tests are indicative of a relationship only; they cannot specify the exact nature of this relationship.

Similar patterns were found for a relationship between age and specific scam types. Statistically significant relationships were identified for lotteries and age (χ^2 (6)=30.86; p< 0.001; Cramér's V=0.1956), AFF and age (χ^2 (6)=14.75; p< 0.05; Cramér's V=0.1352) and personal details (phishing) and age (χ^2 (6)=17.49; Cramér's V=0.1472). However, these associations were considered mild. As a general rule, the older

Table 4 Age in years and sex of those responding positively to scams, 2008

	Responded positively to scams by age in years and sex (n=168)		
	Male	Female	Responded positively (%)[a]
17 or below	3	0	1.8
18–24	2	5	4.2
25–34	21	18	23.2
35–44	13	23	21.4
45–54	16	15	18.4
55–64	18	19	22.0
65+	13	1	8.3
Missing	0	1	0.6

a: percentages may not add to 100 due to rounding

Source: ACFT Consumer Fraud Survey 2008 [AIC data file]

age groups were more likely than expected to succumb to the various forms of scams—for lotteries, statistically significant differences were found for those aged 55–64 years and 65 years of age and over. The 55–64 year age group also had statistically significant differences for having a higher than expected likelihood to respond positively to AFF and personal details (phishing) scams. While these results are important, a degree of caution should be exercised in inferring trends from these results as most categories contained small numbers of responses. These low counts can affect the reliability of the results.

Scams that elicited a positive response

The 2008 survey had a higher number of reported positive responses to scams than in 2007. In addition, there was a variation in the types of scams that recorded the most victims. There was a slight decrease in the number of people victimised by lottery scams which fell from the most common scam category selected in 2007 (54%) to the second most common (32%) in 2008 (see Table 5). In 2008, scams included in the 'other' category recorded the most victims, (55%), followed by lottery with 32 percent and AFF with 26 percent. However, it is important to note that the 'other' category comprises multiple scam types. As such, lotteries were still the most commonly identified scam category to attract victims.

The survey results showed that a high number of responses in the 'other' category actually included scams that could potentially be classified as AFF scams. These include inheritance scams and work from home scams. It was decided to leave these in the 'other' category as they did not exactly fit the description given in the survey for AFF. The description required a request for money, but these frauds may have also involved requests for personal details or used another method to elicit a response. The figures for the most common 'other' scams are shown in Table 6.

Table 5 Scams that attracted the most victims from the sample in 2008 compared with 2007

	2008			2007		
Scam[a]	n (n=168)	Responded positively to a scam (%)	Total sample (%) (n=919)	n (n=119)	Responded positively to a scam (%)	Total sample (%) (n=841)
Personal information	34	20	4	22	19	3
Financial advice	34	20	4	32	27	4
Lottery	53	32	6	64	54	8
AFF	44	26	5	30	25	4
Other	92	55	10	46	39	6

a: some respondents fell victim to more than 1 scam, so recorded multiple responses

Source: ACFT Consumer Fraud Survey 2007 and 2008 [AIC data file]

Table 6 Scams in the 'other' category that elicited a positive response, 2008 (n)

Scam type	Number of positive responses
Work from home	18
Inheritance	5
Dating scam	4
Scams targeting small business	7
Betting software	7

Source: ACFT Consumer Fraud Survey 2008 [AIC data file]

Money lost to scams

In the 2008 survey, 62 respondents reported losing money to a scam, while seven indicated they would rather not answer and one 'did not know'. Those who lost money represented almost seven percent of the total sample and comprised 37 percent of those who had responded positively to a scam. In 2007, 40 respondents reported a loss, with five who could not remember and four who would rather not reveal the amount. Those who lost money represented almost five percent of the total sample and 37 percent of those who had responded positively to a scam. This showed a small increase in the number of people who had lost money to scams from 2007 to 2008 (see Table 7).

While analysing the amount of money lost to scams, the potential for the respondent to misinterpret the question was highlighted. Many respondents appeared to have included the amount of loss based on the potential earnings had the offer been genuine. Some respondents indicated they had lost $1m in 2008 and $22 million and $1m in 2007, which was not considered likely to be a real amount of loss, particularly as this loss was allegedly not reported in many cases. For this reason, any reported loss greater than $500,000 was excluded from the analysis of money lost to consumer fraud. As a result, in both 2007 and 2008 one case each was excluded from the analysis

The amount of money lost differed between 2007 and 2008 (see Table 8). The minimum reported loss in 2008 was $6, while in 2007 it was $10. The maximum loss in 2008, when the outliers were removed, was over $300,000 while in 2007 it was just over $100,000. The mean loss per respondent was $13,760 in 2008, up from $9,999 in 2007. Due to the relatively small numbers of respondents who lost money to scams, and the large range of losses, changes to amounts in only a few cases can cause large variation to the averages. Because of this, the median may present a more appropriate comparison and differences were still apparent when looking at the median loss between the years. The median loss per respondent was $1,500 in 2008 and $577 in 2007. The results can also be compared by looking at the 25th and 75th percentiles of the amount of money lost by those who responded positively to scams. In 2008 and 2007, 25 percent of respondents lost no more than $250 and $120 respectively while 75 percent of people lost no more than $7,600 and $7,000 in 2008 and 2007 respectively.

While the amounts lost differed in the two years, the pattern of loss remained the same (see Figure 3). The largest proportion of respondents lost less than $500, while losses between $1,000 and $4,000 were quite rare. The proportions of respondents who lost money then increased for those losing more than $4,000; however, this included a large range of losses, up to $310,000. In reality, it was a small number of respondents that were responsible for the large amount of the money lost to consumer fraud (see Figure 3).

Table 7 Respondents who reported a loss, 2007 and 2008 (%)

Number of respondents who specified a loss	2008 (%)[a]	2007(%)[b]
As a percentage of total sample	6.8	4.8
As a percentage of those who responded positively to a scam	36.9	33.6

a: 2008 n=62 (1 case removed)

b: 2007 n=40 (1 case removed)

Source: ACFT Consumer Fraud Survey 2007 & 2008 [AIC data file]

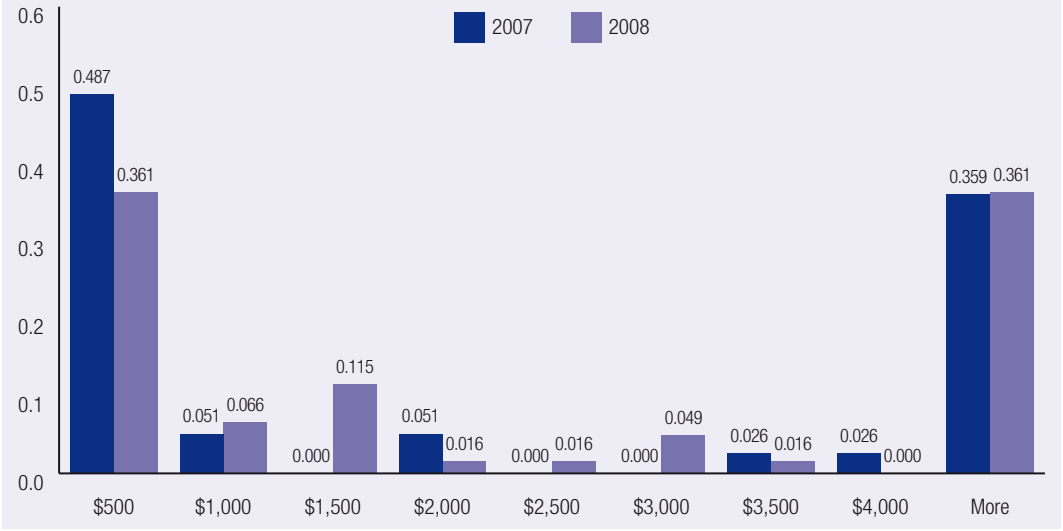
Table 8 Money lost to scams, 2007 and 2008

Year	Min loss ($)	Max loss ($)[a]	Total loss ($)	Mean loss per respondent—total sample ($)	Median loss per respondent—total sample ($)
2007	10	106,000	379,974	9,999	577
2008	6	310,000	839,365	13,760	1,500

a: the largest figures over $500,000 were removed as they likely represent an error in responding to the question (2007 n=1, 2008 n=1)

Source: ACFT Consumer Fraud Survey 2007 and 2008 [AIC data file]

Figure 3 Amount paid to consumer fraud scammers by total sample, 2007 and 2008 (%)



Note: this graph compares percentages, not actual figures

Source: ACFT Consumer Fraud Survey 2007 and 2008 [AIC data file]

Table 9 Number of respondents who reported a scam based on total number of respondents, 2008

Reported scam	Total respondents (n=919)	Percentage of total respondents[a]	Total of those who responded positively to scams (n=168)	Percentage of those who responded positively[a]
Yes	334	36	106	63
No	446	49	61	36
Missing	49	5	0	0
n/a	90	10	1	<1

a: percentages may not total 100 due to rounding

Source: ACFT Consumer Fraud Survey 2008 [AIC data file]

Reporting consumer fraud

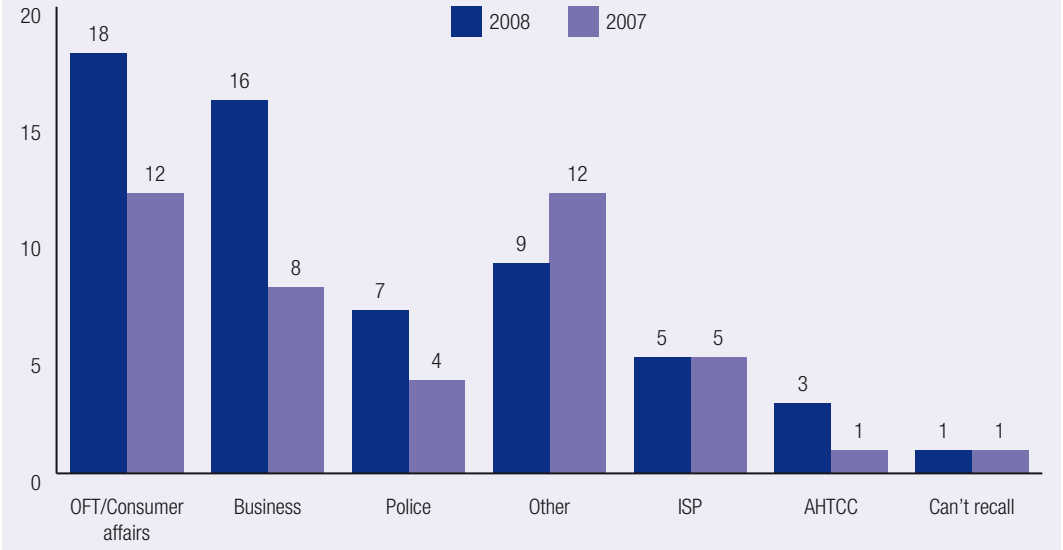
Respondents were asked whether they reported the scam(s) they received and/or responded to, and if so, to which agency. Table 9 shows that in 2008, just over 36 percent of the total sample reported the scam(s) in some way; only marginally fewer respondents than the previous year (2007=39%). Of those who responded positively to scams in 2008, just over 63 percent reported a scam, which is nearly double the reporting of the overall sample. However, a large proportion of victims (37%) still do not report scams.

There has been a slight increase in reporting scam invitations to most agencies when comparing 2008 results with those from 2007 (see Figure 4). In 2008, the agencies that respondents reported to most frequently were consumer affairs/the Office of Fair Trading agencies (18%). These agencies experienced a 50 percent increase in reporting from 2007 figures. This was followed by reporting to the business involved (16%), which is double the reporting figure from last year. Unsurprisingly, those who responded positively to a scam were more likely to report a scam victimisation (63%) than those who were not victimised (36%; see Table 9).

Perceptions of scams

Figure 5 illustrates how the 2008 respondents perceived the four scam types specified. All scam types were considered 'a crime' by an overwhelming majority of respondents for AFF (86%), lottery (80%)

Figure 4 Reporting to agencies by total sample, 2007 and 2008 (%)



Source: ACFT Consumer Fraud Survey 2008 [AIC data file]]

Table 10 Perception of scams by victims of that scam type, 2008[a]

	Lottery (n=53)		AFF (n=44)		Phishing (n=34)		Financial advice (n=34)	
	n	%	n	%	n	%	n	%
A crime	42	79.25	38	86.36	22	64.71	20	58.82
Wrong, but not a crime	2	3.77	1	2.27	1	2.94	4	11.76
Just something that happens	5	9.43	1	2.27	1	2.94	1	2.94
Don't know	1	1.89	1	2.27	0	0.00	5	14.71
Missing	3	5.66	3	6.82	10	29.41	4	11.76

a: percentages may not total 100 due to rounding

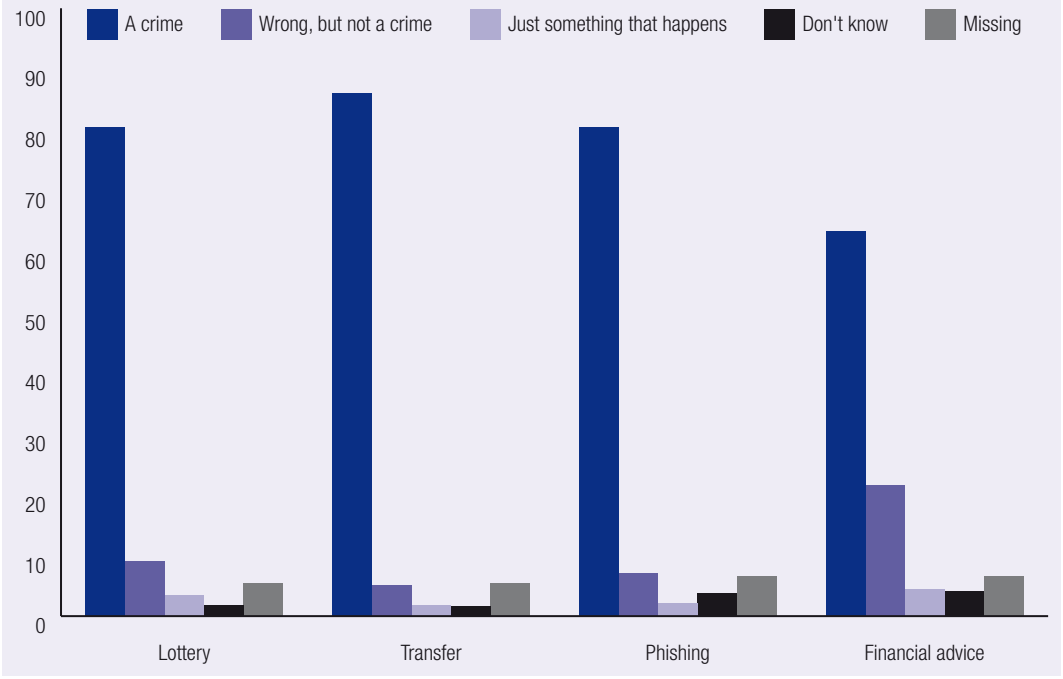
Source: ACFT Consumer Fraud Survey 2008 [AIC data file]

and phishing (80%) scams. Although financial advice scams were not reported as being a crime as frequently as the other three categories (63%).

Table 10 shows how respondents view different scams and whether they consider each type as a criminal offence. Since overall counts for each scam category were low and were spread across five options, both counts and percentages are included in Table 10.

The majority of respondents who were victimised by AFF (86%) and lottery scams (79%) perceived the scams were a crime. While this was still the case for phishing (65%) and financial advice (59%) scams, these percentages appeared noticeably lower than the other two categories. However, this does not indicate that the remaining respondents for each category did not think that the scam they responded to was not a crime. For example, nine (27%) financial advice victims either did not respond or did not know if it was a crime; and nearly a third (n=10) of phishing victims did not respond to the question, with only two responses for phishing not categorised in the missing or not 'a crime' category.

Figure 5 Perception of scams by scam type, 2008 (%)



Source: ACFT Consumer Fraud Survey 2008 [AIC data file]

The 2009 consumer fraud survey results

2009 ACFT awareness campaign

In March 2009, the ACFT conducted a week-long campaign to raise awareness about consumer fraud which was timed to coincide with global awareness efforts. The 2009 survey has been amended from previous surveys to include questions on additional scam types, loss of personal information and a more probing look at the factors that can lead to victimisation, or avoiding victimisation, from scams. The 2009 survey also excludes respondents residing outside Australia or New Zealand.

Results

Responses to the ACFT survey

Respondents

In 2009, there were 708 responses to the survey. During data cleaning, 16 respondents were removed as they indicated that they resided outside the target population of Australia and New Zealand. After removing these responses, 692 responses were included in analysis. This was a decrease of 25 percent (n=227) from the 919 responses in 2008.

Only one-quarter (24%) of the respondents were aware of the other activities in the 2009 consumer fraud awareness campaign (ie the broader campaign activities that include the survey, fraud awareness messages in the media etc) and just 11 percent were aware of the campaign in 2008. This is similar to the 2008 survey, where only 10 percent of respondents were aware of the previous campaigns. Of those who responded to the survey in 2009, only a few had also responded in previous years; there were 12 respondents in 2008, 11 respondents in 2007 and eight respondents to the pilot survey in 2006. Of these, 12 had responded to the survey in just one other year, two had responded in two other years and five people had responded in all three years.

Characteristics of the sample

Age and gender

The majority (82%) of respondents were aged between 25 and 64 years. The age groups most represented in the sample were the 45–54 year age group (24%), 55–64 year age group (20%) and the 25–34 year age group (19%). The gender of respondents was split almost evenly, with 50 percent male, 49 percent female and less than one percent who did not specify. However, there were differences in the gender distribution in different age categories.

The 18–24, 25–34 and 35–44 year age group categories were predominantly female, while there were more males in the 55–64 year and over 65 years age group categories (see Table 11).

Compared with the 2008 survey sample, there has been a change in the spread of the age of respondents, with an increase in the number of respondents aged 55–64 years (5% increase) and those aged over 65 years (6% increase), and a decrease in the number of 35–44 year olds (3% decrease) and 25–34 year olds (6% decrease).

Region

The majority of the sample came from Western Australia (24%), New South Wales (19%) and New Zealand (18%; see Figure 6). This is a substantial

Table 11 Respondents, by age in years and sex, 2009

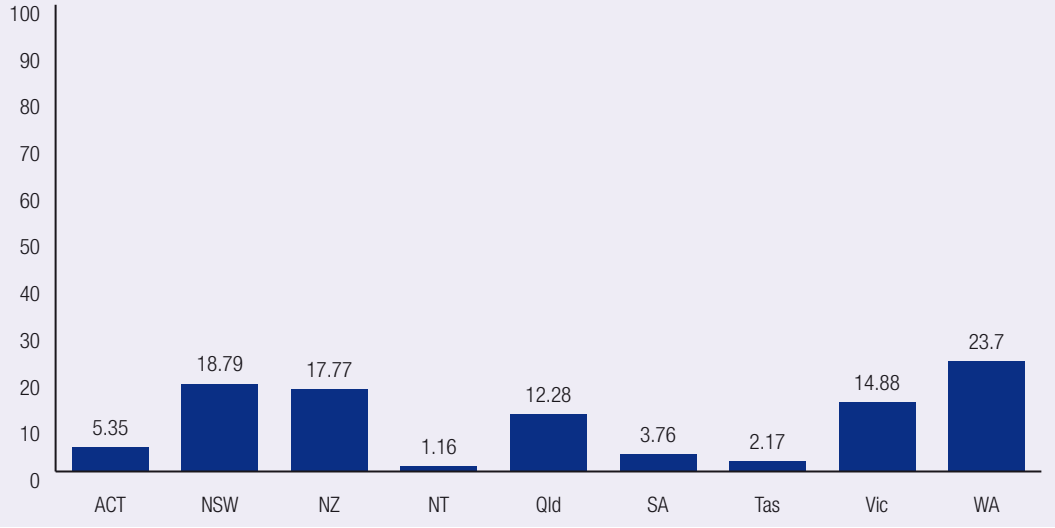
	Respondents (n)				
Age category (years)	Male	Female	Missing	Total respondents (n)	Total sample (%)[a]
17 and under	4	4	0	8	1
18–24	15	29	0	44	6
25–34	55	78	0	133	19
35–44	47	80	1	128	18
45–54	81	81	1	163	24
55–64	87	51	2	140	20
Over 65	56	18	1	75	11
Missing	1	0	0	1	<1
Total	346	341	5	692	100

a: percentages may not total 100 due to rounding

n=692

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

Figure 6 Respondents by region, 2009 (%)[a]



a: percentages may not total 100 due to rounding and missing data

Note: 0.14% of the sample did not specify region

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

increase in the number of respondents from New Zealand, who represented just two percent of the sample in 2008. The Northern Territory was the least represented (1%), alongside Tasmania (2%) and South Australia (4%). In 2008, Victoria had the greatest number of participants (31%). This difference could be the result of differential promotion of the survey and Fraud Awareness campaigns across jurisdictions and years. It is up to the individual jurisdictions as to how they promote the survey and campaign, although there were some nationally targeted media campaigns.

Income

The income of respondents was a new question in 2009. The two categories of income that were most common were $40,000–60,000 (22%) and over $80,000 (22%; see Figure 7). People earning less than $20,000 a year represented only nine percent of the sample, making this the smallest group. Just over 16 percent of respondents did not answer the question.

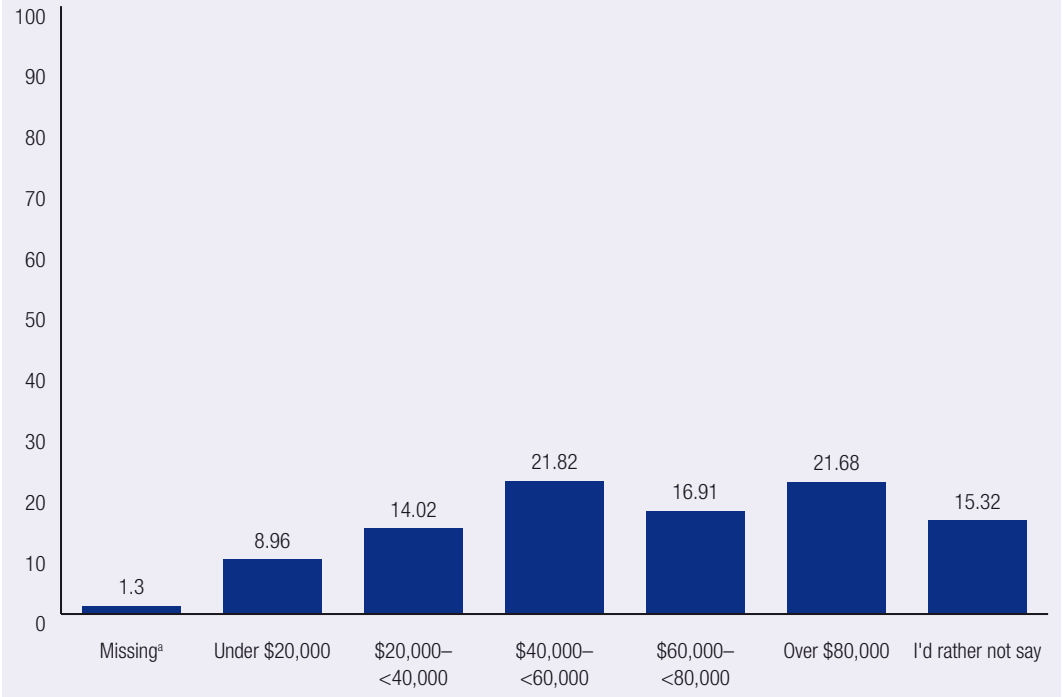
Scam invitations

Numbers of people receiving scam invitations

In 2009, 86 percent (n=598) of survey respondents had received at least one scam invitation in the previous 12 months. Table 12 shows the number of respondents who received invitations by fraud type and method. The type of scam invitation received by the majority of respondents was lottery and prize scams (63%), followed by work from home scams (53%) and AFF (51%). Overwhelmingly, email was the most common method to receive scam invitations (73%), more than three times the amount received by mail (23%) which was the second most common method. When looking at both fraud type and method of delivery, lottery scams were principally sent via email (51%), although this proportion was only marginally higher than AFF (49%) and work from home scams (47%).

Analysis was also conducted on the number of different scam invitations a respondent received.

Figure 7 Annual income of total respondents, 2009 (%)



a: 1.3% of the sample did not specify annual income

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

Table 12 Invitations received, by method and type, 2009 (%)[a]

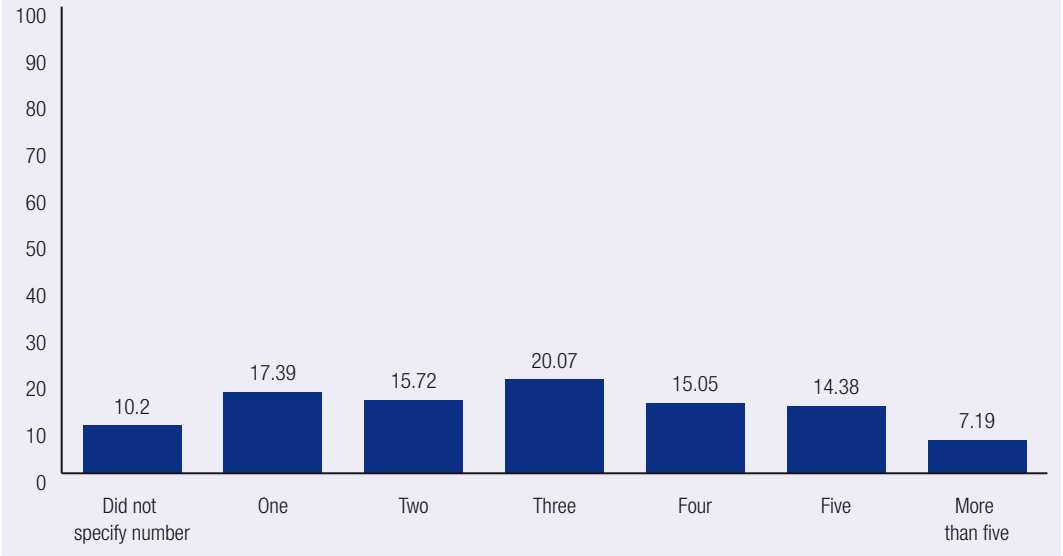
Type	Mail	Email	Phone	Mobile/SMS	Website/Internet	Other	Any method
Lottery	13	51	7	3	4	<1	63
AFF	3	49	1	1	2	<1	51
Inheritance	3	31	0	<1	1	<1	33
Phishing	1	43	4	1	2	<1	45
Financial	4	23	8	2	2	1	30
Work from home	7	47	3	1	5	2	53
Dating/romance	0	10	<1	<1	3	<1	12
Other	3	9	3	3	3	3	23
Any fraud type	23	73	18	9	13	7	86

a: respondents could receive an invitation for more than 1 type and by more than 1 method

n=598

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

Figure 8 Number of different types of scam invitations received, 2009 (%)



Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

This is not the number of actual invitations received, which could include multiple invitations to the same scam type, but rather how many different scams respondents were exposed to. In line with the 2008 survey results, the majority respondents received more than one type of scam invitation (see Figure 8). Of those who received an invitation, 72 percent received invitations to more than one type of scam. One in five (20%) had received invitations to three scam types, while seven percent received invitations to more than five types of scam.

Despite attempts to categorise scams into specific types, such as AFF and lottery scams, there remains some variation in the content of the invitations within these categories. In the survey's qualitative responses, it became evident that the category of 'inheritance scams' involved two slightly different narratives to lure victims. The first involved asking the potential victim to pretend to be the deceased's relative to fraudulently obtain the money, while the second tried to convince potential victims they were a relative of the deceased, albeit a distant one.

Consumer fraud victimisation

Victimisation in the survey was defined in three ways:

- responding positively;
- losing money; and
- losing personal information.

In previous years, losing money and personal details were not classified separately. Any contact that was intended to further the communication was considered responding positively, including contacting the perpetrator to request further information, providing personal details, or sending money to the scammer. Respondents who had communicated to request not to be contacted again, or who had deliberately tried to 'bait' the perpetrator with no intention of participating in any deal were not considered as victims.

Who responds positively to scams?

Overall, 17 percent (n=121) of the sample had responded positively to a scam in the previous 12 months. This equated to 20 percent of those respondents who had received a scam invitation, which was the same figure as seen in 2008. Although the surveys have used different sampling frames, the number of victims identified has remained relatively stable over the past three years, with a decrease of one percent in 2009 after an increase of five percent in 2008 (see Table 13).

Scams in the 'other' category recorded the most victims, representing seven percent of the total sample and over 40 percent of victims responding to invitations (see Table 14). However, this generic category contains several different scam types, including sports arbitrage betting software packages (eg where scammers sell computer prediction betting software often disguised as a legitimate investment claiming to give a foolproof profit on sports betting such as horse racing virtually risk free, that in reality rarely works; see http://www.scamwatch.gov.au/content/index.phtml/tag/SportsInvestmentScams for more information) and general non-delivery of goods and services, rather than a single scam. While scams in the 'other' category appear to attract the most responses,

Table 13 Receiving and responding positively to scam invitations, 2007–09 (%)

Year (total n)	Received an invitation	Responded positively to an invitation
2009 (n=692)	86 (n=598)	17 (n=121)
2008 (n=919)	90 (n=824)	18 (n=168)
2007 (n=841)	86 (n=724)	13 (n=108)

Source: ACFT Consumer Fraud Survey 2007, 2008 and 2009 [AIC data file]

Table 14 Responded positively by scam type, 2009

Scam	n	Percentage who responded positively to a scam[a](n=121)	Percentage of total sample (n=692)
Lottery	30	25	4
AFF	18	15	3
Inheritance	9	7	1
Phishing	14	12	2
Financial	14	12	2
Work from home	39	32	6
Dating/romance	14	12	2
Other	51	42	7

a: respondents could select more than 1 scam type

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

Table 15 Number of times victims responded to invitations by fraud type, 2009 (n)[a]

Times responded	Fraud type							
	Lottery	Transfer/ AFF	Inheritance	Phishing	Financial	Work from home	Dating	Other
Once	17	9	1	5	9	29	9	29
Two times	5	3	5	6	4	10	3	3
Three times	3	1	0	1	0	3	0	1
Four times	1	0	0	0	1	0	0	0
Five or more times	4	5	2	2	0	5	2	6
Other	0	0	1	0	0	0	0	2
Total	30	18	9	14	14	47	14	41

a: respondents could select more than 1 scam type

n=121

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

Table 16 Number of invitations received by scam type and number of respondents who responded positively to each scam type, 2009

Scam type[a]	Received scam type by total sample		Received scam type by those who responded positively	
	n	(%)[b]	n	(%)[b]
Lottery	438	63	30	4
AFF	351	51	18	3
Inheritance	226	33	9	1
Phishing	314	45	14	2
Financial	207	30	14	2
Work from home	364	53	39	6
Dating/romance	84	12	14	2
Other	160	23	51	7

a: respondents could select more than 1 scam type

b: n=692

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

the number of victims in 2009 was slightly lower than that in the previous year where 55 percent of victims responded to a scam in this category. This could be at least partly explained by the addition of new categories in the 2009 survey that would previously have been included in the results for the 'other' category.

Of the seven scam categories provided in the survey, work from home scams were the most commonly reported scam type that survey participants responded to. The victims of these scams accounted for nearly six percent of the total sample, which was over 30 percent of those who were victimised. The second most successful scam category was lottery and prize scams, with four percent of the sample or almost 25 percent of victims. These results represent an increase on the number of work from home scams identified in 2008; however, 2009 is the first year this category has been included as an identified scam rather than part of the 'other' category.

As well as determining the types of scams that attract victims, the survey also asked the number of times victims responded to scam invitations. For most scam types, the majority of those who

responded to scams responded only once (see Table 15). The exceptions were inheritance and phishing scams, where the majority of these victims responded twice. Despite this, there were small numbers of people who responded five or more times to a scam, which was the case for six victims of 'other' scams, five victims of work from home and AFF scams, and four from lottery and prize scams.

Table 16 shows the number of people receiving invites for each scam type and the number of people who responded to them. A discrepancy can be seen in the number of people receiving invitations to, and becoming victimised by, 'other' scams. Invitations for the 'other' scam type were received by only a small number of respondents (23%), however, these scams netted the largest group of victims (7%; n=51) compared with the other groups, followed closely by work from home scams (6%; n=39).

Loss of money and personal information to scams

Alongside questions about victimisation in general, respondents were also asked whether they had lost money or personal information to any scams. Losing money was defined as money paid out by the victim as a result of a request and before any reimbursement from banks, insurance or legal action. This figure did not include the loss of potential earnings had the scam been legitimate, such as the payout for a lottery win specified in some scams, which can be millions of dollars. Self-reported figures on loss from victimisation should be used with caution as it is not always possible for victims to calculate the amount they have lost and sometimes they are not aware of the loss for some time, if at all.

Table 17 shows the number of victims who lost money and/or information to any scam. Fewer victims lost money (7%) than information (9%), while four percent experienced both types of victimisation. A chi-square analysis showed a strong significant relationship between sending money to a scam and losing personal information (χ^2 (1)=155.7069, p<0.001; Cramér's V=0.4744). Furthermore, in 2009 the seven percent of the sample who had sent money in response to a scam equated to 41 percent of victims, while over half of the victims in the sample had lost personal information (52%). The total dollar amount lost from all victims was over half a million dollars ($544,694), ranging from $7 to $300,000 (see Table 18). The mean loss was just over $12,000 per respondent ($12,379) while the median was $1,050. Unlike the 2007 and 2008 responses in this category, there were no cases where the amount loss exceeded $500,000 and therefore no cases were excluded on this basis. However, six cases were not included in the calculation due to missing data (n=5) and specifying a loss of $0 (n=1).

Table 19 shows the number of people who lost money and/or information to each type of scam. The 'other' category resulted in the most victims

Table 17 Loss of money and personal information to scams, 2009 (%)[a]

Loss type	Percentage of total sample (n=692)	Percentage of those who responded positively to scams (n=121)
Money (n=50)	7	41
Information (n=63)	9	52

a: respondents could respond to more than 1 category

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

Table 18 Money lost to scams, 2007–09

Year	Lost money (%)	Min loss ($)	Max loss ($)[a]	Total loss ($)	Mean loss ($)	Median loss ($)
2007	6	10	106,000	379,974	9,999	577
2008	7	6	310,000	839,365	13,760	1,500
2009	7	7	300,000	544,694	12,379	1,050

a: the largest figures over $500,000 were removed as they likely represent an error in responding to the question

Source: ACFT Consumer Fraud Survey 2007, 2008 and 2009 [AIC data file]

Table 19 Loss of money and information by scam type, 2009

	Sent money			Lost information		
Scam[a]	n	Percentage of total sample (n=692)	Percentage who responded positively (n=121)	n	Percentage of total sample (n=692)	Percentage who responded positively (n=121)
Lottery	6	0.9	5.0	17	2.5	14.0
AFF	2	0.3	1.7	5	0.7	4.1
Inheritance	2	0.3	1.7	3	0.4	2.5
Phishing	1	0.1	0.8	9	1.3	7.4
Financial	4	0.6	3.3	6	0.9	5.0
Work from home	14	2.0	11.6	17	2.5	14.0
Dating/romance	4	0.6	3.3	6	0.9	5.0
Other	21	3.0	17.4	19	2.7	15.7

a respondents could respond to more than 1 category

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

incurring a financial loss (17%), which is consistent with the rate of victimisation. This was followed by work from home scams with 12 percent of victims losing money to this scam. Less than one percent of victims reported paying money to a phishing scam, which is not surprising given that phishing scams often target personal details rather than requesting advance fee payments.

There was a difference between victims reporting loss of personal information and financial losses. 'Other' and work from home scams were two of the more common scam types that resulted in victims losing information (16% and 14% respectively). The number of victims reporting a loss for lottery scams rose sharply when comparing financial loss (5%) to information (14%). A similar difference was seen with phishing scams, where just 0.8 percent of victims lost money but 7.4 percent lost information.

Scam victimisation and demographic variables

In total, there were 692 responses to the survey, with 121 victims who responded to invitations, of which 50 sent money and 63 sent information. These groups of respondents were compared based on demographic variables to examine any differences between the groups. When examining the ages and victimisation, the 25–34 year and 35–44 year age categories appeared to be over-represented in the groups that sent money and information as a result of a scam when compared with their proportion in the total sample (see Tables 20 and 21). While the 25–34 year olds and 35–44 year olds represented six and 19 percent of the total sample respectively, 25–34 year olds accounted for 26 percent of those who sent money and 27 percent of those who sent information and 35–44 year olds represented 24 percent of those who sent money and 27 percent of those who sent information.

Conversely, those in the 45–54 year age category represented almost a quarter of the sample and 26 percent of those who responded to a scam, but only 19 percent of those who sent information and 22 percent of those who sent money. Likewise, those respondents aged over 65 years comprised 11 percent of the sample, but just two percent of those who sent information and had no instances of sending money to a scam. It appears that those aged 25–34 and 35–44 years may have been more inclined to send money and information, while older respondents 45–54 and over 65 years were less likely to provide information and the respondents aged over 65 years were less likely to send money, even when they responded to a scam. However, due to the small sample sizes, these differences could not be tested for statistical significance. In addition, tests of statistical significance (chi-square) were not able to be carried out on the likelihood of victimisation with the variable of age.

The sample was divided almost evenly between male and female respondents. This pattern also continued when looking specifically at victims of scams. Although females were slightly more likely to send money (53% compared with 47%) and information (57% compared with 43%) than males (see Table 22), a chi-square test performed on the data indicated that these results were not statistically significant.

Most victims who responded positively to a scam in the 2009 survey came from New South Wales (21%), Victoria (21%), New Zealand (16%), Queensland (13%) and Western Australia (12%). No scam victims from the Northern Territory responded to this survey (see Table 23). There appears to be discrepancies in the pattern of victimisation in different regions, such as Victoria who represented 15 percent of the sample but 21 percent of victims, or Western Australia, which represented a quarter of the sample but only 12 percent of those who responded positively to scams. Victimisation and region where respondents lived was statistically significant (χ^2 (8) =19.35 p<0.05; Cramér's V=0.1833) but there was only a mild relationship between the two variables. Respondents from Western Australia were less likely to respond positively to a scam, whereas Tasmanian respondents were more likely to respond positively.

The annual income of respondents was included for the first time in the 2009 ACFT survey. To explore the relationship between victimisation and annual

Table 20 Respondents who responded positively to scams by age in years, 2009

Age	Percentage of total sample by age[a, b] (n=692)	Responded positively by age (n=121)	Percentage of age group who responded positively to scams[a] (n=121)
17 and under	<1	1	1
18–24	1	8	7
25–34	6	25	21
35–44	19	24	20
45–54	24	32	26
55–64	20	26	21
65+	11	5	4

a: percentages may not total 100 due to rounding

b: 1 respondent did not specify age

Source: ACFT survey 2009 [AIC computer file]

Table 21 Respondents who responded positively to scams by sending money and/or information by age in years, 2009 (%)[a, b]

	Sent money		Sent information	
Age	Respondents who sent money (n=50)	%	Respondents who sent information (n=63)	%
17 and under	0	0	0	0
18–24	3	6	5	8
25–34	13	26	17	27
35–44	12	24	17	27
45–54	11	22	12	19
55–64	11	22	11	17
65+	0	0	1	2

a: percentages may not total 100 due to missing data and rounding

b: respondents could respond to more than 1 category

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

Table 22 Victims of scams by gender, 2009 (%)[a, b]

Gender	Total sample	Responded positively (n=121)	Sent money (n=50)[c]	Sent information (n=63)
Male	50	48	46	43
Female	49	52	52	57

a: percentages may not total 100 due to missing data and rounding

b: 1 percent (n=5) did not specify gender

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

Table 23 Victims of scams by region, 2009 (%)[a]

Region	Total sample (n=692)[b]	Responded positively (n=121)	Total sample who sent money (n=50)	Total sample who sent information (n=63)
ACT	5	6	4	3
NSW	19	21	26	25
NZ	18	16	14	14
NT	1	0	0	0
Qld	12	13	12	13
SA	4	6	2	6
Tas	2	6	8	3
Vic	15	21	16	22
WA	24	12	18	13

a: percentages may not total 100 due to missing data and rounding

b: 0.14% did not specify region

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

income, respondents who declined to answer the question on income were excluded from the analysis (n=115), reducing the sample to 577 respondents. No significant relationship was found between victimisation in general and income, or income and sending money as a result of a scam. However, there was a significant relationship between income and sending information as a result of a scam (χ^2 (4)=9.5759, p<.05, Cramér's V=0.1288), with a mild correlation between the two categories. It was found that those earning less than $20,000 a year were more likely to send information to a scam, while those earning more than $80,000 were less likely to send information. For this analysis, the category *I'd rather not say* was excluded. Those earning over $80,000 equated to 22 percent of the sample, but only 12 percent of those who sent information (see Table 24). Conversely, those earning less than $20,000 annually represented just nine percent of the sample but 20 percent of those who sent information.

Preventing scam victimisation

In 2009, respondents were asked for the first time about what prevented them from responding to fraud invitations. This was asked of victims as well as non-victims, as it is possible that even those victimised by a particular scam have chosen not to respond to other invitations.

In line with previous studies that found that prior knowledge about scams can prevent victimisation (see Titus, Heinzelmann & Boyle 1995), well over half of respondents who received an invitation said they did not respond because they had received a similar offer before (61%). This increased to 64 percent of those who did not respond to any scams and fell to 53 percent of scam victims. Nevertheless, it was the most common reason among all three groups (see Table 25). Just over half of the respondents who received an invite stated that the offer seemed *too good to be true* (53%) and that *something was not right* with the invitation (51%), while responses such as *knew a victim* were comparatively lower (5%).

Table 24 Victims of scams by annual income, 2009 (%)[a]

Yearly income	Percent of income by total sample (n=692)[b]	Percent responded positively (n=121)	Sent money (n=44)	Sent information (n=50)[c]
Under $20,000	9	18	14	20
$20,000–<40,000	14	19	27	22
$40,000–<60,000	22	26	23	28
$60,000–<80,000	17	18	18	18
Over $80,000	22	18	18	12

a: percentages may not total 100 due to missing data and rounding

b: respondents who did not provide annual income (n=1) or selected *I'd rather not say* (n=106) were excluded from analysis

c: 12 respondents who said they sent information did not specify income

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

Even among the victim group, the *too good to be true* category was selected by half of the respondents.

There was also variation in those who were/were not a victim of a scam and whether they were made aware of the scam via the media or another public source. Fifty-four percent of the total sample did not respond if the scam was made public via the media. Those who did not respond to any scam represented 59 percent of this sample compared with only 40 percent of victims. Responses to the categories *wanted to but couldn't afford to* and *was told it was a scam* options were comprised mainly of those who identified as victims.

Reporting consumer fraud

The survey also contained questions about reporting behaviour by respondents. Reporting fraud is imperative to increase the level of knowledge about scams and create effective fraud prevention campaigns. Traditionally, the levels of fraud reporting are low, with only an estimated 25 percent of all fraud being reported (Rollings 2008). These figures differ depending on fraud type and reporting agency. The results of the 2009 ACFT survey have shown similar findings, with rates of reporting to different agencies varying from 20 percent of respondents to just two percent.

Table 25 Reasons for not responding to invitations received, 2009[a]

Reason for not responding	n	Respondents who received invite (%) (n=598)	Respondents who did not respond (%) (n=456)	Respondents who responded positively (%) (n=121)
Offer was too good to be true	315	53	53	50
Had received something similar before	364	61	64	53
Previously seen in media or public source	325	54	59	40
Was told it was a scam	57	9	8	14
Knew a victim of a similar scam	28	5	4	7
Wanted to participate but couldn't afford to	19	3	1	11
Something not right with the offer	315	53	51	50
Other	94	15	14	17

a: respondents were able to select more than 1 response

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

In addition to reporting to formal agencies, in 2009, respondents were also asked about reporting scam invitations to family and friends. Sixty-nine percent of the total sample and 84 percent of those who responded positively to scams reported or disclosed the attempted or successful scam attempt to an agency or another individual. While this figure is high, 17 percent of victims did not disclose their experience to anyone. Of those who responded positively to scams, most reported to family and friends (50%) or a consumer affairs/fair trading agency (34%; Table 26).

There was no substantial change to the number of people reporting a scam from previous years, with the figure remaining at just below 40 percent (37% in 2009, 36% in 2008 and 39% in 2007). However, there was a change in the number of people reporting to specific agencies. The number of respondents reporting to the Office of Fair Trading or a consumer affairs agency rose to 20 percent (from 11% in 2007 and 16% in 2008) and those reporting to the business involved increased to 17 percent (from 7% in 2007 and 14% in 2008; Table 27).

Victimisation and reporting

A respondent could report a scam regardless of whether they responded positively to a scam. Intuitively, victims of scams would be expected to report their experiences more frequently than those who receive invitations but do not respond. The

Table 26 Reporting rates by agency, 2009 (%)[a]

Reported scam to (n=478)	2009 responded positively
Family/friends	50
Office of Fair Trading/Consumer Affairs	34
The business involved	26
Police	14
Other	12
ISP	12
Australian High Tech Crime Centre	3
Can't recall	4
Any formal agency	54

a: percentages may not total to 100 as respondents could respond to more than 1 category

Source: ACFT Consumer Fraud Survey 2007, 2008 and 2009 [AIC data file]

Table 27 Reporting rates by agency, 2007–09 (%)[a]

Reported scam to (n=478)	2009 responded positively	2009 total sample (n=692)	2008 total sample (n=919)	2007 total sample (n=841)
Family/friends	50	42	n/a	n/a
Office of Fair Trading/Consumer Affairs	34	20	16	11
The business involved	26	17	14	7
Police	14	6	6	4
Other	12	9	5	11
ISP	12	9	4	5
Australian High Tech Crime Centre	3	2	2	1
Can't recall	4	5	1	1
Any formal agency	54	37	36	39

a: percentages may not total to 100 as respondents could respond to more than 1 category

Source: ACFT Consumer Fraud Survey 2007, 2008 and 2009 [AIC data file]

survey results indicated this was partly the case, as being a victim of a scam generally had a significant effect on whether the scam was reported to a formal agency, with a mild correlation between the two variables (χ^2 (1)=9.32, p<0.01 Cramér's V=0.1271). There was no significant difference in reporting to family and friends. Of all victimised respondents in general, 55 percent reported at least one scam to a formal agency, compared with 40 percent of non-victimised respondents.

There was a significant relationship found between reporting to a formal agency and whether the victim had sent money. Of those victims who sent money, 52 percent reported at least one fraud to a formal agency compared with 35 percent of those who did not lose money (χ^2 (1)=5.54, p<0.05, Cramér's V=0.0895). Unlike victimisation, these factors were also significant in reporting to family and friends. When including reporting to family and friends, the reporting rate increased to 82 percent of those who sent money, compared with 68 percent of those who did not send money (χ^2 (1)=4.21, p<0.05, Cramér's V=0.0780). However, both relationships were weak.

Similar reporting patterns were found for those victims who lost personal information. Fifty-six percent of those who sent information reported to a formal agency compared with 35 percent of those who did not send information. This relationship was mild, yet was still statistically significant (χ^2 (1)=10.78, p<0.01, Cramér's V=0.1248). Again, the strength of the relationship increased when those who reported to family and friends were included, increasing to 89 percent of those who sent information compared with 67 percent of those who did not. This was also considered statistically significant (χ^2 =12.74, p<0.001, Cramér's V=0.1357), although the correlation between reporting to anyone and sending information was only mild.

Demographics and reporting

Demographic variables also appeared to play a role in the reporting behaviour of the sample. Chi-square tests showed there were statistically significant differences in reporting behaviour by demographics. Reporting a scam either formally (eg police, ACCC) or informally (eg family, friends) had statistically significant differences by age (χ^2 (6)=21.74, p<0.001; Cramér's V=0.1774), with a mild correlation between the categories. Overall, 25–34 year olds were less likely than expected to report to anyone, whereas 55–64 year olds were more likely to report a scam to anyone. Region and reporting differences were also significant, with a moderate correlation between the two categories. Respondents from New South Wales were more likely to report a scam than expected and respondents from Western Australia were less likely than expected to report a scam (χ^2 (8)=39.56 p<.001; Cramér's V=0.2393).

There were statistically significant results for the category of income when reporting a scam to formal agencies, as well to formal and informal reporting combined. For this analysis, the category *I'd rather not say* was removed from the calculation. Those with an annual income of less than $20,000 were more likely to report to a formal agency (χ^2 (4)=10.43, p<0.05; Cramér's V=0.1345, with a mild correlation between the two variables). When formal and informal reporting methods were combined, respondents with a yearly income of $60,000–80,000 were statistically less likely to report to anyone (either a formal agency or family/friends; χ^2 (4)=10.63 p<0.05; Cramér's V=0.1357). This correlation was also considered relatively mild. However, when reporting to only formal agencies was analysed, there was no significant results.

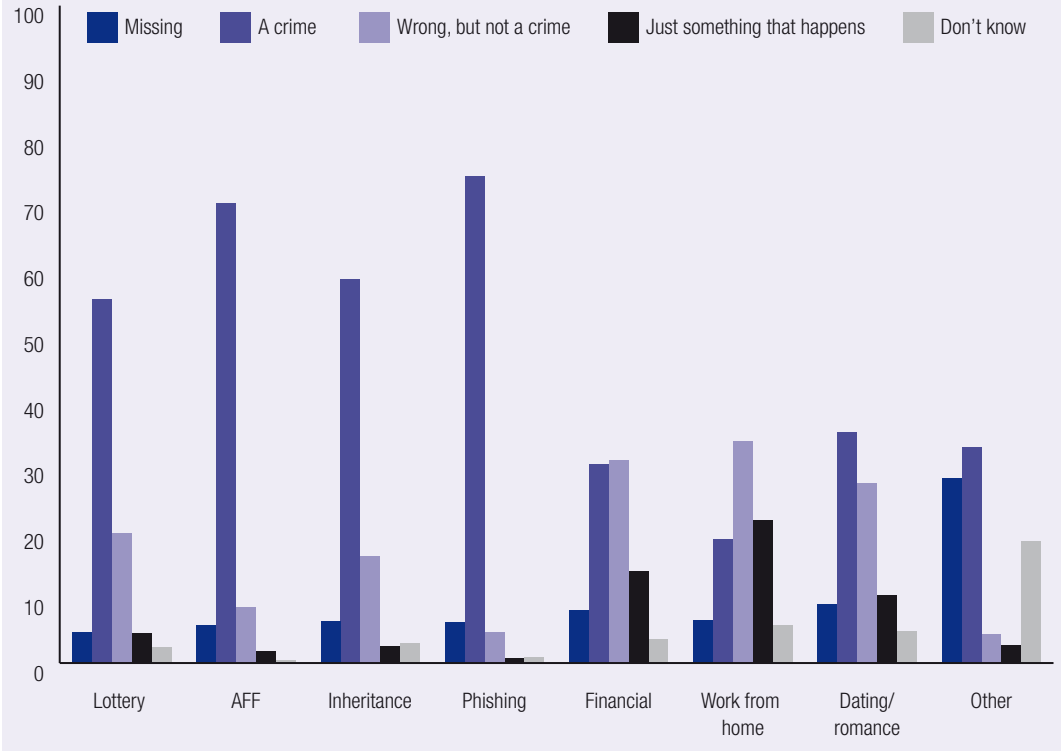
Perception of scams

Respondents were asked how they perceived each scam type. They were asked to indicate whether they considered each scam type listed was:

- a crime;
- wrong, but not a crime;
- just something that happens; and
- an option for 'don't know'.

There were distinct differences in how respondents viewed different scam types. Figure 9 charts respondent's perceptions of different scams. Four scam types were considered criminal by a much larger percentage of respondents than the remaining scams; these were phishing (74%), AFF (70%), inheritance (58%) and lottery (55%). This is in contrast to the considerably lower number of

Figure 9 Perceptions of scams by scam type, 2009 (%)



Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

Table 28 Perceptions of scams by victims of that particular scam, 2009 (n)

	A crime		Wrong but not a crime		Just something that happens		Don't know	
Scam type	n	%	n	%	n	%	n	%
Lottery (n= 30)	19	63.3	7	23.3	3	10.0	1	3.3
AFF (n= 18)	15	83.3	0	0	2	11.1	1	5.5
Inheritance (n=9)	6	66.7	1	11.1	1	11.1	1	11.1
Phishing (n=14)	11	78.6	2	14.3	1	7.1	0	0
Financial (n=14)	4	28.6	5	35.7	4	28.6	1	7.1
Work from home[a] (n=39)	15	38.5	11	28.2	10	25.6	1	2.6
Dating/romance (n=14)	7	50.0	4	28.6	2	14.3	1	7.1
Other[b] (n=51)	42	82.4	1	2.0	2	3.9	0	0.0

a: missing=2

b: missing=6

Source: ACFT Consumer Fraud Survey 2009 [AIC data file]

respondents who considered dating scams (35%), other (33%), financial (30%) and work from home (19%) scams as criminal.

The number of people who considered scam invitations criminal in 2009 was lower than in the 2008 survey. Each scam category that was measured in 2008 was considered criminal by a larger percentage of respondents than they were in 2009, with AFF (86%), lottery (80%), phishing (80%) and financial advice (63%) scams all showing substantial decreases.

Victimisation and perceptions of scams

The perceptions of scams held by victims compared with the entire sample were also analysed. The biggest discrepancy in opinions of whether scams were criminal or not were for dating and 'other' scams. For 'other', the difference was 22 percent (33% of sample and 55% of victims), while for dating scams it was 18 percent (35% of the sample and 53% of victims).

It is also worth highlighting that victims of scams still have somewhat lower perceptions of what is criminal than the overall sample. Table 28 shows the figures for perceptions of scams among victims of those scam types. Due to the small sample size, both the count and percent of each category is included. Each scam type has at least three victims who did not identify the scam they were victimised by as criminal. Ten of the 14 victims of financial scams did not identify the scheme as a crime, more than double those who said it was a crime (n=4). Likewise 21 of the 39 victims of work from home scams did not identify these as scams as criminal, compared to only 15 who did. Twenty-two victims also did not consider work from home scams criminal.

Overall, 32 percent of victims identified work from home scams as a crime, compared with 22 percent of non-victims. 'Other' scams were considered a crime by 80 percent of victims compared with 50 percent of non-victims, although the exact nature of the scams they are referring to in this group cannot be determined. When applying a chi-square test on perceptions of scams by victimisation, statistically significant results were found between victimisation by any scam and the perceptions of the criminality of work from home scams and 'other' scams. Victims of any scam were more likely to label both work from home scams ($\chi^2(1)=4.61$, $p<0.05$, Cramér's V=0.0927), and 'other' scams as a crime ($\chi^2(1)=23.32$, $p<0.001$, Cramér's V=0.2433) than non-victims. The correlation between perceptions of work from home scams and victimisation was weak, but was moderate between victimisation and perceptions of 'other' scams. Note that this is in relation to victims of *any* scams being more likely to label work from home, 'other' and financial scams as a crime, not just the victims of these crimes.

Conclusion and policy implications

Findings and discussion

Determining the true extent and nature of consumer fraud in Australasia will always be problematic because the types of frauds committed and the methods used are constantly evolving. A large proportion of consumer fraud still goes undetected and/or unreported which exacerbates the problem. Under-reporting of fraud occurs for a number of reasons. In some cases, it is because the victim is unaware that the incident that has taken place is actually fraud. The current survey is restricted in generalising its findings by the limitations of self-selection bias by respondents and the relatively small sample size. Therefore, the findings from this survey should be interpreted and used with caution. Nevertheless, the 2008 and 2009 ACFT Fraud Fortnight and Fraud Awareness surveys have been useful tools to create a snapshot of consumer fraud in Australasia for each year, highlight emerging scam types and offering direction on where further research is needed.

There are fewer responses to the 2009 survey compared with the 2008 survey. This could be due to the corresponding decrease in the campaign length from two weeks to one. In both the 2008 and 2009 Consumer Fraud surveys, the majority of people who received a scam invitation did not respond. In total, 18 percent of the sample in 2008 responded positively to a scam and seven percent lost money as a result of this, whereas in 2009, 18 percent responded positively to a scam, with seven and nine percent losing money and/or personal information respectively. These results for responding positively to scams were similar to the 2007 findings. While in 2008 and 2009 there were increases in the percentage of people responding positively and losing money, these increases were only slight.

The low victimisation rate was not unexpected and reflects findings from both the previous consumer fraud surveys, as well as other studies conducted on fraud (eg ABS 2008). Despite this, consumer fraud remains an issue of concern because of the large number of attempted fraud incidents, the serious financial losses successful fraud causes, as well as the pain and humiliation that fraud can inflict on victims. Differences between male and female scam victims were examined in both 2008 and 2009. However, no statistically significant gender difference in the rate of victimisation was discovered.

The types of scams affecting respondents differed in 2009. Work from home scams attracted the most victims from the current sample, whereas in previous years, the lottery scam had more victims from the sample. This is possibly due to the evolution of scam invitations, but could also be as a result of the new scam categories included in the survey. That work

from home scams attracted the most victims in 2009 (a category not available in 2008), highlights the need to raise awareness of this specific scam, not least because of the illegality of working as a money mule and the risk of prosecution to the participant. In both 2008 and 2009, losses to scams ranged from very low amounts of money (such as less than $10), to amounts over $300,000. The vast differences in the amount of money lost by victims' highlights the diverse experiences of victimisation.

How scams are received

In the 2009 and 2008 surveys, as was the case in the previous surveys, email was still the primary medium through which people receive scam invitations. Despite the large number of invitations received via email, it is likely that this still underestimates the true proportion of invitations sent, as most email providers will automatically scan for spam and prevent suspicious emails reaching the inboxes of users. As such, it is fitting that much of the research on consumer scams is discussed interchangeably with research on cybercrime. While consumer fraud is only one element of potential cybercrime activities, the ease and low cost associated with sending invitations over the internet makes this method desirable for offenders.

Victimisation rates

The reported victimisation rates in both the 2008 (18%) and 2009 (17%) surveys were higher than those found in similar surveys, such as the *Personal Fraud Survey* conducted by the ABS (2008), which obtained a random sample of individuals from the population as part of the 2007–08 ABS *Multi-Purpose Household Survey*. In the ABS survey, 38.5 percent of the sample had been exposed to a scam and five percent were a victim of personal fraud. This difference is likely due to a self-selection bias among respondents in the ACFT surveys (often seen in this type of voluntary survey), where those with a pre-existing interest in the topic, or personal experience of victimisation, are more likely to respond.

Seventeen percent of victims in 2009 still did not disclose their experience to anyone. UKOFT (2009) found that some victims kept their involvement in these schemes private, even from their family and friends at the time of participation, before it was apparent they had been victimised. This could indicate they were at least partly aware that their involvement in the scheme was not wise. The high rate of victimisation in the 'other' category in both 2008 and 2009 surveys serves to demonstrate the evolving nature of consumer fraud and the vulnerability of people to new scam types. The study by Titus et al. (1995) found that fraud attempts were less likely to be successful if the target had previously heard of the fraud type, which both supports the survey results and reinforces the importance of the ACFT annual awareness campaign to draw consumer fraud to the public's attention.

Problems in identifying and classifying scam types and methodologies

Identifying an unsolicited invitation as legal or illegal can be difficult. For example, with premium SMS services it is hard to identify where the line lies between those that are legitimate and those that are scams. Some premium SMS services are easy to identify and clearly explain the costs involved, such as those used to vote in competitions, while in other cases, the terms and conditions others are less clear, blurring the line between legal and illegal. Some survey respondents reported in qualitative responses that they had received expensive text messages after entering their telephone number on websites. However, it is difficult to know whether these are actually illegal scams, or if they are merely expensive services, which, while seemingly unfair, are legitimate and outlined in the terms and conditions on the website.

In both surveys, the 'other' category was selected more frequently than the other four scam categories specified for many questions asked. This may indicate some respondents may have been confused about the scam definitions and highlights the need to continually update definitions to reflect the changing methodologies used by scammers. The inclusion of emerging scam types as separate categories based on the previous surveys (such as work from home scams, inheritance scams etc) was accompanied by a reduction in the amount of 'other' responses to

this question from 31 percent in 2008 to 23 percent in 2009. Although not a dramatic decrease, this could show support for regularly revising scam definitions to make it easier and less ambiguous for respondents to classify the scam types.

The inclusion of new categories could also significantly alter the rates of victimisation for each scam type across each year, making it impossible to accurately compare the rates for each category over the years. The presence of defined categories could also increase the rate of victimisation in the ACFT survey. For example, while a high proportion of people responding positively to work from home scams in 2009 may represent an increase in victimisation and invitations, it could also suggest an increased awareness of the illegality of such offers, or could merely be the effect of including a memory 'prompt' provided by the specific question about the scam type.

Different narratives for inheritance scams in the 2009 survey responses illustrate how scammers can use a common scam type but modify its contents to attract different types of victims. One version of this scam involves a victim being asked to fraudulently claim to be the relative of a deceased person, while the second tries to convince potential victims they are a relative of the deceased, albeit a distant one. The difference between the two seems minor, but there is an important distinction between an invitation to participate in a dishonest act, much like the earlier Nigerian advanced fee scams, compared with an invitation for a relative to collect something they are entitled to receive. This difference could influence the attitudes, and therefore responses, of those who receive invitations within this single scam category. It may be worthwhile to conduct further research to see if, of those who respond to scams, there are different motivations involved (eg altruistic or solely for profit motives). If any difference occurs, it could influence how scam prevention could be targeted to potential victims.

Each of these identified problems is compounded by the perpetrators constantly adapting the methods and types of scams. This makes it difficult to define scam types each year and to also compare the affects and victimisation by specific scam types over time.

Losing money and/or information

In 2009, the survey made a distinction between money lost and personal information lost to scams. In 2009, more victims lost personal information to scams than lost money directly. In addition, it was found that people who lost personal information were also more likely to have lost money to a scam than those who did not and vice versa. This is not surprising, as many scams request personal details and a payment upfront or at a later date. As this was the first year these questions on potential identity fraud were included, it is not possible to compare these results to those in previous surveys.

It was interesting to note that a much smaller proportion of victims of lottery scams reported a financial loss (5%) compared with a loss of information (14%). A similar difference was seen with phishing scams, where just 0.8 percent of victims of the scam lost money but 7.4 percent lost personal information. These results suggest that, like phishing attacks, the lottery scams received by victims in the sample were initially targeting personal information rather than requesting upfront payments. However, this highlights the need to continue to promote the risks associated with disclosing personal details. Future consumer fraud awareness campaigns could highlight the likelihood that disclosing personal information is likely to result in financial loss.

There also appears to be a weak but statistically significant relationship between sending personal information and belonging to a specific income bracket. Respondents earning less than $20,000 a year were more likely to send personal information to a scam than those earning more. In contrast, respondents earning more than $80,000 a year were less likely to send personal information to a scam than respondents in other income groups. However, income did not have a statistically significant relationship with victimisation in general, or for sending money. The reason for this is unclear from the available data. In addition, as the relationship between the two variables of income and sending personal information was weak, it is likely that other factors are also influence sending personal information. Further analysis needs to be conducted

to examine why the relationship between income and sending personal information might exist and why this is not a factor for sending money.

Age as a possible factor in the likelihood of victimisation

Age still appears to be a significant factor for fraud victimisation, consistent with previous research. However, it is important to note that most of these relationships were relatively weak, indicating that other factors would also have a role to play in an individual's victimisation. In 2008, respondents in the 55–64 year age group had higher than expected victimisation for AFF scams than the other age groups. In addition, the 55–64 and 65 years and over age groups both had higher than expected victimisation rates for lottery and phishing scams, although the relationship between age and phishing scams was relatively weak so should be interpreted with caution. However, due to the relatively small sample size, further research is needed to determine if this finding can be generalised to a more representative sample and to identify the implications this has for future awareness campaigns. In 2009, due to the findings being divided into losing money and losing information, the counts in each were too low to conduct robust statistical analysis. Despite this, observations can be made from general descriptive statistics. Unlike the 2008 survey, in 2009 it appeared that the 25–34 and 35–44 year age categories were over-represented in the groups that sent money and information. Meanwhile, those in the 45–54 year age group were under-represented in the sending personal information category.

These results are important as they indicate a potential relationship between age and the risk of victimisation. However, the nature of this relationship is still unclear because what was found significant in 2008 regarding the older age groups appears to potentially contradict the 2009 survey results. Unfortunately, this difference between 2008 and 2009 cannot be compared due to the different classifications used and the inability of 2009 data to be tested for significance. Regardless, the differences between the two years are consistent with previous research findings that at-risk age groups vary between studies (eg Smith & Budd 2009; Titus, Heinzelmann & Boyle 1995; van Wyk & Benson 1997; van Wyk & Mason 2001). It would be worthwhile investigating this relationship further to determine if certain age groups are more vulnerable to different scams than others. This would have implications for the best approach to educating the public on the risks of scams. For example, it may be more beneficial to target the older age groups for information about lottery scams and requests for personal details than to educate younger age groups on this issue.

How respondents view scams

The number of people who considered scam invitations as criminal in 2009 was lower than in the 2008 survey. Each scam category included in the 2008 survey was considered criminal by a larger percentage of respondents than in 2009. As the 2009 survey included more scam categories to choose from, it is difficult to determine if this is a trend.

In 2009, there were distinct differences in how respondents viewed different scam types. Being a victim of a scam can influence a respondent's perception of a scam's status as a crime. In 2009, a victim of a scam was more likely to consider any of the scams listed in the survey as a crime compared to non-victims. It is particularly interesting that work from home (19%) and 'other' (33%) scams had some of the lowest percentage of respondents who considered them a crime, when these are the scams that elicited the most victims among the sample. However, when testing for a relationship between victimisation and perception of scam types, victims were more likely than non-victims to consider work from home and 'other' scam types as crimes. The 'other' category was included in this analysis as a proxy for previously unidentified/emerging scam types. It is important to note that despite the significant result for the 'other' category, the category comprises a range of scam types so this finding should be interpreted with caution. In addition, the relationships between victimisation and perceptions of scam types had only a weak association; therefore, other factors should not be discounted as also affecting perceptions of scams.

It is particularly concerning that in 2009, 22 people did not consider work from home scams criminal, as this scam often involves recruiting money mules,

which is in itself a criminal act and could lead to the victim being prosecuted. This may support previous research that indicates new scam types are disproportionately successful (UKOFT 2009), as the work from home scam was identified as a new category in 2009 and the 'other' category covers all other scams not yet identified as a separate category.

Overall, despite the efforts of awareness campaigns, the 2009 survey results showed that there are still many respondents who do not consider some scams as criminal, although this varied by scam type. The decrease in the number of respondents who identified scams as criminal between 2008 and 2009 is also concerning, if it is indicative of a robust trend. It is important that steps are taken to ensure that the public do not become complacent about scams and that future awareness campaigns do not just raise awareness of the existence of these schemes, but also highlight their illegality.

Reporting scams

Reporting scams and victimisation

Overall, the rate of reporting of consumer fraud remains poor. Just over half the fraud victims in the 2009 survey reported their experience to a formal agency, a figure down on the 63 percent in 2008. In 2009, it was of concern that 17 percent of victims did not disclose their victimisation to anyone at all. These figures demonstrate that victims and indeed anyone who receives scam material need to be encouraged to report these fraudulent requests. Increased reporting rates will contribute to a greater understanding of the size of the problem and the types of scams affecting individuals. This understanding can, in turn, be used to tailor future prevention campaigns to include the most successful scams and target those individuals most at risk of victimisation.

The 2009 survey examined the relationship between victims and reporting behaviour. Unsurprisingly, being a victim of a scam increased the likelihood of reporting to a formal agency, although not the likelihood of reporting a scam to family and friends. However, this relationship was weak, indicating that there are other factors that influence reporting. A victim not reporting a scam attempt to family and friends is consistent with previous research that found that fraud victims may be embarrassed to report as they feel gullible (UKOFT 2009) or guilty about being scammed (Walsh & Schram 1980). However, it is important to note that the question about whether a person reported a scam does not distinguish whether the respondent answered in relation to a successful scam or for all scam attempts they received. There was also a relationship found between age and reporting. The 25–34 year olds were less likely to report and 55–64 year olds were more likely to report a fraud than expected.

In addition, weak yet statistically significant relationships were found between reporting behaviour and those who sent money to a scam. Those who sent money were more likely to report to a scam in general (ie to family and friends and/or a formal agency) than those who did not send money. The positive relationship between sending money and reporting behaviour remained significant even when the two were tested independently (ie sending money and reporting to a formal agency, and sending money and reporting to family and friends). A similar relationship was found with respondents who sent information. They were more likely to report a scam generally (ie either family and friends or a formal agency), or to a formal agency only than those who did not send information. However, there was no relationship between sending information and reporting a scam to friends and family only. In addition, the relatively small relationship between reporting and sending money and/or information suggests that other factors would also contribute to reporting behaviour and therefore should be considered in any future analysis of reporting behaviour.

Reporting scams and income

A person's level of income can also influence reporting behaviour. Respondents earning less than $20,000 a year were more likely to report a scam to a formal agency than otherwise expected. However, respondents earning over $80,000 a year were less likely to report a scam to family and friends than respondents in other income brackets. It is unclear why these relationships exist, although it is important to remember that a respondent does not need to have responded positively to a scam to report it. In

addition, the strength of this relationship is relatively weak, suggesting a more thorough examination into income and reporting is required.

It is important to work towards increasing the level of awareness that scams involve illegal activities and should be reported just as any other crime would be. Increased reporting would provide greater information on the types of frauds attracting victims, the types of victims most in need of intervention and targeting of prevention campaigns. It is also important that victims of scams are recognised as victims of a crime, rather than just unfortunate people who have lost money.

Reasons for not responding to scams

In 2009, the addition of the question of why people do not respond to scams offered a greater insight into why respondents chose not to respond to certain scam types. As supported by previous research, it appears that prior exposure to the scam (such as receiving similar offers in the past and being made aware of the scam via the media or public source) is a key factor in choosing not to respond, while responses for not responding such as *knew a victim* were comparatively lower (5%). This indicates that people analyse and make judgements about scam invitations, rather than solely relying on information given to them about the risks. Even among the victim group, this was selected by almost 50 percent of respondents, indicating there is a definite process by which people, even victims, determine which invitations to respond to. This means that scams that are more 'realistic' in their approach will be more successful.

There appeared to be a difference between respondents who had seen the scam in the media or another public source and those who had not. This was true for 54 percent of the total sample and 59 percent of those who did not respond, but only true for 40 percent of scam victims, which indicates victims may not have been exposed to scam prevention material as much as non-victims were. Other interesting discrepancies in the responses were in the *wanted to but couldn't afford to* and *was told it was a scam* options, with the victim group providing these responses more often in both cases. This indicates that respondents can make decisions to respond to a scam based on factors other than if the activity might be criminal, such as an inability to respond (eg prohibitive cost of the scam request) or actually being told by someone else not to respond, to prevent victimisation.

Suggestions for future campaigns

As scams are always evolving, with new typologies constantly emerging, the ACFT survey can improve its use as a tool for delivering in-depth knowledge about scams and scam victims, in addition to the general information already gathered. To do this, an addendum could be added each year, which could focus on a particular theme or victim group that the ACFT wishes to examine further. This would allow for a focus on any newly identified or increasing scam types. As each year of the ACFT awareness campaign has a thematic focus, such as the 2008 *Seduction and Deception Scams*, the addendum could be developed to tie in with the theme of each campaign as identified from the previous year's survey.

The findings from the survey regarding the different rates and types of victimisation by age groups, income and perceptions of crime, in addition to the other significant findings, need to be further explored with a more representative sample. The previous research available has also consistently found victim age to be significant in being scammed, but the age group varies between studies. Despite this, early findings suggest that this information could be used to develop a more strategic approach to the campaign, by tailoring scam and fraud messages to appeal to the target at-risk age or income groups. In addition, as highlighted throughout the report, most of the statistically significant findings demonstrated a weak relationship, with only a few exceptions. Therefore, consideration must be given to what other factors may be influencing an individual's behaviour in regards to responding to a scam, their perceptions of scams and reporting behaviours that could then be explored in future surveys.

The need to encourage reporting of scams was also evident in the findings. In light of the research indicating that stigma and embarrassment relating to being scammed are most likely affecting reporting rates, it could be worthwhile to focus campaigns on changing general public attitudes about scam victims. A theme that would help try to reduce the stigma of being a victim could assist in addressing the problem of limited reporting. The fact that some scams are still not perceived as crimes—even by some of the victims—may indicate that the message that scams are crimes needs to be re-highlighted. The ACFT campaign could also place more emphasis on the importance of reporting scams, whether an individual was victimised or not.

The results from the questions that explore why respondents did not respond to a scam invitation have implications for future fraud prevention campaigns. They indicate that having previous exposure to a recognised scam type, either by receiving an invitation, or seeing the scam highlighted in the media or public source, is a factor in preventing people becoming victimised. Overall, this could indicate that raising awareness of scam types could be an effective way to reduce victimisation and lends support to the overall ACFT approach of a wide-reaching media campaign on fraud awareness.

References

All URLs correct at January 2011

Australian Bureau of Statistics (ABS) 2008. *Personal fraud 2007*. cat. no. 4528.0. Canberra: ABS

Australian Competition and Consumer Commission (ACCC) 2008a. *2007–08 Annual report: Incorporating the AER*. Canberra: ACCC

Australian Competition and Consumer Commission (ACCC) 2008b. *The little black book of scams. 2nd ed*. Canberra: ACCC

Australian Institute of Criminology (AIC) 2007. Money mules. *High Tech Crime Brief* no. 16. Canberra: AIC. http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb016.aspx

Australian Institute of Criminology (AIC) 2006. More malware: Adware, spyware, spam and spim. *High Tech Crime Brief* no. 11. Canberra: AIC. http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb011.aspx

Australian Payments Clearing Association (APCA) 2009. Payments fraud in Australia. *Media release* 15 May. http://www.apca.com.au/Public/apca01_live.nsf/ResourceLookup/Press_Release_Payments_Fraud_Statistics_6.pdf/$File/Press_Release_Payments_Fraud_Statistics_6.pdf

Choo K-K R, Smith RG & McCusker R 2007. The future of technology-enabled crime in Australia. *Trends & Issues in Crime and Criminal Justice* no. 341. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/341-360/tandi341.aspx

deVaus DA 1995. *Surveys in social research* (4th ed). St Leonards NSW: Allen & Unwin

Doig A 2006. *Fraud*. Devon: Willan

Grabosky PN, Smith RG & Dempsey G 2001. *Electronic theft: Unlawful acquisition in cyberspace*. Cambridge: Cambridge University

Hayes H & Prenzler T 2003. *Fraud. Profiling fraudsters: A Queensland case study in fraudster crime; final report to Crime Prevention Queensland*. Mt Gravatt, Queensland: Griffith University

Holt TJ & Graves DC 2007. A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology* 1(1): 137–154

KPMG 2009. *Fraud survey 2008*. Sydney: KPMG. http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/Fraud-Survey-2008.pdf

Kroll 2009. *Global fraud report: Annual edition 2008/2009*. New York: Kroll. http://www.kroll.com/library/fraud/FraudReport_English-UK_Sept08.pdf

Levi M & Burrows J 2008. Measuring the impact of fraud in the UK: A conceptual and empirical journey. *British Journal of Criminology* 48: 293–318

Levi M, Burrows J, Fleming M, Hopkins M & Matthews K 2007. *The extent, nature and economic impact of fraud in the UK*. UK: Association of Chief Police Officers' Economic Crime Portfolio

Mayhew P 2003. *Counting the costs of crime in Australia: Technical report*. Technical and background paper no. 4. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tbp/1-20/tbp004.aspx

Meyers S 2007. Introduction to phishing, in Jakobsson M & Meyers S (eds), *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. New Jersey: John Wiley & Sons

National Fraud Authority (NFA) 2010. *A fresh approach to combating fraud in the public sector: The report of the Smarter Government Public Sector Fraud Taskforce*. http://www.attorneygeneral.gov.uk/nfa/WhatAreWeSaying/Documents/Smarter%20Government%20Public%20Sector%20Fraud%20Taskforce.pdf

Organisation for Economic Co-operation and Development (OECD) 2008. *Scoping paper on online identity theft: Ministerial background report DSTI/CP(2007)3/FINAL*. Paris: OECD. http://www.oecd.org/dataoecd/35/24/40644196.pdf

Office of Consumer and Business Affairs (OCBA) 2008. *Annual report 2007–08*. Adelaide: OCBA

PricewaterhouseCoopers 2007. *Economic crime: People, culture and controls: The 4th biennial global economic crime survey*. Berlin: PricewaterhouseCoopers

Roberts L & Indermaur D 2009. *What Australians think about crime and justice: Results from the 2007 Survey of Social Attitudes*. Research and public policy series no. 101. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/100-120/rpp101.aspx

Rollings K 2008. *Counting the costs of crime in Australia: A 2005 update*. Research and public policy series no. 91. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/81-99/rpp91.aspx

Shoepfer A & Piquero NL 2009. Studying the correlates of fraud victimization and reporting, *Journal of Criminal Justice* 37(2): 209–215

Smith RG 2008. Online personal fraud: Quantifying the extent of semantic and syntactic attacks in Australia. Paper presented at the *Twenty-Sixth International Symposium on Economic Crime*: 3 September: Cambridge

Smith RG 2007. Consumer fraud in Australia: An overview. *Trends & Issues in Crime and Criminal Justice* no. 331. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/documents/B/E/0/%7BBE011C7E-BC1B-44EF-AFD2-2332CD01EBE1%7Dtandi331.pdf

Smith R & 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

Smith R & Budd C 2009. Consumer fraud in Australia: Costs, rates and awareness of the risks in 2008. *Trends & Issues in Crime and Criminal Justice* no. 382. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi382.aspx

Smith RG, Holmes MN & Kaufmann P 1999. Nigerian advance fee fraud. *Trends & Issues in Crime and Criminal Justice* no. 121. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/121-140/tandi121.aspx

Stamp J & Walker J 2007. Money laundering in and through Australia, 2004. *Trends & Issues in Crime and Criminal Justice* no. 342. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/341-360/tandi342.aspx

Titus RM 1999. *The victimology of fraud*. Paper presented at the Restoration for Victims of Crime Conference convened by the Australian Institute of Criminology in conjunction with Victims Referral and Assistance Service: Melbourne: September 1999. http://www.aic.gov.au/events/aic%20upcoming%20events/1999/~/media/conferences/rvc/titus.ashx

Titus RM & Gover AR 2001. Personal fraud: The victims and scams in repeat victimisation, in Farrell G & Pease K (eds), *Crime prevention studies*, vol 12. Monsey, NY: Willow Tree Press

Titus RM, Heinzelmann F & Boyle JM 1995. Victimisations of persons by fraud. *Crime and Delinquency* 41(1): 54–72

Tomison AM 1999. Professional decision making and the management of actual or suspected child abuse and neglect cases: An in situ tracking study. Unpublished Doctoral Thesis. Melbourne: Monash University

UK Office of Fair Trading (UKOFT) 2009. *The psychology of scams: Provoking and committing errors of judgement May 2009*. Prepared for the Office of Fair Trading by the University of Exeter School of Psychology. http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf

Van Dijk JJM, Van Kesteren JN & Smit P 2008. *Criminal victimisation in international perspective: Key findings from the 2004–2005 ICVS and EU ICS*. The Hague: Boom Legal Publishers

Van Wyk J & Benson ML 1997. Fraud victimisation: Risky business or just bad luck? *American Journal of Criminal Justice* 21(2): 163–179

Van Wyk J & Mason KA 2001. Investigating vulnerability and reporting behaviour for consumer fraud victimisation: Opportunity as a social aspect of age. *Journal of Contemporary Criminal Justice* 17: 328–345

Walsh ME & Schram DD 1980. The victim of white-collar crime: Accuser or accused? in Geis G & Stotland E (eds), *White-collar crime: Theory and research*. Newbury Park, CA: Sage: 32–51

Yates D, Moore D & McCabe G 1999. *The Practice of Statistics* (1st Ed). New York: WH Freeman

Appendixes

Appendix 1: 2008 online questionnaire

Australasian Consumer Fraud Taskforce survey

AUSTRALASIAN
CONSUMER FRAUD
TASKFORCE

AN INITIATIVE OF THE STATE, TERRITORY AND
AUSTRALIAN AND NEW ZEALAND GOVERNMENTS

1. Over the last 12 months, have you ever received a call, email, SMS or letter from someone you don't know in relation to a notification of a) having won a lottery b) a request for assistance to transfer money from another country (such as Nigeria or other African countries) c) a request by a business (such as a bank) to confirm your bank account or personal details (phishing scams) d) a request to supply you with financial advice, or e) some other scam request?

☐ Yes

☐ No [Click on this link to go to question 8]

2. How were you contacted in relation to:

Type of scam	Mail	Email	Phone	SMS	Other
Notification of having won a lottery	☐	☐	☐	☐	☐
A request for assistance to transfer money from another country (such as Nigeria or other African countries)	☐	☐	☐	☐	☐
A request by a business (such as a bank) to confirm your bank account or personal details	☐	☐	☐	☐	☐
A request to supply you with financial advice	☐	☐	☐	☐	☐
Other type of scam	☐	☐	☐	☐	☐

If 'Other' type of scam please specify what the contact was about

3. Over the past 12 months have you ever replied positively to any of these unsolicited contacts?

- ☐ Yes
- ☐ No [Click on this link to go to question 6]

4. How many times over the last 12 months have you replied positively to each of the following types of unsolicited invitation? (Please answer each one)

Type of scam	Never	Once	Twice	Three time	Four times	Five or more times	Don't know
Notification of having won a lottery	☐	☐	☐	☐	☐	☐	☐
A request for assistance to transfer money from another country (such as Nigeria)	☐	☐	☐	☐	☐	☐	☐
A request by a business (such as a bank) to confirm your bank account or personal details	☐	☐	☐	☐	☐	☐	☐
A request to supply you with financial advice	☐	☐	☐	☐	☐	☐	☐
Other type of scam	☐	☐	☐	☐	☐	☐	☐

If other selected please specify what that content was about

5. What is your best estimate of how much money you paid out as a result over the last 12 months?

NOTE: this is **before** any repayment by your insurance, the bank or legal action—this is the **amount you have lost** as a result of the scam **NOT** the amount of money you would have received had the offer been true

- ☐ None
- ☐ Don't know/can't remember
- ☐ I'd rather not answer
- ☐ The amount in the box below

The following amount $

6. Have you reported any of these unsolicited invitations to any agency, regulatory authority or business?

- ☐ Yes
- ☐ No [Click on this link to go to question 8]

7. If **yes**, which ones?

Please check more than one box if applicable

- ☐ Police agencies
- ☐ Consumer Affairs or Fair Trading Agency
- ☐ Australian High Tech Crime Centre
- ☐ The business represented (eg eBay or financial institution or Trade Me in NZ)
- ☐ Internet Service Provider
- ☐ Unable to recall
- ☐ Other (specify below)

8. How do you regard each of the following incidents?

Please answer for each one. Only one option available for each line.

Type of scam	A crime	Wrong, but not a crime	Just something that happens	Don't know
Lottery scams	☐	☐	☐	☐
Advance fee/money transfer scams	☐	☐	☐	☐
Phishing scams	☐	☐	☐	☐
Unsolicited financial advice scams	☐	☐	☐	☐

9. How did you hear about the Fraud Fortnight Campaign in 2008?

Please select one.

- ☐ Media article
- ☐ Agency website
- ☐ Scamwatch website
- ☐ Poster or pamphlet
- ☐ Referred by other agency
- ☐ Word of mouth (friends, family etc)
- ☐ I've not previously heard about the Fraud Fortnight campaign
- ☐ Other (specify)

10. Were you aware of the Australasian Consumer Fraud Taskforce campaign that was conducted in March 2007?

- [ ] Yes
- [ ] No

11. Did you answer the online survey conducted in March 2007?

- [ ] Yes
- [ ] No

Could you please provide some general information about yourself so the Taskforce will know which groups of people have taken part?

12. Which of the following age brackets contains your age?

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

13. Where do you normally reside?

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

14. What is your sex?

- [ ] Male
- [ ] Female

15. In what capacity did you fill out this survey?

Please choose the option that best suits you.

Not supplied

Member of the public

A member of the police

My employer is a private sector Australasian Consumer Fraud Taskforce partner

My employer is a government sector Australasian Consumer Fraud Taskforce partner

Australian Capital Territory Office of Fair Trading

Australian Communications and Media Authority Department of Communications, Information Technology and the Arts

Australian Competition and Consumer Commission

Australian High Tech Crime Centre

Australian Institute of Criminology

Australian Securities and Investment Commission

Consumer Affairs Victoria

Department of Broadband, Communications and the Digital Economy

New South Wales Department of Fair Trading

New Zealand Commerce Commission

New Zealand Ministry of Consumer Affairs

Northern Territory Department of Justice

Queensland Department of Tourism, Fair Trading and Wine Industry Development

South Australia Office of Consumer and Business Affairs

Tasmanian Office of Consumer Affairs and Fair Trading

Western Australia Department of Consumer and Employment Protection

Appendix 2: 2009 online questionnaire

Australasian Consumer Fraud Taskforce Survey 2009

Question 1—Over the last 12 months, have you been contacted in any way (including by phone, email, letter, on the internet and 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

Yes	☐
No (Skip to Q12)	☐

Question 2—How were you contacted in relation to each of the following?

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	☐	☐	☐	☐	☐	☐
a request for assistance to transfer money out of another country (such as Nigeria)	☐	☐	☐	☐	☐	☐
a notification of an inheritance	☐	☐	☐	☐	☐	☐
a request by a business to confirm your personal details or passwords (phishing scams)	☐	☐	☐	☐	☐	☐
a request to supply you with financial advice	☐	☐	☐	☐	☐	☐
an opportunity to work from home	☐	☐	☐	☐	☐	☐

pursuing a personal relationship that later turned out to be false						
other type of scam						

If 'other' type of scam, please specify what the contact was about	

Question 3—Over the last 12 months, have you responded positively in any way to these unsolicited contacts?

Responding positively includes contacting the person/s in any way to request further information, providing personal details or sending money etc

Yes	
No (Skip to Q9)	

Question 4—How many times over the last 12 months have you responded positively to each of the following type of unsolicited contact?

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							
a request for assistance to transfer money out of another country (such as Nigeria)							
a notification of an inheritance							
a request by a business to confirm your personal details or passwords (phishing scams)							
a request to supply you with financial advice							
an opportunity to work from home							
pursuing a personal relationship that later turned out to be false							
other type of scam							

Question 5—Have you ever sent money as a result of any of these unsolicited contacts?

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 sent before any intervention or repayment from insurance, your bank, or legal action.

Type of Scam	Yes	No	Don't know/ can't remember
notification of having won the lottery or some other prize			
a request for assistance to transfer money out of another country (such as Nigeria)			
a notification of an inheritance			
a request by a business to confirm your personal details or passwords (phishing scams)			
a request to supply you with financial advice			
an opportunity to work from home			
pursuing a personal relationship that later turned out to be false			
other type of scam			

Question 6—If you responded 'yes' to any of the options in Question 5, what is your best estimate of the 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 eg $1,000.00 should be entered as 1000.

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

Don't know/Can't remember	
I'd rather not say	
The amount in the box below	

Please indicate the amount in whole dollars	

Question 7—Have you ever disclosed personal details or passwords as a result of these unsolicited contacts?

Type of Scam	Yes	No	Don't know/can't remember
notification of having won the lottery or some other prize			
a request for assistance to transfer money out of another country (such as Nigeria)			
a notification of an inheritance			
a request by a business to confirm your personal details or passwords (phishing scams)			
a request to supply you with financial advice			
an opportunity to work from home			
pursuing a personal relationship that later turned out to be false			
other type of scam			

Question 8—How many times were you in contact with the person before you sent money or personal information?

Once only	
Between one and five times	
Five to twenty times	
More than twenty times	
I can't recall	

Question 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	
Had received similar offers before and thought they were scams	
Had seen/heard this was a type of scam in the media or a public source	
Was told it was a scam by someone I knew	
Someone I know has responded positively to a scam before	
Wanted to respond but could not afford to participate	
Something was not quite right with the offer or invitation	
Other (please specify below)	

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

Family/friends	
Police Agencies	
Consumer Affairs or Fair Trading Agency	
Australian High Tech Crime Centre	
The business represented (e.g bank, ebay etc)	
Internet Service Provider	
Unable to recall	
Other (please specify below)	

Question 11—How do you regard each of the following incidents?

Type of Scam	A crime	Wrong but not a crime	Just something that happens	Don't know
notification of having won the lottery or some other prize				
a request for assistance to transfer money out of another country (such as Nigeria)				
a notification of an inheritance				
a request by a business to confirm your personal details or passwords (phishing scams)				
a request to supply you with financial advice				
an opportunity to work from home				
pursuing a personal relationship that later turned out to be false				
other type of scam				

Question 12—How did you find out about this survey?

Media Article	
A government website	
Scamwatch website	
Poster or pamphlet	
Referred by other agency	
Word of mouth (family, friends etc)	

Other	
If other please specify	

Question 13—Have you responded to the online survey in any previous years?	
2008	
2007	
2006	

Question 14—Are you aware of the 2009 fraud awareness campaign run by the Australasian Consumer Fraud Taskforce?	
Yes	
No	

Question 15—Were you aware of any previous campaigns run by the Australasian Consumer Fraud Taskforce?	
Yes	
No	

Question 16—What is your age?	
17 and under	
18–24	
25–34	
35–44	
45–54	
55–64	
65+	

Question 17—What is your gender?	
Male	
Female	

Question 18—Where do you normally reside?

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

Please specify country

Question 19—What is your average yearly income?

- Under $20,000
- $20,000–$39,999
- $40,000–$59,999
- $60,000–$79,999
- Over $80,000
- I'd rather not say

Question 20—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 partner
- My employer is a government sector Australasian Consumer Fraud Taskforce partner
- Other government agency