ACCC Report

Targeting scams

Report of the ACCC on scams activity 2013

June 2014

ISBN 1 922145 24 6

Important notice

This guideline is designed to give you basic information; it does not cover the whole of the *Competition and Consumer Act 2010* (Cth), the *Australian Securities and Investments Commission Act 2001* (Cth) or other relevant legislation and is not a substitute for professional advice.

Moreover, because it avoids legal language wherever possible and there may be generalisations about the application of the above Acts, some of the provisions referred to have exceptions or important qualifications. In most cases, the particular circumstances of the conduct need to be taken into account when determining how these Acts apply to that conduct.

ACCC_05/14_864

www.accc.gov.au

Foreword

Delia Rickard

The Australian Competition and Consumer Commission's (ACCC) fifth annual report on scams activity in Australia highlights the significant harm that scams continue to cause to the Australian community.

In 2013 nearly 92 000 scam-related contacts were received by the ACCC, an increase of nearly 10 per cent from 2012. Breaking the rising trend of recent years, in 2013 reported financial losses from scams decreased slightly to a total of nearly $90 million. Actual losses are likely to be much higher than what is reported to the ACCC—people report scams to a number of agencies, some don't recognise that they have fallen for a scam, and unfortunately many others are too embarrassed to report their experience.

Financial losses form just one part of the picture of the impact of scams activity in Australia, with the non-financial losses borne by victims unquantifiable. Scams have the capacity to devastate the lives of victims, who report suffering adverse effects to their mental health, work capacity and close personal relationships. Unfortunately victims often suffer in silence because of the social stigma that is attached to falling victim to a scam. The ACCC works hard to change this attitude through education and awareness raising.

Scams also cause significant harm to businesses through loss of revenue either directly as victims, indirectly through scammers impersonating them, or in costs associated with ongoing monitoring and security upgrades.

The flow-on effect of scams to the economy more broadly should also not be underestimated. Consumer trust and confidence to participate in the economy is undermined by scams activity, particularly where scammers target new products and services, or evolving markets such as online shopping.

Finally, when someone's life savings and home are lost as a result of scam victimisation, they may ultimately become dependent on Australia's welfare system.

This year's report highlights that relationship scams cause the most significant individual, social and economic harm in Australia. In these scams, the perpetrators invest considerable time and energy into building a relationship based on deceit to ultimately secure personal gain. These scams are more often than not carried out online, with scammers using the internet as a way to shield their identity and remain at arm's length while establishing a connection.

Unfortunately the statistics prove that scammers are reaping the rewards of adopting a personalised approach—in 2013 dating and romance scams moved to number one position for reported financial losses, with over $25 million lost.

The ACCC has previously directed efforts at dating and romance scams and we note a continuing decline in the number of people who responded to an approach by a scam admirer and subsequently lost money—from 48 per cent in 2011 to 46 per cent in 2012 to 43 per cent in 2013. Nevertheless, this conversion rate is still significantly higher when compared to most other scam categories, and total financial losses remain high. Clearly, there is still much more to be done.

In 2014 the ACCC will take steps to do just that, with the disruption of relationship scams a compliance and enforcement priority. We will use financial intelligence to identify and warn suspected victims that they have been defrauded. We will also work with business enablers such as online dating service providers, money remittance agencies and financial institutions to make it harder for scammers to access victims or receive money from them. This work will be done in collaboration with other public and private sector bodies working to help unsuspecting Australians cease to be scam victims. Supporting this will be ongoing educational efforts, with

the Australasian Consumer Fraud Taskforce's 2014 Fraud Week campaign, 'Know who you're dealing with', asking people to take a step back and think twice about sending money to someone they met online.

In addition to going online to connect with victims, 2013 data also suggests that scammers are getting better at stealing people's personal details and money online. While online scams remained second to phone in terms of overall scam delivery levels, they caused the most financial harm—close to $42 million was reported lost via this approach.

It is now more important than ever to be aware that scammers are not just after money—our personal information is valuable, too. In 2013 the ACCC observed a significant increase in phishing and identity theft scams, with scam contacts increasing by over 73 per cent from 2012 levels to over 15 000 contacts. At the same time, reported financial losses remained relatively low compared to other scam types, with scammers primarily 'fishing' for personal identification to be used for later gain. Such a rise in this type of scams activity is a sobering reminder that we need to be vigilant in protecting our personal information, particularly where consumer data is only going to increase in value as a commodity. As with relationship scams, it is imperative that consumers consider who they're really sharing their personal details with to avoid misuse.

The ACCC and other agencies continue to work hard to protect the Australian community from scams. The global nature of today's scam can frustrate law enforcement efforts, which is why education and awareness raising is a key pillar in scams prevention. It is pleasing to observe that the ACCC's SCAMwatch website continues to grow year on year as a resource turned to by the public, with visits to the site increasing by 25 per cent in 2013. The SCAMwatch free radar alert service, which in 2013 increased by 30 per cent to nearly 30 000 subscribers, is a good example of government and industry working together for the common goal of protecting the Australian community by alerting them to current scams.

While scammers are professionals at evading the law, the ACCC does take enforcement action where appropriate to deter and discourage scammers targeting Australians. In 2013 the ACCC successfully took court action against a number of traders targeting small businesses with misleading and deceptive or scam-like conduct including a pyramid selling scheme, an online business directory scam with a philanthropic slant, and an office supply scheme.

The ACCC is also determined to find other innovative ways to counter scammers' evasive behaviour, with disruption a key tool in this approach. In 2013 the ACCC continued to collaborate with private and public sector entities to tackle current scams, including leading a coordinated effort in its ongoing role as chair of the Australasian Consumer Fraud Taskforce. The ACCC looks forward to working with the Taskforce to disrupt relationship scams in 2014.

Relationships are tricky at the best of times. As connections become easier to forge online, it's timely that we reflect on those elements that form the basis of a relationship. Trust, honesty and respect—these are universal factors that transcend what platform we engage in. However, in the online environment, extra precaution is necessary as the subtle cues that people normally rely on to inform their judgement are often not visible in the virtual world. If someone is avoiding meeting in person or asks for money, watch out—they could be a scammer.

We hope that this report, and the work of the ACCC in coming years, helps reinforce the need for Australians to really ask themselves who they are dealing with.

Delia Rickard

Deputy Chair, Australian Competition and Consumer Commission
Chair, Australasian Consumer Fraud Taskforce

Contents

1. Snapshot of 2013

Overall contacts levels and financial losses

- In 2013 the ACCC continued to observe a high level of scams activity in Australia, with 91 927 scam-related contacts received from consumers and small businesses, an increase of nearly 10 per cent over 2012.
- Estimated scam losses reported to the ACCC totalled $89 136 975, representing an almost 5 per cent decrease from 2012 ($93 423 030)—a reversal in trend from 2011 and 2012 where large increases were observed. However, actual losses are likely to be higher as many scams go unreported and the ACCC is only one of several agencies that receive scam reports.

Most reported scams

- In 2013 dating and romance scams moved to number one position in terms of financial losses, with $25 247 418 reported lost. For the third consecutive year the ACCC has observed a decrease in the conversion rate of people who responded to an approach by a scam admirer and subsequently lost money—from 48 per cent in 2011 to 46 per cent in 2012 to 43 per cent in 2013. However, financial losses continue to remain substantially disproportionate to contacts, with dating and romance scams making up only 3 per cent of all scam-related contacts in 2013.
- Similar to previous years, the majority of people contacting the ACCC about scam-related activities in 2013 (slightly over 86 per cent) reported no financial loss. Nearly one third of people who lost money reported losing between $100 and $499, which indicates scammers continuing to prefer 'high volume scams'—that is, scams that are delivered to large numbers of recipients but cause smaller amounts of loss per victim.
- At the same time, the ACCC continued to receive reports of individuals suffering significant losses. Over 10 per cent of scam contacts reported losing above $10 000. However, there were only two reports of losses above $1 million in 2013 compared to six reports in 2012.
- In 2013 the top 10 scams reported to the ACCC in terms of contact levels remained the same with some minor movements in ranking. The three most commonly reported scams were advance-fee fraud, phishing and identity theft, and computer hacking scams.
- The ACCC observed a significant increase in phishing and identity theft scams, with reports increasing by over 73 per cent from 2012 to 15 264 contacts. Actual financial losses remained low, suggesting that scammers are instead seeking personal information for later gain.
- Computer prediction software scams saw a significant increase in both contacts and financial losses from the previous year, with an increase of 41 per cent in contact levels and associated losses more than doubling to a total of $9 144 288. This increase is likely attributable to a collapsed gambling system in Victoria, which received widespread media coverage.

Age range and location demographics

- In 2013, of all individuals who contacted the ACCC and provided their age, scams were most commonly reported by persons in the 45 to 54 age category. The percentage of reports from people who identified as 65 years and over nearly doubled to 18 per cent.
- The greatest amount of scam reports came from New South Wales, Victoria and Queensland. Contact levels and associated losses were largely consistent with the percentage of the Australian population by state and territory.
- At the end of 2013 the ACCC updated its data collection process and in 2014 will be able to analyse scam categories against new fields such as a victim's gender, whether they are a small business, or may be disadvantaged or vulnerable.

Scam delivery method

- In line with a shift in recent years, in 2013 over half (52 per cent) of scams were delivered via phone and text message, with combined total financial losses of $29 391 887. Telephone calls remained the most popular delivery method, with reports and losses rising in parallel by nearly 13 and 14 per cent respectively, and losses totalling $3 335 763. Scams delivered by text message decreased by around 35 per cent, while reported losses more than doubled to $1 848 805.
- Despite representing a lower percentage of contacts (40 per cent), scams delivered online caused the greatest financial harm with associated losses totalling $41 781 071. While contacts of reports delivered via email increased by nearly 14 per cent, financial losses almost halved (49 per cent), which could indicate scammers using email to 'fish' for personal information but turning to other online communication platforms such as social networking sites for monetary gain.

The ACCC's education and awareness raising activities

- The ACCC continued to educate the public about how to identify and avoid scams, and raise community awareness about current scams targeting Australians. SCAMwatch, the Australian Government's website for information about scams that is run by the ACCC, received 1 228 599 unique visitors in 2013, an increase of over 26 per cent from the previous year.
- The ACCC also continued to issue SCAMwatch radar alerts to its free subscription base, which in 2013 increased by 30 per cent to reach 29 150 subscribers. A total of 18 SCAMwatch alerts were issued warning about current scams, including joint radars issued with other government agencies and companies about scammers misusing consumer trust in these well-known entities.
- The ACCC's SCAMwatch_gov Twitter profile also continued to communicate with its 4374 followers in real time as scams emerged, with 583 tweets posted during the year.
- The 2013 National Consumer Fraud Week campaign, 'Outsmart the scammers!' (17–23 June), received significant media coverage as the ACCC and the Australasian Consumer Fraud Taskforce urged people to stay one click ahead of scammers when shopping online.
- *The Little Black Book of Scams* is the ACCC's most popular publication and 91 203 copies were distributed in 2013. A new small business scams factsheet was also produced.

The ACCC's collaboration, disruption and enforcement activities

- In 2013 the ACCC worked with a range of private and public sector representatives to disrupt scams including online shopping scams and the 'Yellow Pages' small business scam.
- The ACCC continued to chair the Australasian Consumer Fraud Taskforce, and hosted a conference and workshop as part of National Consumer Fraud Week where representatives across government, industry and academia explored how to minimise scams activity in the digital economy.
- The ACCC successfully prosecuted the perpetrators behind schemes targeting small businesses including the operators of a pyramid selling scheme, an online business directory scam with a philanthropic slant, and an office supply scheme.
- The ACCC also commenced planning for a national disruption project aimed at relationship scams, which is a 2014 compliance and enforcement priority. The ACCC will work closely with other agencies on this project, building upon previous work undertaken to disrupt relationship scams.

2. Scam contacts and trends

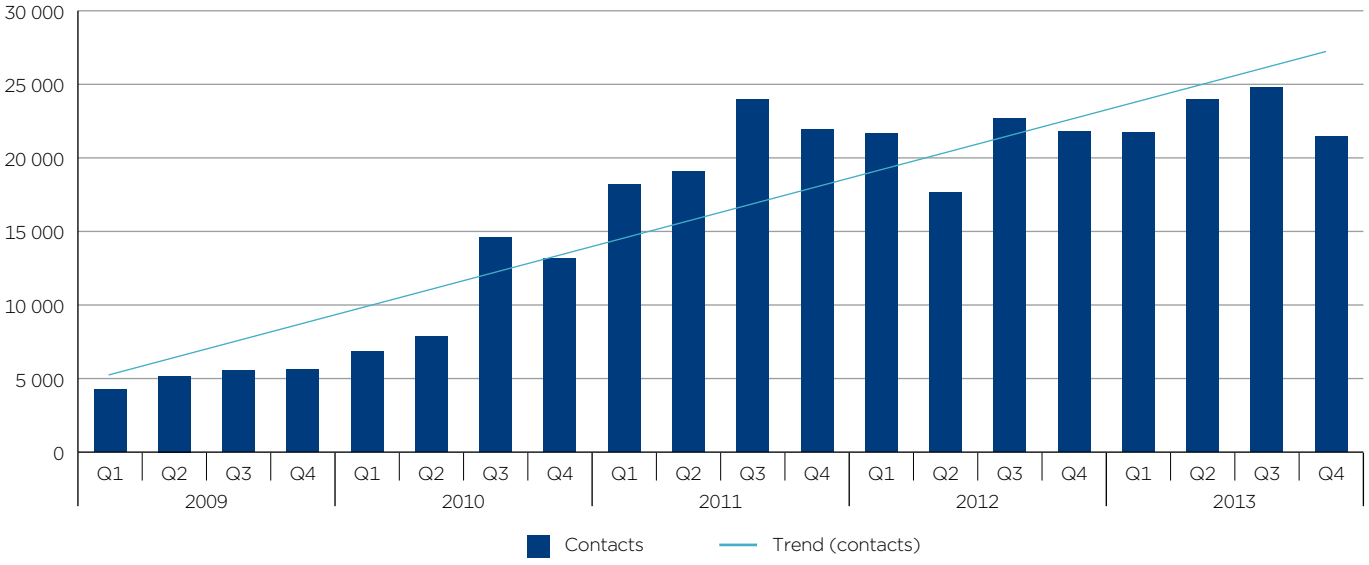
2.1 Scam contact levels

In 2013 the ACCC received 91 927 scam-related contacts (91 441 complaints and 486 inquiries).

This report is based solely on scam-related contacts to the ACCC and thus provides only part of the picture in terms of the scale of scams activity in Australia. The ACCC is just one of the primary government reporting agencies for scams, with many other authorities also performing an important role in assisting scam victims, including local consumer protection and law enforcement bodies. Recipients may also not report a scam to any agency, particularly where they have not identified or recognised the scam, or where no financial loss has occurred. Further, many scam victims may be too embarrassed to report their experience.

Figure 1 provides a comparison of scam-related contacts to the ACCC over the past five years, which shows a general upwards trend in contact levels.

Figure 1: Number of scam-related contacts to the ACCC 2009—2013



2.2 Financial losses to scams

In 2013 reports of financial losses arising from scams activity totalled $89 136 975, representing a nearly 5 per cent decrease on the amount reported in 2012 ($93 423 030). This is a reverse in trend from 2011 and 2012 where large increases were observed.

It is important to note that this total is based on information provided only to the ACCC and as such is likely to represent only a fraction of the financial losses suffered by Australians to scams in 2013.

In 2013 the number of consumers and businesses who contacted the ACCC about scams and who reported no financial loss remained relatively stable at 86 per cent. The remaining 14 per cent reported losses ranging from very small amounts for unsolicited credit card deductions and 'free' online offers to several millions reported lost to sports betting schemes.

The ACCC recognises that some reported losses may represent amounts that people believe they would have been entitled to if the offer were genuine. Where these reports have been identified, the reported loss has been removed from the data.

Figure 2 provides a comparison of scam-related financial losses reported to the ACCC over the past five years, with a slight decrease observed in both 2010 and 2013.

Figure 2: Reported financial losses to the ACCC from 2009 to 2013

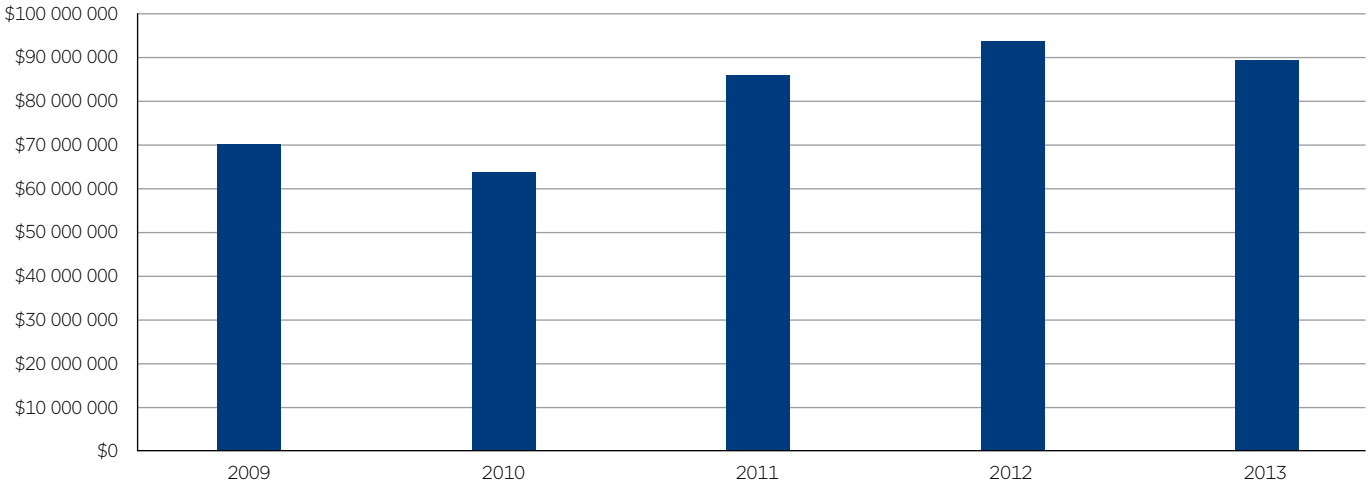


Table 1 provides an overview of financial losses reported arising out of each scam type. The top three scam categories were the primary source of money lost, with dating and romance, advanced fee/up-front payment and computer prediction software scams accounting for around two thirds of reported financial losses.

A list of scam categories by state and territory is provided at appendix 1.

Table 1: Overview of scam types reported to the ACCC in 2013 in order of total reported losses

Scam category	Amount reported lost	Contacts	Contacts reporting loss	Less than $10k lost	Greater than $10k lost	Contacts reporting no loss	Conversion rate
Dating and romance	$25 247 418	2 777	1 189	791	398	1 588	42.8%
Advanced fee/up-front payment	$24 988 234	28 748	2941	2578	363	25 807	10.2%
Computer prediction software	$9 144 288	1 037	392	284	108	645	37.8%
Investment	$9 083 512	829	235	146	89	594	28.3%
Lottery and sweepstakes	$5 065 359	9 354	581	488	93	8 773	6.2%
Online shopping	$5 046 729	8 402	3 766	3 678	88	4 636	44.8%
Job and employment	$3 206 486	2 979	401	354	47	2 578	13.5%
Phishing and identity theft	$2 467 287	15 264	665	612	53	14 599	4.4%
Computer hacking	$1 130 947	10 415	935	917	18	9 480	9.0%
Unexpected prizes	$995 288	3 933	190	169	21	3 743	4.8%
False billing	$724 772	3 672	445	431	14	3 227	12.1%
Psychic and clairvoyant	$482 746	132	58	52	6	74	43.9%
Door-to-door and home maintenance	$322 212	345	118	113	5	227	34.2%
Chain letter/pyramid scheme	$248 757	393	60	56	4	333	15.3%
Health and medical	$114 127	558	304	302	2	254	54.5%
Spam and 'free' internet offers	$60 705	1 046	140	140	0	906	13.4%
Mobile phone	$51 775	1 351	269	268	1	1 082	19.9%
Fax back	$24 071	173	3	2	1	170	1.7%
Other—scams outside predefined categories	$732 262	519	40	33	7	479	7.7%
Total	**$89 136 975**	**91 927**	**12 732**	**11 414**	**1 318**	**79 195**	**13.9%**

The true cost of scams

The impact of scams on Australian society and the economy is substantial, with financial losses just one part of the picture.

Financial losses

Reports of financial losses to the ACCC are only the tip of the iceberg as scam victims may report to other authorities, may be unwilling to report their experience, or may not even realise they have been scammed.

The Australian Bureau of Statistics' most recent *Personal Fraud Survey* (2010–11) estimates that Australians lost $1.4 billion to personal fraud (which includes credit card fraud, identity theft and scams).*

The financial repercussions resulting out of scams victimisation can range from a few dollars to losing one's life savings and/or house.

Non-financial losses

Scams can also devastate the lives of victims and their families beyond financial costs, with the emotional toll of these experiences an unquantifiable loss.

Individuals may suffer adverse effects on their mental health, work capacity, relationships and family.

Victims often suffer in silence as they are too embarrassed to speak up about their experience and seek help.

In reality, everyone is vulnerable to scams at some stage in life (see page 28 for more information).

Economic and societal losses

The cost of scams to the Australian economy and society more broadly should not be underestimated, with significant flow-on effects as a result of this activity.

Scams can cause significant harm to businesses through loss of revenue either directly as victims, indirectly through scammers impersonating them, or in costs associated with ongoing monitoring and security upgrades.

Scammers also increasingly undermine legitimate corporate and government entities by misusing consumers' trust in well-known brands, reputations and authority.

At the same time, consumer trust in new or evolving products, services and markets is undermined by scams activity, with one bad experience sufficient to discourage future participation in these parts of the economy.

Where scams result in total financial loss, victims ultimately become dependent on Australia's welfare system.

* Australian Bureau of Statistics, *Personal fraud survey 2010–2011*, Canberra, April 2012.

Table 2 provides a comparison of financial losses reported to the ACCC in 2013 and 2012 by loss range. As with previous years, scammers continued to favour sending 'high volume scams', which involve targeting a large number of victims with requests for small amounts of money. At the same time, reported losses between $1 million and $10 million fell from six reports in 2012 to two reports in 2013.

Table 2: Comparison of scam-related monetary losses reported to the ACCC in 2013 and 2012

Losses	Number of people reporting this loss amount in 2013	Percentage	Variance 2012
1–99	1 949	15.3%	–1.3
100–499	4 155	32.6%	0.5
500–999	2 096	16.5%	0.6
1000–9999	3 214	25.2%	0.2
10 000–49 999	961	7.5%	–0.6
50 000–499 999	340	2.7%	–0.4
500 000–999 999	15	0.1%	–0.1
1 million–10 million	2	0.02%	–0.04
Grand total	**12 732**	**100%**	**n/a**

2.3 Scam delivery methods

Scammers adopt a range of communication channels to deliver scams, and are quick to change their approach to exploit new developments in technology or popular mediums.

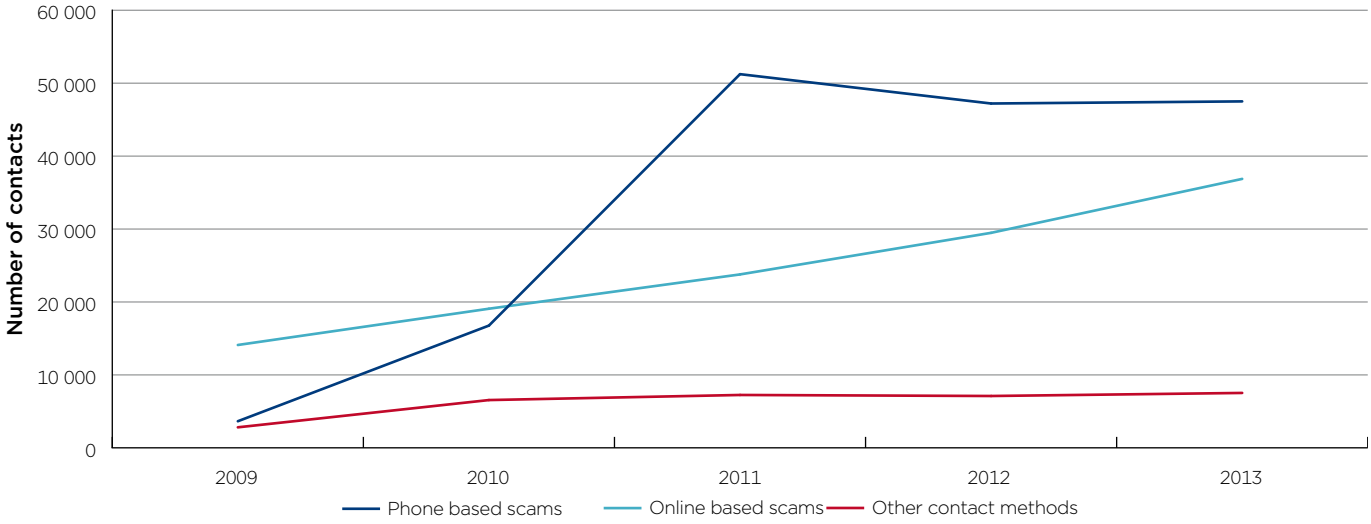
Table 3 provides a comparison of all scam delivery methods reported to the ACCC in 2013 and 2012, which highlights that scams delivered by phone (telephone calls and text messages) continued to be the most common method of targeting the public. Online delivery methods also continued to be favoured by scammers in 2013.

Table 3: Scam delivery methods during 2013 and 2012 based on reports to the ACCC

	2013		2012	
Scam delivery method	Number	Percentage	Number	Percentage
Telephone call	39 921	43.4%	35 419	42.3%
Text message	7 586	8.3%	11 797	14.1%
Email	22 155	24.1%	19 478	23.2%
Internet	14 724	16.0%	10 003	11.9%
Mail	5 845	6.4%	5 912	7.1%
In person	1 055	1.2%	764	0.9%
Fax	625	0.7%	430	0.5%
Not supplied	16	0.0%	NA	NA
Total	**91 927**	**100%**	**83 803**	**100%**

Figure 3 provides an overview of scam delivery methods over the past five years, which shows online scams closing the gap on phone as the preferred method of delivery.

Figure 3: Scam delivery methods 2009-2013 based on reports to the ACCC



Scams delivered by phone (landline and mobile)

In 2013 phone (landline and mobile) remained the most common scams delivery method reported to the ACCC. Almost 52 per cent of reported scams were delivered in this manner (47 502 contacts), with reported financial losses totalling $29 398 547.

Telephone calls remained the most popular scam contact method, with reports rising by nearly 13 per cent from 2012 to 39 921 and an associated rise in reported financial losses of nearly 14 per cent to $27 549 742.

Scams delivered by text message decreased by around 35 per cent from 2012 levels, while reported losses more than doubled to $1 848 805. This increase may be attributed to four contacts where reported losses arising from a scam delivered via text message were over $100 000, two of which exceeded $400 000. In 2012 the highest loss reported was approximately $80 000.

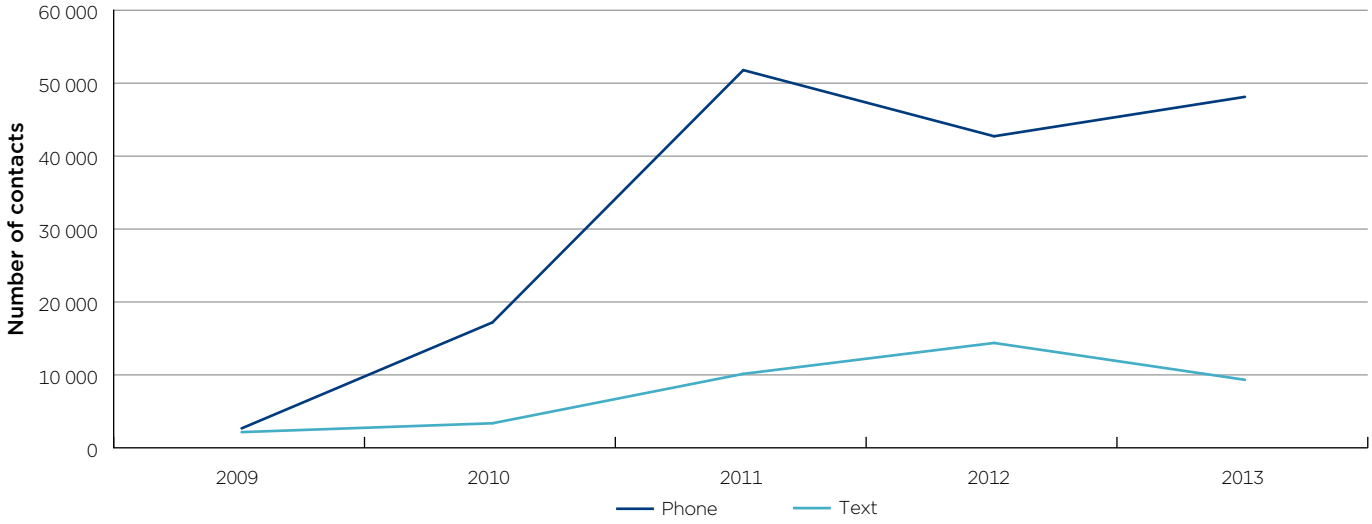
The most prominent scams delivered via telephone calls were advanced fee/up-front payment, computer hacking, and phishing and identity theft scams. The vast majority of scams delivered via text message were fake lotteries, unexpected prizes and online shopping scams.

Scammers typically called or sent text messages where they pretended to be from government or large well-known companies including banks, computer companies, telecommunications service providers and lottery agencies.

As with previous years, the ACCC continued to receive reports that indicate many telephone scams may be operating through overseas call centres. This is likely to be due to the continued outsourcing by criminal networks of scripted call centre operations to cheap overseas providers, as well as the growing availability of low or no-cost VoIP call services. These cold calling scams are usually directed at the home telephone and account for the majority of telephone scams reported to the ACCC.

Figure 4 highlights the shift in scams delivered via a phone call or SMS reported to the ACCC over the past five years.

Figure 4: Scams delivered via telephone (voice and text message) 2009–2013



Scams delivered online (internet and email)

In 2013 scammers continued to take advantage of the online environment to deliver scams to Australians, with this delivery method netting the highest financial losses.

Contacts of scams delivered online increased in 2013 by 6.5 per cent to represent just over 40 per cent of all scam approaches. The ACCC received 14 724 reports of scams delivered via the internet and 22 155 reports of scams delivered via email, increases of nearly 47 and 14 per cent respectively.

While total reported financial losses from online scams decreased in 2013 by 20 per cent, losses remained high at $41 781 071. Reported losses from scams delivered by the internet increased only slightly by 5 per cent to $29 382 173, however losses arising out of scams delivered via email decreased significantly by 49 per cent to $12 398 898. This decrease may suggest that scammers are primarily using email to phish for personal details, and that other online communication channels such as social media are being used to con people out of their money.

Just as the internet has revolutionised the way that people connect with each other, so too has it opened up the world to scammers, who are able to reach would-be victims with the click of a button. Online communication channels such as email and social networking forums allow scammers to communicate anonymously from anywhere in the world. Victims are often not even aware that they have been scammed, with the realisation only dawning when they receive a credit card statement or invoice.

The internet also provides scammers with a smokescreen to hide behind, with the global and anonymous nature of the online environment helping to mask their physical location.

The ongoing evolution of online and mobile communications means that the public needs to be alert to new scam approaches. Scammers will take advantage of the internet to transmit scams to any personal device that is connected to the web—whether it be at home on the computer, in one's pocket via a smart phone, or anywhere through a tablet.

In 2014 the ACCC updated its scams reporting form and, in future reports, will be able to provide more detailed analysis on scams, including the degree of scams activity delivered via social media.

Misuse of consumer trust and data online

In the online environment, scammers are quick to exploit not only consumer trust, but also data, in their efforts to secure personal or financial gain.

Consumer trust

Misuse of consumer trust online is rife as scammers take advantage of well-known corporations or authorities, or legitimate and popular online communication platforms, to pretend to be genuine.

Online shopping scams are premised on scammers deceiving victims into thinking that they are transacting with a legitimate buyer or seller, with activity often occurring on trusted shopping platforms.

In the classic phishing scam, email platforms are used to deliver scams into people's inboxes that appear to come from a trusted entity such as a financial institution or government body, with the scammer 'fishing' for personal or financial details.

Scammers are also not afraid to adopt a more personalised approach, using social networking forums to 'befriend' victims and then use their personal information against them.

Scammers also create mirror websites where consumers believe that they are transacting with a legitimate company, but instead are being tricked into handing over personal information and money.

The impact of this activity cannot be underestimated, with consumers more likely to stop participating as digital citizens after having been defrauded.

Personal data

Like legitimate businesses, scammers also recognise the value of personal data—a commodity that is only going to increase in value with the uptake of online shopping. In the context of scams activity, personal data is a commodity in itself with scammers buying and selling identity kits in black markets to commit other criminal acts.

Scammers harvest personal data online in a number of ways. The phishing scam is the most common approach, with people responding to phoney requests for information that sound plausible at the time. Scammers also use malicious software to gain access to people's computers and the information stored within. They may also simply listen in on conversations that take place on social networking forums.

Personal data can open the door for a scammer to carry out a range of criminal activity such as computer hacking, network attacks or identity theft. In some of the more sophisticated scams, personal data is used as the basis of social engineering whereby the target has their own information used against them to manipulate them into falling victim.

When engaging online, it is critical that consumers consider who they are sharing their data with to avoid it being misused.

2.4 Demographics

Demographics are a useful tool in scams prevention by providing authorities with a deeper understanding of where scams are causing the most harm based on personal dimensions such as age, gender and location. This information can help inform what areas of the community are being most affected by scams and thereby inform possible targeted prevention strategies.

While the provision of personal information is voluntary, in 2013 the ACCC received a number of scam-related contacts where an individual self-identified their age or location.

This section provides a summary of 2013 contacts by age and location, and a look at additional demographic data that the ACCC is now collecting.

Age range

The following information is a summary of observations about the age range of people who reported scams activity to the ACCC.

The ACCC notes limitations in what can be analysed from 2013 data, with a change in scams data collection processes during the reporting period resulting in only a small percentage of contacts where the individual identified their age—2152 contacts in 2013 compared to 21 116 in 2012. This issue was resolved when the ACCC updated its scams reporting form for 2014 with a greater focus placed on the collection of demographics. This lower sample size therefore reduces the confidence in the distribution of scams activity by age for the reporting period.

Table 4 outlines scam contacts to the ACCC where individuals self-identified their age. Contrary to the concerns of some, young people were not overrepresented in scam contacts to the ACCC, with people aged under 25 continuing to comprise around 6 per cent of contacts where age range was indicated.

On the other hand, Australians aged 64 or older comprised 18 per cent of scam contacts where age was provided.

People who indicated their age as falling between the 35 to 44 and 45 to 54 age brackets remained the most likely to report a scam to the ACCC, together representing just over 40 per cent of contacts where age was provided.

Table 4 also provides a comparison of scam conversion rates by age range. The conversion rate is the percentage of scam contacts that report a loss. A low conversion rate would indicate a high probability that the scam is recognisable while a high conversion rate suggests that a scam contact is more likely to result in the loss of money.

In 2013 individuals under 18 years were less likely to report a scam to the ACCC, yet had the highest conversion rate of all groups at 44 per cent. At the other end of the spectrum, Australians aged 64 or above had the lowest conversion rate out of all age groups at 7 per cent.

Table 4: Age ranges provided by consumers reporting scams to the ACCC in 2013

Age range	Percentage	Conversion rate
<18	0.4%	44%
18–24	5.9%	24%
25–34	14.5%	26%
35–44	19.2%	15%
45–54	22.9%	13%
55–64	18.6%	14%
>64	18.4%	7%
Total	**100%**	**N/A**

Geographic location

The ACCC also collects data on the geographic location of people reporting scams.

Figure 5 shows a comparison of scam contacts received by the ACCC in 2013 from within Australia. New South Wales again received the greatest number of scam reports followed by Victoria and Queensland. Contacts for the remaining states and territories were below 10 per cent.

In addition to the above figures the ACCC received 3959 scam contacts from people based overseas, and a further 170 where their location was not provided, representing approximately 4.5 per cent of total contacts.

Figure 5: Scam contacts' location by state and territory 2013

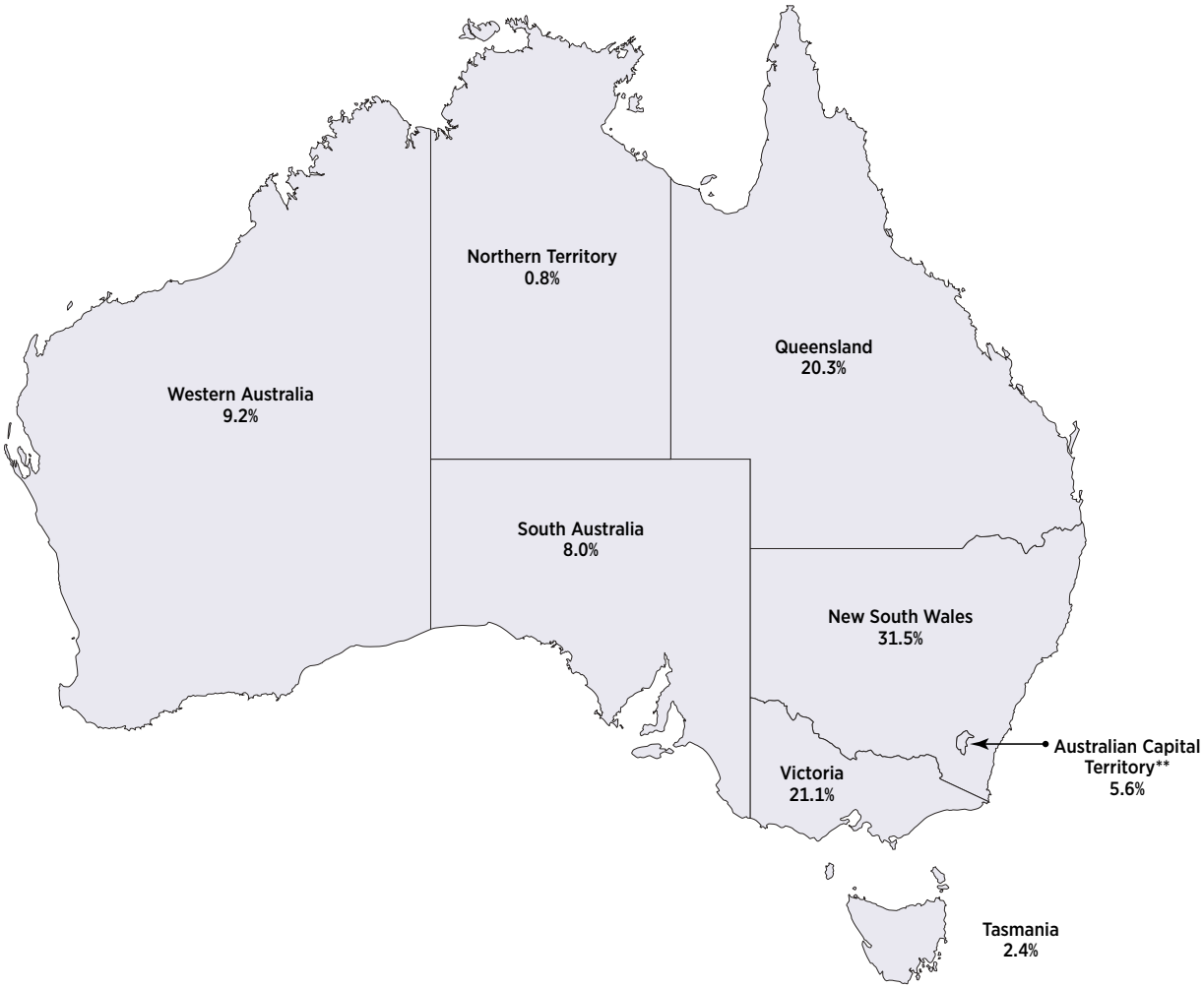


Table 5 provides a comparison of scam contact levels and financial losses against the distribution of the Australian population as a whole. Contact levels and associated losses reported to the ACCC were largely consistent with the percentage of the Australian population by state and territory, with the exception of the Australian Capital Territory (ACT). In 2013 the SCAMwatch online reporting form listed the ACT as the default state or territory, which has artificially inflated ACT figures. This default option was removed when the ACCC updated the SCAMwatch reporting form at the end of 2013.

A breakdown of scam categories by state and territory is provided at appendix 1.

Table 5: Scam contacts' location by state and territory 2013

State	Percentage of scam contacts who were based in Australia	Percentage of reported loss who were based in Australia	Percentage of the Australian Population*
New South Wales	31.5%	29.3%	32.0%
Victoria	22.1%	27.2%	24.8%
Queensland	20.3%	19.8%	20.1%
Western Australia	9.2%	9.7%	10.9%
South Australia	8.0%	6.2%	7.2%
Australian Capital Territory**	5.6%	5.8%	1.6%
Tasmania	2.4%	1.3%	2.2%
Northern Territory	0.8%	0.6%	1.0%

* Australian Bureau of Statistics' 3101.0—Australian demographic statistics, SEP 2013, released March 2014.

** Scam contact report levels for the Australian Capital Territory were artificially inflated in 2013 due to it being the default state or territory listed in the SCAMwatch online reporting form.

Future insights—new scam demographics

In 2013 the ACCC reviewed its collection of scams data and made several improvements to the way in which information will be gathered, including demographics data. Previously the ACCC had a narrower field of demographic data collection covering age and location.

As of January 2014 individuals reporting scams activity to the ACCC will have the option to self-identify their gender, whether they are a small business, or may be from a disadvantaged or vulnerable background.

This additional data will enable the ACCC to better understand where scams are being targeted, or if particular community groups display vulnerabilities that increase their susceptibility to scams.

A snapshot of what the ACCC has identified on scams demographics for the first quarter of 2014 is included below.

Spotlight on 2014 scams data by age (January–March)

- Women were more likely than men to report scams, with 53 per cent of contacts where the individual provided their gender identifying as female.
- While women were marginally more likely to report a loss, men lost more money overall, with men reporting nearly $9 million in losses compared to under $7 million for women.
- Men aged 25–34 were most likely to lose money to a scam, representing nearly 12 per cent of contacts where money was lost to a scam. However, men and women aged 45–54 reported the highest financial losses to scams, with men accounting for 19 per cent and women 15 per cent of total money lost.
- Dating and romance scams were most likely to result in financial harm to men and women in the 55–64 age bracket, with 39 per cent of women and 23 per cent of men who fell victim to this type of scam suffering a loss.

Spotlight on 2014 scam reports by different social groups (January–March)

- 1442 people reported a small business scam to the ACCC. The most common scam reported by businesses was false billing.
- 144 people who identified as Indigenous reported a scam to the ACCC.
- 418 people who identified as being from a non-English speaking background reported a scam to the ACCC.

2.5 Conversion rates

The overall scam conversion rate remained relatively stable, with a slight increase from around 13 per cent in 2012 to nearly 14 per cent in 2013.

The relatively low percentage of people reporting a financial loss suggests that the public is generally alert to scams activity and how they can protect themselves. It may also reflect the success of the concerted efforts of the ACCC and many other agencies to raise community awareness so that Australians are better able to identify scams and avoid victimisation.

While it is positive that the conversion rate remains relatively low, there are several factors that make it difficult to grasp a complete picture of the scale and scope of scams activity in Australia.

Scams activity will always be under-reported as recipients may not recognise a scam when they receive it, may not report it where a loss did not arise, or may be too embarrassed to report their experience.

Additionally, there are many other government agencies that play an important role in dealing with scams activity, and to whom consumers can report a scam and seek help. The upcoming Australian Cybercrime Online Reporting Network (ACORN), which will be launched in 2014, will help to create a fuller picture of the extent of scams that occur online—see section 7.4 for more information.

Some scam categories achieve very high conversion rates and may highlight a particular susceptibility of victims to these types of scams. A high conversion rate is therefore one of the factors that the ACCC considers when deciding where to direct its resources. This is why in 2014 the ACCC will be focusing efforts on relationship scams—see highlight box on page 17.

Figure 6 compares conversion rates by scam categories in 2012 and 2013, with marked increases for health and medical, online shopping, and psychic and clairvoyant scams. The conversion rates for computer prediction software and false billing scams saw sizeable decreases. Mobile phone, advance fee fraud and computer hacking scams remained relatively stable.

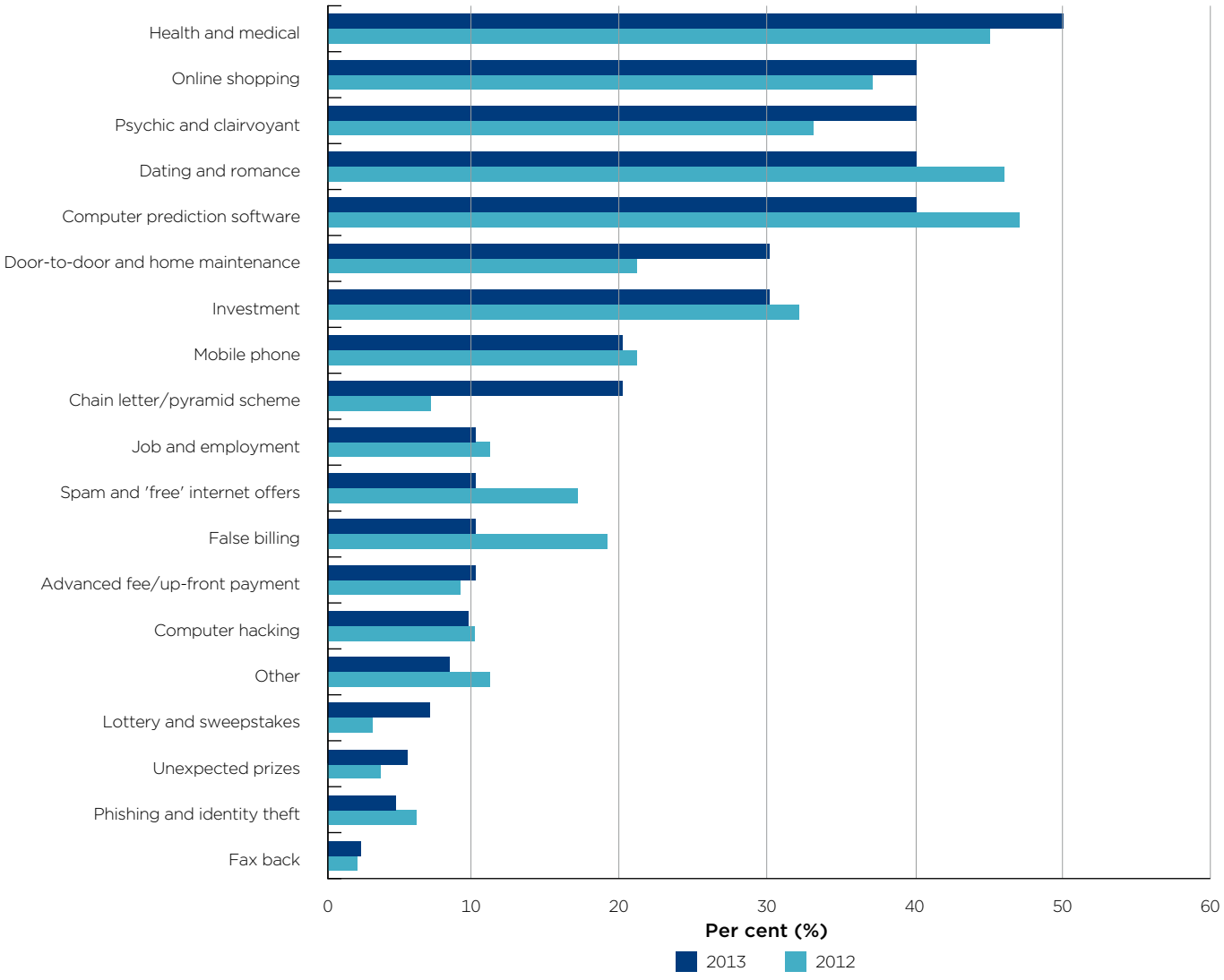
Measuring the impact of a scam

Conversion rates show the percentage of people that report a loss resulting from a scam, as opposed to those that recognise a scam and simply report it.

The conversion rate is a useful tool in understanding which scams are more likely to result in consumer harm. Essentially, the conversion rate indicates the 'success rate' of a scam type by revealing how likely it is that an individual who receives and responds to a particular scam will go on to lose money.

Conversely, the lower the conversion rate, the greater the likelihood that more people are successful at recognising a scam and avoiding victimisation.

Figure 6: Conversion rates by scam category 2012–13



Spotlight on relationship scams

Scammers have recognised that a personalised approach can pay dividends, with relationship scams often yielding a high financial return. The fact that high conversion rates are observed in scam categories predicated on a deceptive relationship is a testament to the effectiveness of this technique.

Relationship scams are acts of fraud that are premised on a scammer building a deceptive connection with an individual or business in order to secure their personal details or money. They refer to any scam type where the scammer invests time and effort into convincing the victim that a relationship exists and then manipulates them to secure a personal gain.

Dating and romance scams are the most destructive form of a relationship scam. In 2013 dating and romance scams netted the highest overall financial losses for any scam type, with over $25 million reported lost. While the conversion rate for this type of scam has slowly declined in recent years, it continues to be comparatively higher than other scam categories—in 2013 almost 43 per cent of those who reported an approach by an online admirer went on to lose money. These scams also cause significant emotional harm, with many victims reporting a break down in relationships with friends and family as well as financial ruin.

A sound investment for scammers

Scammers have recognised that relationships can prove to be a highly profitable investment, and therefore are prepared to invest a considerable amount of time engaging with victims to develop a deep connection.

While some people report scammers making their first request for financial assistance within just a few weeks of connecting with them, other reports show that scammers will wait months before requesting money.

Once the first request and money transfer is made, scammers will continue to make further requests for the lifespan of the relationship.

Just like a professional investor, when the scammer realises that there is little return to be had on their investment—for instance a target turns out to have little money, or a victim's financial resources are drying up—they will move on to other scam relationships.

It is of no consequence to scammers that victims make a significant emotional investment as they become more and more entangled in what they believe to be a genuine relationship. Scammers are adept at emotional manipulation, which causes victims to ignore doubts and is a key reason for the high success rate for scammers in obtaining large amounts of money.

How does a relationship scam work?

While relationship scams are by nature a personalised experience, there are a range of elements that underpin them.

- **Personalised approach**: scammers are prepared to do their research on who a person or business is in order to maximise their likelihood of success. Social engineering is a practice employed by sophisticated scammers, whereby personal information about the target is collected and then used against them to elicit a response. Scammers may obtain this information online through social networking forums.
- **Emotional manipulation**: scammers are experts at playing on people's emotions to slip under their radar. Scammers will appeal to people's charitable side, make an urgent plea for help, or claim to be in love. These approaches are designed to create a sense of guilt, anxiety and personal attachment that will push targets to fall for the scheme.
- **Removal of 'red flags'**: phone and online are the preferred method of scams delivery today. Scammers take advantage of these indirect communication channels to connect with victims in a way that disables the normal cues that people rely on for crosschecking information. Scammers use a range of excuses to avoid chats online or face-to-face meetings, which prevents targets from testing the background and story of their admirer.

Repeat victimisation

Relationship scams can also result in repeat victimisation, whereby the victim unwittingly falls for the scammer over and over again. In order to continue to extract funds from the victim, the scammer may morph one scam type into another, such as approaching a victim who has fallen for them as part of a dating and romance scam with an investment scam or advance fee fraud.

Scams intervention work carried out by law enforcement agencies in Queensland and Western Australia has also highlighted that victims who realise they have been duped and cease contact with the scammer will often then be targeted by a secondary scam. This may include the scammer declaring their love anew, offering to return their money, or even pretending to be an official who is contacting them about the original fraud.

Past and upcoming work to disrupt relationship scams

In recent years the ACCC has prioritised efforts aimed at minimising harm arising out of dating and romance scams, and has observed a continuing decline in the conversion rate—from 48 per cent in 2011 to 46 per cent in 2012 to 43 per cent in 2013. In 2014 the ACCC will build upon its previous efforts by launching a national disruption project aimed at relationship scams more broadly.

For a detailed overview of this project, and the important work already underway by other agencies to disrupt relationship scams, see section 6.1.

3. The top 10: 2013's most reported scams

3.1 Overview of most common scam types reported to the ACCC

In 2013 the ACCC continued receiving contacts about a broad range of scams targeting Australians.

Table 6 provides an overview of all scam types reported to the ACCC in 2013 in order of number of contacts per category.

A list of scam categories by state and territory is provided at appendix 1.

Table 6: Overview of scam types reported to the ACCC in 2013 in order of contact levels

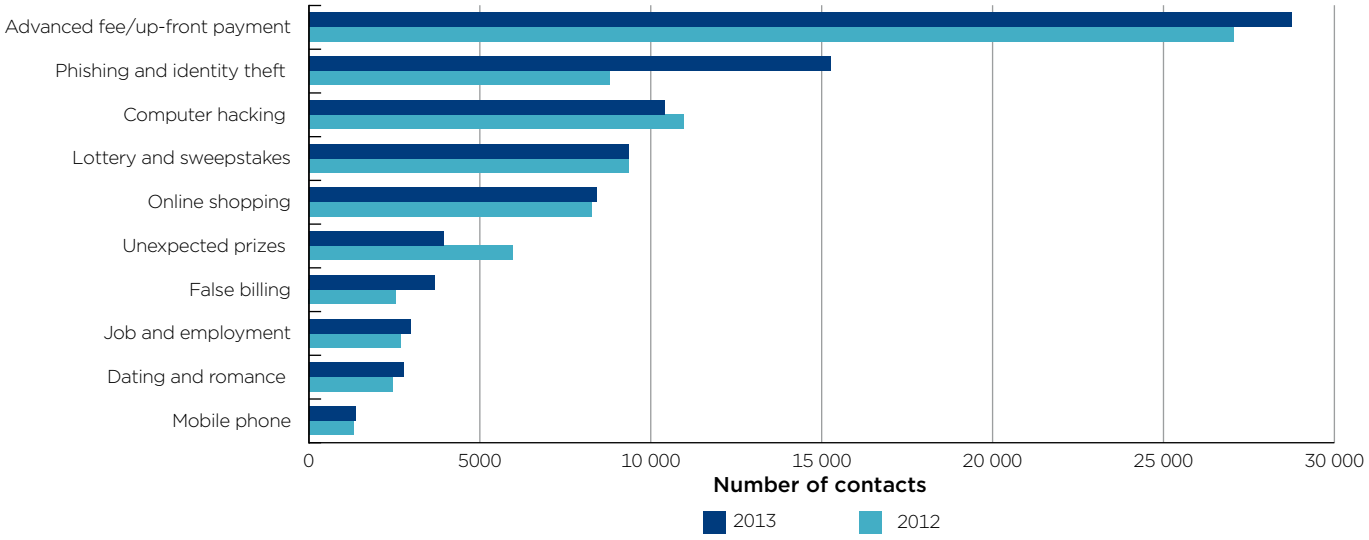
Scam category	Contacts	Amount reported lost	Contacts reporting loss	Less than $10k lost	Greater than $10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	28 748	$24 988 234	2 941	2 578	363	25 807	10.2%
Phishing and identity theft	15 264	$2 467 287	665	612	53	14 599	4.4%
Computer hacking	10 415	$1 130 947	935	917	18	9 480	9.0%
Lottery and sweepstakes	9 354	$5 065 359	581	488	93	8 773	6.2%
Online shopping	8 402	$5 046 729	3 766	3 678	88	4 636	44.8%
Unexpected prizes	3 933	$995 288	190	169	21	3 743	4.8%
False billing	3 672	$724 772	445	431	14	3 227	12.1%
Job and employment	2 979	$3 206 486	401	354	47	2 578	13.5%
Dating and romance	2 777	$25 247 418	1 189	791	398	1 588	42.8%
Mobile phone	1 351	$51 775	269	268	1	1 082	19.9%
Spam and 'free' internet offers	1 046	$60 705	140	140	0	906	13.4%
Computer prediction software	1 037	$9 144 288	392	284	108	645	37.8%
Investment	829	$9 083 512	235	146	89	594	28.3%
Health and medical	558	$114 127	304	302	2	254	54.5%
Other—scams outside predefined categories	519	$732 262	40	33	7	479	7.7%
Chain letter/pyramid scheme	393	$248 757	60	56	4	333	15.3%
Door-to-door and home maintenance	345	$322 212	118	113	5	227	34.2%
Fax back	173	$24 071	3	2	1	170	1.7%
Psychic and clairvoyant	132	$482 746	58	52	6	74	43.9%
Total	**91 927**	**$89 136 975**	**12 732**	**11 414**	**1 318**	**79 195**	**13.9%**

3.2 The top 10 scams in 2013

In 2013 the top 10 scams reported to the ACCC in terms of contact levels remained the same with some minor movements in ranking. Advance fee/up-front payment scams remained the most reported scam type, however phishing and identity theft moved from fourth to the second most reported scam category. Computer hacking scams remained in the top three scams, having been the second most reported scam in 2012.

Figure 7 provides a comparison of the top 10 scams from 2012 to 2013. Contact levels stabilised or increased slightly across all scam categories with the exception of phishing and identity theft, which saw a sizeable increase, and unexpected prizes, which showed a substantial decrease.

Figure 7: Comparison of the top 10 scam report levels 2012—2013



#1. Advanced fee/up-front payment scams

Number of scam reports:
28 748

Per cent of total scams reported:
31 per cent

Number of consumers reporting losses:
2941

Total losses reported by consumers:
$24 988 234

Scam conversion rate:
10 per cent

For the fifth consecutive year, advanced fee/up-front payment scams was the most commonly reported scam type, constituting 31 per cent of all scam contacts. The ACCC received almost twice as many reports of this scam type than it did for any other scam category.

In 2013 the ACCC received 28 748 reports of advanced fee fraud, increasing by 6 per cent from 2012 levels. Financial losses saw a marked decrease of over 17 per cent, yet the overall figure remained high with $24 988 234 reported lost.

The number of people who reported receiving an advance fee fraud scam and then went on to lose money rose only marginally from nearly 9 per cent in 2012 to just over 10 per cent in 2013. While this overall conversion rate suggests that most people are able to identify an up-front payment scam when they receive it, the sheer scale of this type of fraud still results in significant losses to victims and the Australian economy.

The advanced fee/up-front payment scams category is broad and crosses over a range of scams, with the basic premise being an approach by a scammer with an offer to receive a sum of money or goods in exchange for money provided in advance. Recipients are usually directed to make the up-front payment via money or wire transfer. In the end, the promise is never delivered upon, with any money handed over almost impossible to recover.

These scams range from outlandish offers to extremely sophisticated schemes that involve a gradual entrapment of victims over many months or years.

Some examples include: reclaim scams; inheritance scams; native language scams; promises of goods or profits from commodities such as gold, gemstones and oil; rental scams; and fake accommodation vouchers.

The reclaim scam is one of the most common cases of advance fee fraud reported to the ACCC, whereby consumers receive a call out of the blue from a 'government representative' claiming that they are entitled to money for some reason or another.

'Refund', 'entitlement', 'reclaim', 'rebate' and 'overpaid taxes'—all of these are trigger words that an up-front payment scam is in play.

PROTECT YOURSELF TIPS

1. If someone asks you to pay money up-front in order to receive money, walk away—it's a scam.
2. Don't get taken in by a plausible sounding explanation as to why you are entitled to money—scammers are highly skilled story-tellers.
3. If someone instructs you to send money via wire or money transfer, stop—it's nearly impossible to recover money sent this way.

Victim's story:
Grace's 'government refund' ends up costing her money

Grace* received a phone call from Bill who told her that he was from a law firm working for the Australian Government.

Bill said he had discovered that Grace had been overcharged for her energy usage for a number of years and was entitled to a refund of $8000 from the government. Bill told Grace that in order to receive the refund, she would need to pay $1000 in administrative fees before the money could be released.

Bill instructed Grace to pay the $1000 via money transfer in order to 'expedite the payment process'.

The next day, Grace received a phone call from Sarah, Bill's personal assistant, who informed her that the payment had been received and the application for a refund was now lodged.

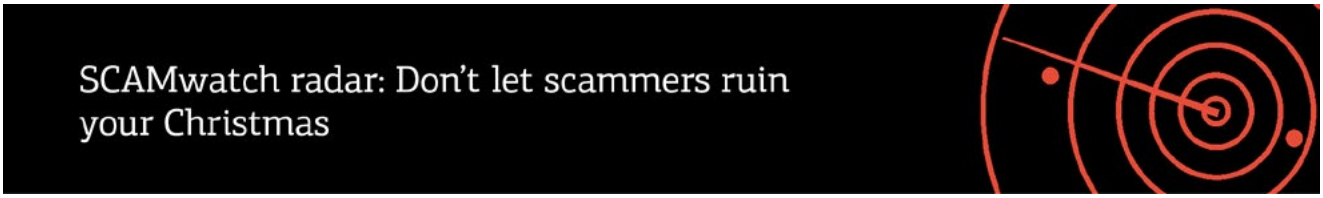
Sarah then informed Grace that in order to process the refund, she would have to pay an additional fee of $100 and provide her credit cards to set up an electronic transfer.

A week later, Grace still had not received her refund, and noticed several unauthorised charges to her credit card. When Grace contacted her local government, she found out that she'd been scammed.

"Scammers often take advantage of people's trust in government authorities by claiming to be a government representative. If you get a call out of the blue, ask yourself who you are really dealing with."

ACCC Deputy Chair Delia Rickard

** All names have been changed and accounts fictionalised for illustrative purposes.*



Scammers take advantage of busy times of the year to target Australians.

In December 2013 the ACCC issued a SCAMwatch radar warning Australians to watch out for fake delivery scams arriving in their inbox or letter box.

Scammers jump on the mail rush at Christmas time by posing as postal and courier service providers who, for an up-front fee, will redeliver a parcel that doesn't exist.

The ACCC urged the public not to be fooled by an email or phone call out the blue requesting a fee for a parcel to be re-delivered. A tell-tale sign of a bogus delivery is if the scammer asks for the up-front fee to be paid by international wire transfer—it's rare to recover money sent this way.

Read more at www.scamwatch.gov.au.

#2. Phishing and identity theft scams

Number of scam reports:
15 264

Per cent of total scams reported:
17 per cent

Number of consumers reporting losses:
665

Total losses reported by consumers:
$2 467 287

Scam conversion rate:
4 per cent

In 2013 the ACCC received a significant increase in the number of reports and associated financial losses for phishing and identity theft scams. Phishing and identity theft climbed from fourth to the second most reported scam, representing approximately 17 per cent of all contacts.

The ACCC received 15 264 reports of this scam type, an increase of nearly 74 per cent compared to 2012. While overall financial losses remained relatively low compared to other categories, with a total of $2 467 287 reported, this nonetheless represented an increase of just over 64 per cent. The number of contacts reporting a financial loss was also up by almost 35 per cent.

Despite these increases, the number of people who reported receiving a phishing and identity theft scam and then went on to lose money remained low, with a slight decline from 6 per cent in 2012 to just over 4 per cent in 2013. This supports the ACCC's observation that phishing scams are primarily 'fishing' for personal information rather than instant monetary gain. This information can be used to carry out other fraudulent acts, including to commit identity theft or bank account and credit card fraud.

Phishing and identity theft scams typically involve people receiving a message that claims to be from a legitimate and well-known government, corporate or financial entity. The scammer claims that the person needs to provide their personal information for a range of reasons, such as to update or verify their account details, or to win a prize. They are usually after usernames, unique user numbers and passwords. If this information is provided, the scammer will exploit it for personal gain.

Scammers continue to favour email to deliver phishing scams, however SMS has also become a popular method.

Phishing scams are so common that it is likely the majority of recipients do not report it and simply put it down as a 'nuisance' act.

The rise in phishing and identity theft reports and financial losses reported to the ACCC in 2013 shows that it continues to be a winner for scammers.

Scammers do not expect a high success rate when they 'fish' for victims. Rather, they rely on the sheer volume of activity to produce results, with phishing scams issued in bulk via spam emails or SMS.

PROTECT YOURSELF TIPS

1. If you receive an email out of the blue from someone asking you to confirm, verify or update personal information, don't respond—just press 'delete'.
2. If you are unsure whether an email is legitimate, contact them directly to verify. Don't rely on contact details provided in the email—find them through an independent source such as a phone book or online search.
3. Never click on links or open attachments in an email from an unverified sender—they may contain malicious software.

Scam survivor's story:
David nearly takes the bait on a sophisticated phishing scam

David received an email from what appeared to be his bank asking him to confirm a few details to enable his expired online banking password to be reset.

Worried that he would not be able to access his bank account for an important transaction he needed to make, David quickly clicked on the link provided in the email. This took him to a website that had all the logos and branding associated with his bank.

David was about to begin filling in his details including his address, mobile number, online banking customer account number and old password when he became suspicious. He wondered why he had only been contacted after his password had already expired. On closer inspection, David also realised that the website's URL address was slightly different to the one he normally used when banking online.

David shut down the web page and called his bank to find out what was going on. He was told that his online banking password had not expired and that the bank would not ask him to confirm his details by clicking through a link in an email. David had received a phishing scam.

"Phishing scams often create a sense of urgency to get you to click through and provide personal information without thinking—don't let scammers press your buttons."

ACCC Deputy Chair Delia Rickard

SCAMwatch radar: Beware of scam surveys and fake free offers

In September 2013 the ACCC issued a SCAMwatch radar reminding people to beware of online scams—surveys, emails and social-media posts—offering fake gift vouchers or other bogus inducements in return for disclosing credit card and other personal information.

While many online surveys are legitimate and may be backed by some reward, the ACCC and Woolworths received a number of complaints about scams misusing the Woolworths name and logo, going under such titles as 'Get a free $50 Woolworths voucher' or 'Customer Satisfaction Survey'.

Scams such as these often ask people to provide credit card or other personal details, which criminals can use to commit identity theft and other fraud.

The ACCC urged people to verify whether offers are legitimate, even those passed on from family or friends. If the offers are represented as coming directly from a particular retailer, check they are listed on the retailers' official websites—or call a business' official customer-service line. Don't click on links or call numbers listed in the offers—they can link to fake websites and even fake call centres.

Read more at www.scamwatch.gov.au.

#3. Computer hacking scams

Number of scam reports:
10 415

Per cent of total scams reported:
11 per cent

Number of consumers reporting losses:
935

Total losses reported by consumers:
$1 130 947

Scam conversion rate:
9 per cent

In 2013 reports of computer hacking to the ACCC declined in terms of both contact levels and losses. This scam type represented just over 11 per cent of all reports.

The ACCC received 10 415 reports for this scam category, decreasing by around 5 per cent from 2012 levels. Reported losses fell by an even greater margin of almost 14 per cent to $1 130 947.

This downwards trend is a significant reversal from 2012, where the reported losses were more than double those of 2011. This decline is likely attributable to increased community awareness about the most common computer hacking scam in play, the cold calling computer virus scam. The sheer level of calls made—with some reporting receiving several calls in one day—may mean that people are more immune to this scam approach. Significant media coverage about these nuisance calls has also helped to raise its profile and thereby help the public to identify a scam call.

The computer virus scam starts with a call out of the blue from someone claiming to represent a legitimate and well-known organisation. The caller claims that the person's computer is infected and needs to be fixed immediately. The caller states that they can fix it on the spot—if the person gives remote access and pays a fee.

In another twist scammers may claim a fault with the person's internet service, with disconnection imminent if they do not pay or give access.

Whatever the story, victims not only lose their money but also compromise any personal information stored on the computer.

Other acts of computer hacking include social network and email account hacking. Scammers send phishing emails where they 'fish' for passwords, such as directing them to follow a link to a mirror copy of a social networking site or login page. Scammers then go on to commit identity theft, posing as the owner to gain money or personal details from friends, family, followers or contacts.

In 2012 a coordinated international law enforcement effort saw some of the perpetrators behind the cold calling computer virus scam caught. Unfortunately ongoing reports received in 2013 highlight the challenges authorities face in trying to stop a scam through litigation. If a particular ruse proves successful, then where one scam cell is shut down, other scammers are bound to step in. Scammers are also quick to change the story behind a scam when the community catches on.

In the end, the best defence is to not respond—if a call comes out of the blue, just hang up.

PROTECT YOURSELF TIPS

1. Be careful what you store on your computer—if a scammer gains access, they can steal your personal identity and money.
2. Keep your computer secure—always update your firewall, anti-virus and anti-spyware software, and only buy from a verified source.
3. If you think your computer has been compromised, run a virus check. If you still have doubts, contact your anti-virus software provider or a computer specialist.

Victim's story:
Richard downloads spyware to 'fix' fake fault

Richard received a phone call out of the blue from Mel who told him she was from Telstra Support. Mel said that Richard's computer was sending error messages to Telstra that there was a problem with his internet connection.

Richard was thrilled—his computer had been a bit slow lately but he thought it had just passed its expiry date. Now he would be able to sort out the issue.

Mel gave Richard instructions to give her remote access to his computer so that she could run a scan to check exactly what the problem was.

Richard was a little apprehensive to allow Mel access to his computer, but he followed her instructions after she explained that this would allow her to fix the problem faster.

After running the scan, Mel said that she had found what the problem was and that if Richard paid her a fee of $100 she would fix the problem straight away. She also said that if nothing was done, Richard's internet would disconnect in the next couple of hours. Richard was thankful that the problem had been identified just in time and provided Mel with his credit card details.

That night Richard told a friend about the phone call that saved him from losing his internet connection. However, to his surprise and horror, David's friend told him that he had probably been scammed—apparently lots of people had received this call.

Devastated, Richard called Telstra to ask whether they had contacted him. Telstra told him that they had not and confirmed that he had received a scam call.

Richard then contacted his bank to let them know what had happened and asked them to take steps to ensure the scammer could not access his bank account or use his credit card details. He also called a computer technician to take a look at this computer and to make sure that the security was up to date.

"Computer hackers will try anything to gain access to your computer as it's a treasure trove of information. Never give anyone who contacts you out of the blue access to your computer."

ACCC Deputy Chair Delia Rickard

SCAMwatch radar: Police scareware scam continues to target Australians

In March 2013 the ACCC issued a SCAMwatch radar warning Australians to remain alert to scammers posing as the Australian Federal Police (AFP) trying to scare people into handing over money to regain control of their computer.

A SCAMwatch alert on this scam was previously issued in October 2012, yet reports continued to be received in 2013.

In this scam, internet users found their computer had been frozen, with a pop-up alert claiming to be from the AFP appearing on their screen. The alert stated that the user's computer had been locked because they had visited an illegal website or breached various laws. The scammer claimed that the computer would be unlocked if a fee was paid.

The ACCC warned that even if money was handed over, the computer may remain locked. Further, once access was regained, malware may continue to operate, allowing the scammers access to personal details stored within.

Read more at www.scamwatch.gov.au.

#4. Lottery and sweepstake scams

Number of scam reports:
9354

Per cent of total scams reported:
10 per cent

Number of consumers reporting losses:
581

Total losses reported by consumers:
$5 065 359

Scam conversion rate:
6 per cent

In 2013 scammers appeared to be the winners, with reported financial losses from lottery and sweepstake scams almost doubling. Lottery and sweepstake scams slipped from third to the fourth most reported scam type, however, reports remained high representing just over 10 per cent of all scam contacts.

The ACCC received 9354 reports for this scam type, increasing by a marginal 2 per cent from 2012 levels. At the same time reported losses increased substantially by over 93 per cent to $5 065 359. The conversion rate, that is the success rate of a scammer in securing a financial gain from its targets, increased from 3 per cent in 2012 to 6 per cent in 2013.

The significant increase in financial losses associated with these scams is in part attributable to an increase in reported losses above $100 000. In 2013 the ACCC received 13 reports where losses reached this threshold, compared to only eight reports in 2012.

As per the previous year, in 2013 scammers continued to favour SMS to deliver lottery and sweepstake scams. Traditionally these scams were delivered to the door, with slick 'promotional' material used to make the scam appear genuine. In 2013 less than 10 per cent of these scams were delivered by post.

Lottery and sweepstake scams try to trick people into giving personal details or money up-front in order to receive a prize from a lottery, sweepstake or competition that the person never entered.

The scammers typically claim to be affiliated with a genuine overseas lottery entity or company, with 'winnings' offered in foreign currencies such as British pounds or American dollars. To claim their money, the recipient is asked to provide personal details and/or an up-front payment, typically via money or wire transfer. Victims are not able to use their 'winnings' to pay these fees.

If the person hands over their money, they will never see it again, nor the promised windfall. Any personal detail provided may also be exploited.

Scammers move with the times, using new communication channels to deliver old scams. It is unsurprising that scammers have shifted from traditional postal services to SMS given how cost effective this electronic medium is as a means of sending scams en masse while evading detection.

PROTECT YOURSELF TIPS

1. Remember: you cannot win a lottery or competition unless you entered it.
2. Ask yourself who you're really dealing with—scammers pose as legitimate organisations to make them appear to be the real deal.
3. If someone asks you to pay money up-front in order to receive money, walk away—it's a scam.

Victim's story:
Kim 'wins' a (mis)fortune

Kim received a text message from the European Lottery Commission informing her that she had won 14 million Euros, the first prize in the most recent draw of the European lottery. Kim couldn't believe her luck—she had never won anything before!

Kim emailed the commission using the address provided in the text message. Almost immediately she received a response from the chairman of the commission congratulating her on her win. The chairman explained that the funds were ready to go, but under European Union law, they could only be released after Kim made a commission payment to the European Lottery Fund. The chairman explained that the payment was a mere AU$5000 when compared to the windfall that awaited her.

Kim was instructed to make the payment to a European bank account. The chairman advised that once the $5000 was received, the 14 million Euros would be deposited into her account within 24 hours.

Kim was so excited that she immediately drove to her bank and arranged an electronic transfer.

The following day Kim checked her bank account but found that no money had been deposited. She returned home and emailed the chairman, but he did not respond. Kim repeatedly checked her bank and email accounts throughout the week, but nothing further eventuated.

It dawned on Kim that she had been scammed. On reflection, Kim realised that it was odd for her to have 'won' a lottery that she hadn't entered.

"Don't let scammers win the ultimate lottery by gaining your personal details and money—if something seems too good to be true, it probably is."

ACCC Deputy Chair Delia Rickard

Everyone is vulnerable at some stage to a scam

Many people may look at a lottery and sweepstake scam and wonder, 'how could someone fall for this?'

The ACCC has observed that there exists a social stigma attached to falling for a scam. This perception can have a significant impact on victims, who may be too embarrassed to tell others about their experience for fear of being judged.

It is important to understand that there are a number of reasons why people fall victim to a scam, and that everyone is vulnerable at some point in life to a scam approach.

Some vulnerability factors include:

- Financial troubles—when people are experiencing financial difficulties, they may be more likely to ignore cues that an offer is a scam.
- Gambling or risk-taking personality—some personality types are more likely to accept an offer and see where it will take them, before realising that it is a scam.
- Charitable nature—some people are more predisposed to want to help those in need, which makes them vulnerable to the many scams that are masked as pleas for help.
- Personal circumstances—people are more likely to fall for a scam if the ruse personally relates to them, particularly where it elicits an emotional response. For example, someone who has lost a loved one to an illness may be more vulnerable to scammers making pleas for financial help to cover costs associated with a medical emergency.
- Time-poor—where a person or business is pressured in terms of available time, they may respond to a scam before realising what it is.
- Urgency—people may respond to a scam when it creates a sense of urgency around something important, such as disconnection of an essential service or limited 'stock'.

By raising the profile of scams, the ACCC hopes to remove this stigma so that victims will feel more confident in speaking out and seeking support.

#5. Online shopping scams

Number of scam reports:
8402

Per cent of total scams reported:
9 per cent

Number of consumers reporting losses:
3766

Total losses reported by consumers:
$5 046 729

Scam conversion rate:
45 per cent

In 2013 scammers continued to target Australians buying and selling in the online retail market. Online shopping scams remained the fifth most reported scam type, representing just over 9 per cent of scam contacts.

Reports of online shopping scams remained relatively stable, with a small increase of 1.5 per cent over 2012 levels to reach a total of 8402 contacts. At the same time, reported financial losses increased markedly by almost 25 per cent to a total of $5 046 729.

Scammers appeared to have more success in tricking people into handing over their money when shopping online, with the conversion rate rising from 37 per cent in 2012 to 45 per cent in 2013. This means that close to half of the people who reported receiving an online shopping scam in 2012 lost money to it. However, while overall losses increased, reports of significant losses remained steady.

Online shopping scams target both buyers and sellers, with the two most common types being:

1. **Classified ad scams**—a scammer posts a fake ad on a legitimate classifieds website for inexpensively priced common products. If a recipient shows interest in an item, the scammer will claim that the products will be delivered following receipt of payment. If the recipient pays, they will lose their money, not receive the products nor be able to contact the seller.
2. **Overpayment scams**—a scammer responds to a seller's ad with a generous offer and then 'accidentally' overpays. The scammer will request that the seller refund the excess amount by money transfer in the hope that the seller will transfer the money before they discover that the scammer's cheque has bounced or that the money order was phony. The seller will lose the money, as well as the item they were selling, if they have already sent it on to the scammer.

Scammers know to target popular consumer goods where there is high demand, low supply levels or high prices.

Common products that scammers use when 'buying' or 'selling' online include pets, used cars, boats and bikes, and electronic items such as smart phones, tablet devices and laptops.

For online shoppers, the tell-tale sign of a scam is a sought-after item at a price that seems too good to be true.

PROTECT YOURSELF TIPS

1. Don't trust the legitimacy of an ad just because it appears in a reputable newspaper or online classifieds website—scammers often use these.
2. If you are buying online, only ever pay via a secure payment method such as a credit card—look for a web address starting with 'https' and a closed padlock symbol.
3. If you are selling online, be very wary of any buyer who only wants to pay by cheque, money order or money transfer—they're more than likely a scammer.

Scams survivor's story:
Alex avoids being taken for a ride by a scammer

Alex, who lives in Melbourne, advertised his car for sale on a popular online classifieds site for $5000. The following day he received an email from Brian who said he was interested in buying the car. In fact, Brian was happy with the going price as the car was exactly what he was after.

Alex was ecstatic as he had only just advertised the car, and thought it would take a lot longer to find a buyer. He asked Brian when he would like to come inspect the car and take it for a test drive. To his surprise, Brian replied that he was not able to inspect the car as he was currently working as an engineer offshore from New Zealand. However, Brian was still keen to go ahead with the purchase as it was exactly what he was after, and he would arrange for the car to be shipped to him.

Brian asked for Alex's PayPal account details so that he could transfer the money. Brian also informed Alex that the shipping company he wanted to use to ship the car from Melbourne to New Zealand would only accept payment from the seller. Therefore, Brian would transfer $6000 to Alex via PayPal—$5000 for the car and $1000 to cover shipping costs—and Alex would then need to send $1000 to the shipping company via wire transfer.

Alex provided Brian with his PayPal account details, and Brian provided him with the details of where to transfer the money for the shipping costs.

The following day Alex received an email from what appeared to be PayPal saying that $6000 had been transferred into his account. The email had all the logos and branding associated with PayPal. Alex was just about to begin transferring $1000 to the shipping company when he was struck with the thought, 'Why would someone buy a car without inspecting it first?' He then checked his PayPal account and found that no money had actually been transferred into it. He also noticed that the email from PayPal had not come from the usual PayPal email address. He then called the shipping company and was told that the number had been disconnected.

Alex realised that he had almost fallen victim to a scam. He called PayPal and provided details of what had happened.

"If you are looking to sell something online, never accept money that is more than what you agreed upon for the item's price—it's a tell-tale sign that the 'buyer' is in fact a scammer."

ACCC Deputy Chair Dr Michael Schaper

SCAMwatch radar: Pause to avoid a puppy scam

In April 2013 the ACCC issued a SCAMwatch radar warning that scammers were continuing to use cute and cuddly canines to pull on people's heart strings and get them to part with their money.

This scam typically involves ads for non-existent puppies being placed in newspapers and online classifieds at extremely low prices. The 'seller' provides interested buyers with pictures of an adorable puppy and then tricks them into paying fees for transport, customs or medical costs before the dog can be delivered.

Scammers prey upon individuals and families who just want to give a dog a good home.

Once the payment is made, the puppy and money vanish without a trace.

Read more at www.scamwatch.gov.au.

#6. Unexpected prize scams

Number of scam reports:
3933

Per cent of total scams reported:
4 per cent

Number of consumers reporting losses:
190

Total losses reported by consumers:
$995 288

Scam conversion rate:
5 per cent

Despite retaining its place as the sixth most reported scam type, in 2013 reports of unexpected prize scams decreased by almost 34 per cent on 2012 levels. The ACCC received 3933 contacts about these scams, representing just over 4 per cent of all scam contacts.

Reported financial losses also fell slightly by nearly 6 per cent with total losses of $995 288. This decrease is due to less people suffering substantive losses; in 2013 only one person reported losing more than $100 000, compared to four people reporting losses above this threshold in 2012.

These scams typically involve consumers receiving a notification out of the blue that they have won a prize in a competition that they never entered. Common prizes include a holiday package or popular electronics item.

In order to claim the prize, the 'lucky winner' must first pay a fee up-front to cover various costs such as taxes or administration fees.

If the person hands over their money and personal details, they will never see their money again. The promised prize will also never arrive or, if it does, it will not be what the scammer claimed it would be. Finally, their personal details may be used by the scammer to commit other fraudulent acts.

Unexpected prize scams operate in a similar way to lottery and sweepstakes scams, however the scammer offers a good or service rather than money.

In additional to traditional postal services, these days scammers also use email and SMS to deliver these scams.

Australians seeking a holiday deal need to be wary of any unexpected prizes that come their way, with scammers using them to dress up dodgy holiday packages.

Scammers use fictitious prizes to trick people into signing up for holiday packages with undisclosed terms and conditions. These terms and conditions quickly eat away at any value that the 'prize' may have held.

PROTECT YOURSELF TIPS

1. Ask yourself: how can I win a prize if I never entered a competition for it?
2. Don't respond—if you receive a notification out of the blue about an unexpected prize, ignore it.
3. If someone asks you to pay money up-front in order to receive money or a prize, walk away—it's a scam.

Scams survivor's story:
Nick's bogus 'holiday prize' almost leaves him high and dry

Nick received an unexpected text message telling him that he had won a business class trip for two to Fiji compliments of Global Airways. Nick was excited as he had just been thinking that he needed a relaxing break away from his busy job, and Fiji sounded like just the ticket.

Nick replied to the message and shortly received a response from Global Airways congratulating him on his win. Global Airways instructed him to transfer $100 to cover international taxes and they would then arrange the trip.

Nick was no longer excited—instead, he sniffed a rat. Nick thought back and couldn't remember entering a competition for a holiday, so he texted the airline to ask how they got his details. Global Airways wrote back claiming that he had been randomly chosen by his phone number and that the competition had received government approval.

Nick researched Global Airways online and found that lots of people had written about receiving a scam text message from 'Global Airways'.

Nick deleted the message straight away and wondered how much he needed a holiday after all.

"Always exercise caution if an unexpected prize falls from the sky—remember, scammers will try anything to entice you to hand over your hard-earned money. If you are unsure whether an approach by someone claiming to represent an authority, business or organisation is legitimate, verify who they are by contacting them directly using independently sourced contact details."

ACCC Deputy Chair Delia Rickard

#7. False billing scams

Number of scam reports:
3672

Per cent of total scams reported:
4 per cent

Number of consumers reporting losses:
445

Total losses reported by consumers:
$724 772

Scam conversion rate:
12 per cent

In 2013 Australian small businesses continued to be targeted by scammers with reports of false billing, the most common scam targeting the sector, increasing markedly by 45 per cent. False billing scams represented around 4 per cent of scam contacts with 3 672 reports received.

Reported losses also increased by almost 28 per cent to $724 772.

On a positive note, the number of businesses who reported receiving a false billing scam and then lost money to it fell from 19 per cent in 2012 to 12 per cent in 2013. This suggests that while scammers continue to target small businesses, owners and their staff are becoming more savvy in identifying these scams and avoiding falling victim.

False billing scams attempt to trick businesses into paying for unwanted or unauthorised listings or advertisements in magazines, journals, business registers or directories. Services often used as a ploy include domain name registration and the provision of office supplies.

Common scam tactics are to send a business a subscription form disguised as an outstanding invoice to get the business to sign up for unwanted ongoing advertising services. Scammers also falsely claim that the directory or publication is well known or has a high readership.

Another common scam approach is sending invoices for the renewal of a business's current domain name registration, however the domain name will be slightly different such as '.com' instead of '.com.au'.

Scammers will do anything to get businesses to sign up to a scheme, including claiming a charitable connection.

In 2013 the ACCC took successful court action against the operators behind Adepto Publications, a scam targeting small businesses with false claims about advertising services for publications. This scheme involved claiming that ads would be placed in charitable publications including the National Emergency Relief Guide, Underprivileged Childrens Guide and Volunteer Organisations Guide.

The operators were ordered to pay $75 0000 in penalties—see section 6.2 for more information.

PROTECT YOURSELF TIPS

1. Make sure the business you are dealing with is the real deal—if you receive a form or tax invoice out of the blue, verify who they are by contacting the company directly using contact details you sourced independently through a phone book or online search.
2. Make yours a 'fraud-free' business—effective management procedures can go a long way towards preventing scams. Have a clearly defined process for verifying and paying accounts and invoices, and try to avoid giving too many staff authorisation to make orders or pay invoices.
3. Don't be intimidated—do not let anyone pressure you into making decisions involving payments or ongoing contracts. If you are unsure, always seek independent financial or legal advice.

Scam survivor's story: Jane isn't fooled by a fake domain

Jane, a small business owner, received a letter from what appeared to be her domain name registrar informing her that the domain name for her business would expire in a week and that if the enclosed invoice was not paid within the week, Jane's domain name would be sold to another party.

Jane was worried as her website was hugely important to the success of her business. She handed the invoice over to her office manager, Mary, and told her to pay it immediately.

Mary informed Jane that she had already paid the registration renewal just a few months ago and so it was strange that another payment needed to be made. Jane took a closer look at the invoice and realised that payment was being requested for a '.com' domain name, whereas her domain ended in '.com.au'. She also realised that there was a slight difference in the spelling of her domain name registrar and the name on the invoice.

Jane realised that she had almost paid a scammer and threw the invoice away. She contacted auDA to tell them what had happened.

"Before paying a bill, make sure you check that you are paying the right company for the right service."

ACCC Deputy Chair Dr Michael Schaper

In August 2013 the ACCC issued a SCAMwatch alert warning that the fake 'Yellow Pages' business directory scam was targeting Australian small businesses. This scam was similar to a scheme that the ACCC took successful court action against in 2011.

The ACCC had received a surge in reports from small businesses about a fax claiming to be from 'Yellow Page Australia' and 'Open Business Directory Ltd' that, on first glance, appeared to be seeking confirmation of their business' contact details. However, on closer inspection, the fax was in fact an agreement to sign up to an online business directory service charged at $99 per month for a minimum two-year period.

Businesses were tricked into thinking that the fax was affiliated with Sensis' Yellow Pages® directory by using this well-known Australian company's name and 'Walking Fingers' logo. However, Sensis warned that 'Yellow Page Australia', 'Online Business Directory' and the website 'www.yellow-page-australia.com' were in no way connected with Sensis or Telstra.

Read more at www.scamwatch.gov.au.

For more information on this scam and ACCC disruption activities, see section 6.1.

#8. Job and employment scams

Number of scam reports:
2979

Per cent of total scams reported:
3 per cent

Number of consumers reporting losses:
401

Total losses reported by consumers:
$3 206 486

Scam conversion rate:
14 per cent

In 2013 job and employment scams fell to the eighth most commonly reported scam to the ACCC (previously seventh), representing 3 per cent of total scam contacts. The ACCC received 2979 job and employment scam reports, an increase of just over 11 per cent from 2012.

Reported financial losses also rose by 19 per cent to a total of $3 206 486. The number of people who reported receiving this type of scam and losing money to it rose slightly from 11 per cent in 2012 to 14 per cent in 2013.

Job and employment scams typically involve offers to work from home or to set up and/or invest in a business. Scammers promise a large salary or a high investment return following initial up-front payments. Payments can be for training courses, uniforms, security clearances, taxes or fees.

This type of scam can also involve offers to assist migrants or international students with securing visas and jobs in Australia. Scammers take advantage of students who may not want to return to their home country when their visa is due to expire by 'guaranteeing' them a job for an exorbitant finder's fee paid up-front. Victims never get the promised employment, lose any money sent, and have their hopes destroyed of an extended visa.

Scammers know the basics of economics, taking advantage of situations where there is high demand and little supply—including in the job market. If the job market is tight, people searching for work or business opportunities need to be wary of scam employment offers.

Job and employment scams can be a front for money laundering.

These scam job offers may be advertised as easy money for working from home. If a person signs up, they will be instructed to open a bank account, through which money will be transferred. The person will then be paid a 'commission' for this 'work'.

The money being transferred is usually stolen, with scammers laundering money through an Australian bank account to avoid detection.

Money laundering is a criminal offence. Punishment may include either criminal penalties (such as fines or lengthy periods of imprisonment) or significant civil penalties (of up to $11 million).

The Australian Government is serious about tackling money laundering —individuals handling the proceeds of crime can be prosecuted.

PROTECT YOURSELF TIPS

1. Do your research before agreeing to any offer—ask around, search online and if it involves a significant investment, seek independent advice.
2. Beware of offers or schemes claiming to guarantee income or requiring payment up-front. Never agree to an offer over the phone—ask for it in writing.
3. Remember there are no get-rich-quick schemes: the only people who make money are the scammers.

Victim's story:
Ty's dreams and cash are dashed by scam agency

Ty was studying in Australia on a student visa and was looking to extend her stay before returning to the Philippines.

With only weeks to go until her visa expired, Ty came across an online job advertisement that sparked her interest. The ad was posted by a global recruitment agency and promised to find immigrants a job that would satisfy the requirements of obtaining a long term visa.

Ty could not believe her luck—the agency was promising exactly what she wanted! She emailed the agency to obtain further information. When they replied, Ty was disappointed to learn that she would need to pay a fee of $5000 in order for the agency to secure a job for her. She had saved up some money while studying, but a $5000 fee would almost empty her bank account. However, in the end she decided to go ahead and sign up to the agency as the only other alternative was to leave Australia.

When Ty emailed the agency to sign up to their services, they told her that all she had to do was send them the money, and they would have a job arranged for her within a matter of weeks.

Ty transferred the money immediately and waited for a call back from the agency. Two weeks later, Ty had not yet heard back so she emailed them again. The agency did not reply. Ty emailed them again several times to no avail.

Ty was devastated. She went online and researched the recruitment agency, and to her dismay found that a number of people had shared the same experience.

Ty realised she had fallen victim to a scam—the promised job never came, she would have to leave Australia soon, and she would never see her money again.

"If you are looking for a job, be alert to scammers—they're professionals at selling bogus employment 'opportunities' where only they will bring home the money."

ACCC Deputy Chair Delia Rickard

#9. Dating and romance scams

Number of scam reports:
2777

Per cent of total scams reported:
3 per cent

Number of consumers reporting losses:
1189

Total losses reported by consumers:
$25 247 418

Scam conversion rate:
43 per cent

While 2013 saw dating and romance scams move to number one position for associated financial losses, this scam type remained ninth in terms of contact levels.

The ACCC received 2777 reports of dating and romance scams in 2013, up 14 per cent. Reported losses totalled $25 247 418, up 8 per cent from 2012.

Over the past four years, the conversion rates for dating and romance scams has continued to decline. From a high of 52 per cent in 2010, the rate dropped to 48 per cent in 2011, 45 per cent in 2012 and 43 per cent in 2013. While it is encouraging that more people are recognising these scams and avoiding losing money, the conversion rate is still very high compared to other scam categories. This demonstrates the effectiveness of a scam that has at its basis the exploitation of a relationship that can be carried out over a long time—in some instances years.

In these scams, which are often run by experienced criminal networks, the scammer develops a strong rapport with the victim before asking for money to help cover costs associated with illness, injury, a family crisis, travelling to see them, or to pursue a business or investment opportunity. Scammers exploit their victim's emotions to extract money.

Scammers often approach their victims on legitimate dating websites before quickly attempting to move the victim away from the security of the site, communicating through other methods such as email.

Scammers are also targeting victims through social networking sites, where they 'like' them and then express shared interests based on personal information gleaned from their profile. Clearly, scammers will adapt their approach and follow individuals onto any communication platform—in short, scammers will take advantage of any way to connect with people.

In 2013 the average reported loss from a dating and romance scam was over $21 000, with around one third of victims reporting losses over $10 000. In comparison, all other scams in the top 10 list had average losses below $10 000, with four scam types below $2000.

With such a high return, it is not surprising that scammers are prepared to invest the time and energy into building a romantic connection.

PROTECT YOURSELF TIPS

1. Do a 'Google Image' search of your admirer to help tell if they really are who they say they are.
2. Be alert to things like spelling and grammar mistakes, inconsistencies in their stories and other signs that it's a scam like their camera never working if you want to Skype each other.
3. Think twice: never send money to someone you've met online, especially via money order, wire transfer or international funds transfer—it's almost impossible to recover money sent this way.

The ACCC has announced the disruption of relationship scams as a 2014 priority area. Find out more about these scams at section 2.5, and what the ACCC will do to disrupt them at section 6.1.

Victim's story:
Meg's online admirer leaves her broke and with a broken heart

Meg decided to try online dating as she had recently gone through a divorce and her children had left home. She joined an online dating site, and not long afterwards she came across 'Sam'. Meg was attracted to Sam as he appeared to be physically fit, had a successful career as a Colonel in the US Army, and was also in a similar personal situation to her—single and lonely after his grown up children had left home.

Meg and Sam started communicating via the dating site and they seemed to 'click'—Sam really seemed to understand her and what she had gone through recently. Not long afterwards, Sam suggested that they start communicating by email as this would be more private.

Over the next few months, Meg and Sam emailed each other every day and talked about everything—their families, past relationships, and where their relationship was heading. One day, Sam professed his love for Meg and that he wanted to build a future with her. Even though she hadn't met him in person as he was currently deployed, Meg felt like he was 'the one'.

Meg often tried to get Sam to communicate 'face-to-face' via Skype. However, for some reason they could never quite pull it off—there was something wrong with the computer or webcam, there was an issue with the internet connection, or at the last minute he had to go to a field emergency. Sam promised her that they would meet each other as soon as his deployment ended.

Then Meg received an alarming email from Sam—his 19 year old daughter had just been rushed to hospital, where she had been diagnosed with an aggressive cancer and required immediate chemotherapy. Sam explained that his daughter did not have health insurance and that he did not have enough money to pay for this expensive therapy. Sam was hysterical—if he didn't find the money, his daughter would die.

Meg replied straight away and said that she would help cover the costs. In her mind, it did not matter how much it cost—family came first. Meg had previously told Sam how she had lost her daughter to cancer six years ago, so she knew what he was going through.

Sam was very grateful and asked her to send $20 000 via Western Union, and Sam's daughter began a round of chemotherapy. Unfortunately it was not enough and the following month, Meg sent another $8000 for follow-up treatment. Meg then started sending $1000 each month to pay for expensive medication to keep the cancer at bay.

After six months, Sam sadly told Meg that the cancer was back. However, Sam was not sad for long as he told her that the doctors had told him about a new miracle medicine that they guaranteed would cure his daughter—if he could find $150 000 to pay for it.

Meg was concerned that Sam was getting his hopes up. From her own experience with her daughter's cancer, she knew that there was no such thing as a medical miracle. Meg asked Sam to get more details from the doctors, but for some reason he didn't provide them to her. She pressed him a few more times, and he then asked her if she was doubting him. It was only then that Meg did step back and think about what Sam had told her.

It dawned on Meg how everything she knew about Sam was based on what he said rather than anything in the real world. Meg's heart sunk as she realised that the only thing concrete in their relationship had been the transaction of money. Meg realised that she had been scammed.

"If you are looking for love online, you need to take extra precautions to protect yourself. Don't let a scammer break your heart and leave you broke—cease contact with an online admirer if they ask you for financial help, no matter how genuine they sound."

ACCC Deputy Chair Delia Rickard

SCAMwatch radar: Don't let your heart be blackmailed

In July 2013 the ACCC issued a SCAMwatch radar warning those looking for love online to stay on the lookout for scammers.

Reports to the ACCC showed that scammers continued to target the lonely hearted online, using fake profiles on legitimate dating websites and online forums to form a relationship with an unsuspecting victim. Once trust was gained, the scammer would quickly attempt to move the victim away from the site and its security to communicate and manipulate them into handing over money.

In a new twist, the ACCC warned that scammers were blackmailing victims by threatening to send potentially compromising photos or videos to their family and friends if money was not transferred immediately. Scammers would capture photos or videos from webcam chats with the victim and then threaten to post them on public sites. If the scammer had access to their victim's social network profile, they would also threaten to send the link to the victim's family and friends.

If the victim paid, the scammer might go on to demand further payment before removing the image or video.

Read more at www.scamwatch.gov.au.

#10. Mobile phone scams

Number of scam reports:
1351

Per cent of total scams reported:
2 per cent

Number of consumers reporting losses:
269

Total losses reported by consumers:
$51 775

Scam conversion rate:
20 per cent

Mobile phone scams remained the tenth most commonly reported scam type in 2013. Contact levels increased only slightly by 4 per cent to a total of 1351 reports.

At the same time, reported losses decreased by 86 per cent to $51 775. In 2013 only three people reported losing over $5000 to mobile phone scams.

This scam category is limited to ringtone, competition and missed call scams, and as such does not include all scams delivered by mobile phones (e.g. unexpected prize scams). As previously reported in section 2.3, scams *delivered* via mobile phone recorded a total loss of $1 848 805.

Mobile phone scams can be difficult to recognise. They might come from somebody who talks as if they know the person, they might come through a "missed call" from an unknown number that they redial, or they might be up-front about what they are promoting but have hidden charges. Mobile phone scams may include offers for free or cheap ring tones, or the chance to win fantastic prizes.

Ring tone scams claim to offer 'free' or cheap ring tones that end up leading to a subscription or premium rate service.

Missed calls from unknown numbers can lead to premium rate charges or mysterious text messages that cost a lot of money when replied to.

SMS competition and trivia scams involve an invitation to enter a competition or trivia contest for a great prize but mislead recipients about how much it will cost to take part or their chances of winning.

As reported in chapter 2, while scams delivered to mobile phones via SMS decreased by around 35 per cent in 2013, reported losses almost doubled, with nearly $1.85 million reported lost to an SMS scam.

SMS provides scammers with a relatively cheap method to spam thousands of people at once with scams.

Scams sent en masse via SMS are a type of 'spam', which is unwanted contact by electronic means.

The Australian Communications and Media Authority has a dedicated Spam SMS hotline that consumers can use to forward on scams sent via text message: 0429 999 888.

PROTECT YOURSELF TIPS

1. Subscription or competition offer? Read all the terms and conditions of any offer very carefully: claims of free or very cheap offers can have hidden costs.
2. Don't reply to missed calls from an unknown number—it could be a scammer.
3. Remember: phone numbers starting with '19' are charged at a premium rate and can be very expensive.

Scams survivor's story:
Keith 'STOPS' before replying to a scam SMS

Keith received a text message from a number beginning with '19' with the following message: "Unlucky in love? Bored of your job? Looking for a change? Look no further! Reply 'YES' together with your date of birth and we will provide you with the answers you are looking for!"

Keith was intrigued but he had a nagging feeling that something wasn't quite right. He went online and typed the phone number into a search engine. He found a lot of posts from people who had received the same message - they warned that this was a scam. When they had replied 'YES', they began to receive a daily SMS containing their horoscope. However, they had received a nasty surprise when their mobile bill arrived, with lots of additional charges included. Unbeknownst to them, by replying 'YES' to the original message, they had signed up for an expensive and ongoing subscription service.

Keith was relieved that his gut instincts had turned out to be right and he immediately deleted the SMS from the '19' number. He also contacted his mobile phone provider and asked them to block any further messages being received from that number.

"Calls and SMS from '19' numbers are for premium services and you will be charged a premium fee. Make sure you know exactly what you are replying 'YES' to."

ACCC Deputy Chair Delia Rickard

Mobile apps: the next platform for scams?

Scammers move with the people, adapting their approach to take advantage of innovations in technology and communications.

These days Australians are increasingly using smart devices as a useful tool in everyday life with mobile applications, or 'apps', helping people go about their lives in ways that would have seemed unimaginable not that long ago.

For many, apps are now indispensable in helping them to connect with others, transact online, record moments in photos or journals, play games or organise one's life.

Given the increasing popularity of apps, it is important that people are alert to scams delivered through them. Just as scammers embed electronic content in emails, attachments and websites with malicious software, apps can also be similarly infected.

When one considers the amount of personal information that is stored on smart devices—contact details, financial information, social schedules and business meetings, photos… the list goes on—it is unsurprising that scammers will seek to infiltrate them. If they are successful in accessing this information, scammers can then use it to commit identity theft, steal money, and in other fraudulent acts.

Mobile apps may be increasing in popularity with people, but that also means that scammers are likely to increase using them too.

People can help to protect themselves by thinking twice before downloading any app—verify that it is a legitimate and safe app by researching other users' experience.

Above all, consumers should be careful about what information is stored on a smart device—where possible, lock access, change passwords regularly, update security software and backup content.

4. Research

Research plays an important role in dealing with scams activity, helping to form a better understanding of how scams operate, the scale of activity, their impact on victims and emerging trends.

Scams-related research is critical in informing the ACCC and other law enforcement agencies' strategies to tackle scams activity so that these efforts are as effective as possible in addressing the conduct.

This chapter outlines some key recent and upcoming research undertaken around scams.

4.1 Australasian Consumer Fraud Taskforce research

Since 2006 the Australian Institute of Criminology (AIC), on behalf of the Australasian Consumer Fraud Taskforce, has conducted an annual online survey to understand the changing experience of consumer fraud and how it affects Australian and New Zealand residents.

The latest report, *Australasian Consumer Fraud Taskforce: Results of the 2013 online consumer fraud survey*, was based on the experiences of 1059 survey participants. As respondents self-selected to complete the survey, the results are not representative of the Australian or New Zealand population as a whole. However, the survey does provide an indication of the types of scams that were experienced by a selection of individuals who were exposed to scam invitations in the 12 months prior to completing the survey.

A high proportion (97 per cent) of survey participants reported receiving a scam invitation in 2013, and 34 per cent responded to the invitation in some way (requesting more information, providing personal details, sending money or a combination of these acts). Six per cent of survey participants sent personal details as a response to a scam invitation, 4 per cent suffered a financial loss and 7 per cent reported both sending their personal details and experiencing a financial loss. With outliers removed, the total financial loss reported was $1 110 106 with a median amount of $2150.

Dating and romance scams were responsible for the greatest number of respondents sending both money and personal details or passwords to a scammer, and were among the most likely to convert to a financial loss, with over $536 000 reported lost. This finding aligns with 2013 scam contacts to the ACCC, where dating and romance scams became the number one scam type for financial losses.

The 2013 survey highlighted the need for developing a greater understanding of the consequences of scams—one that goes beyond the financial impact of scams and examines the psycho-social aspects and lasting effects that victims may experience.

4.2 Curtin University small business scams national survey

In 2012 and 2013 Curtin University undertook national research into scams affecting Australian small businesses to identify the most common scams targeting small businesses, the scale of financial loss, and how they respond to a scam approach.

The research report, *Small business scams national survey 2012/13*, was based on responses from 192 businesses, with the sample representing every ANZSIC class of business, annual turnovers ranging from $10 000 to $20 million per annum, and male and female respondents broadly representative of the small business population in Australia.

Key findings of the small business scams research were as follows:

- The most common scams reported were lottery and sweepstake scams, advance fee fraud and free 'spam' type offers.
- Email was the primary method of scams delivery, with social media also gaining popularity.
- Reported financial losses ranged from $100 to $10 000 per annum. The time spent dealing with the repercussions of scams activity was estimated to be as high as 100 hours.
- Financial risk-taking and increasing scam propensity (scam amount lost) may be linked, with a somewhat greater quantum of loss exhibited by respondents who take higher financial risks.

- 'Routine Activity Theory', which proposes that victimisation is likely to increase in line with time spent in 'harm's way', can help predict scam losses, with a relationship found between financial losses and the degree of online activity.

The survey also included a gullibility test, which found that 19 respondents selected an option that was 'too good to be true'. These respondents also self-assessed as being unconfident in identifying a scam.

The report outlines a list of self-help strategies for small businesses to identify scams and avoid victimisation, which includes a range of precautions to take in the online environment.

The ACCC provided assistance to Curtin University to undertake this research.

4.3 Upcoming Australian Bureau of Statistics' personal fraud survey

In 2013 the Australian Bureau of Statistics (ABS) commenced work on the 2014–15 personal fraud survey.

This national survey is a key piece of work in helping to understand the scale of scams activity across the country, with comprehensive data from the populace providing a detailed overview of the number of people in Australia affected by scams, the nature of scams and their impact.

The most recent report, *Personal fraud survey 2010–11*, found that Australians lost $1.4 billion due to personal fraud (which includes credit card fraud, identity theft and scams).

The results of the 2014–15 survey will be released in 2016.

5. Education and awareness raising initiatives

The ACCC uses a range of tools to protect consumers from scams, with education and awareness raising a key pillar in its efforts to minimise the impact of scams on society.

Scams present a considerable challenge for law enforcement agencies, with the perpetrators often frustrating traditional regulatory approaches by setting up schemes that are difficult to trace, based overseas and cross multiple jurisdictions. Scammers take advantage of instant and anonymous communication channels to connect with targets, and are quick to morph and phoenix operations into a new scam when authorities close in.

Education and awareness raising therefore plays a key role in preventing harm arising from scams activity, by empowering individuals with the knowledge and skills to identify and avoid victimisation in the first instance.

This chapter outlines ACCC initiatives to help the Australian community self-protect against scams.

5.1 SCAMwatch

The ACCC runs the Australian Government's SCAMwatch website (www.scamwatch.gov.au), which provides the public with information and advice on how to recognise, avoid and report scams, as well as what to do if one thinks that they have been scammed. Consumers and small businesses can also receive information over the phone through the SCAMwatch hotline.

SCAMwatch has significant brand awareness amongst the community with the Australian Government, state and territory government departments, police forces, media, consumer groups and private companies directing people to the website for information on scams. SCAMwatch is also considered a valuable resource internationally, with a number of regulators in overseas jurisdictions including Canada, New Zealand, and the United Kingdom referring consumers to the site.

SCAMwatch also operates as the web portal for the Australasian Consumer Fraud Taskforce, promoting Taskforce initiatives such as its annual National Consumer Fraud Week campaign. More information about the Taskforce is provided at section 7.1.

In 2013 the SCAMwatch website received 1 228 599 unique visitors, an increase of 256 775 or 26 per cent from 2012. Figure 8 shows that SCAMwatch visits have consistently trended upwards since the ACCC assumed responsibility for the site in 2006, with recent years seeing an increase in over 40 per cent from 2010-11, and 25 per cent and above in 2011–12 and 2012–13.

Although the majority of visitors were located in Australia, SCAMwatch was also visited by people located around the world.

Figure 8: Unique visitors to the SCAMwatch website from 2006 to 2013

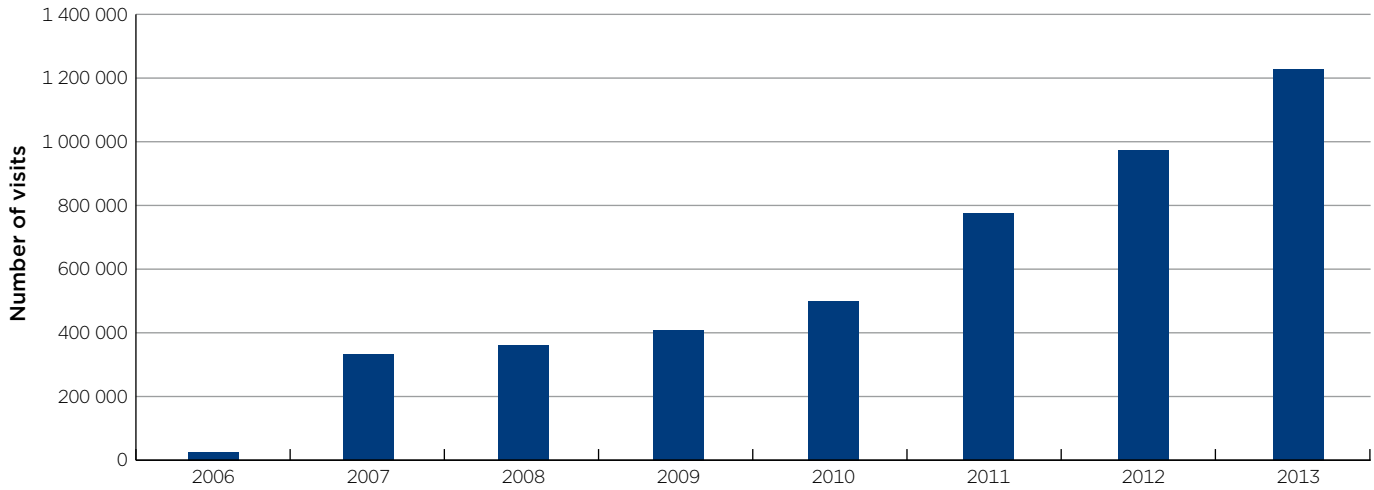
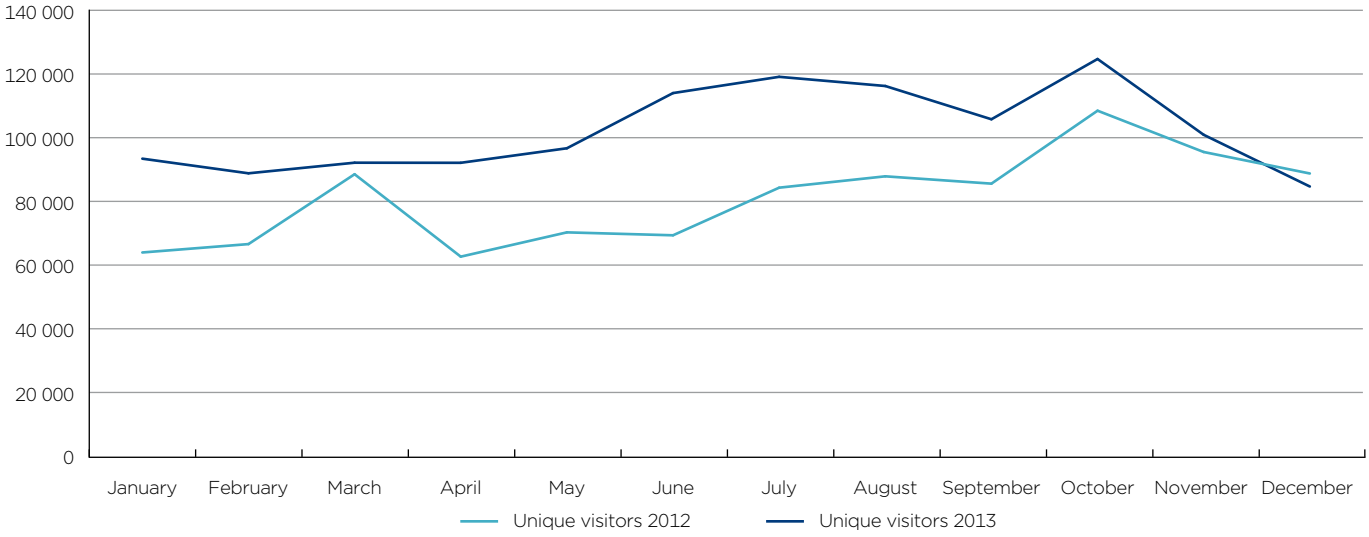


Figure 9 shows that in 2013 SCAMwatch attracted on average more unique visits per month compared to 2012, with the exception of a slight decline in December. SCAMwatch received an average of between 2700 and 3800 visits per weekday.

Figure 9: Comparison of monthly visits to the SCAMwatch website in 2012 and 2013



As in previous years, visits to SCAMwatch were higher than average during the annual Fraud Week campaign (17–23 June 2013). During this week, SCAMwatch received between 2989 and 8248 visits per day.

SCAMwatch radar alert service

The ACCC also runs a free SCAMwatch subscription service whereby subscribers receive email alerts, known as 'SCAMwatch radars', on emerging scams.

In 2013 the subscriber network reached 29 150 subscribers, an increase of 30 per cent from 2012.

The ACCC issued 18 SCAMwatch radars in 2013 to warn Australians about the imminent risk of scams, including around current events such as the summer bushfire season, Valentine's Day, the Boston Marathon tragedy, tax time, spring racing season and the launch of the 2015 Anzac Day commemorations ballot for the 100th anniversary of the Gallipoli campaign.

SCAMwatch radar alerts are also an effective mechanism for a collaborative approach between government and industry to alert the public to scams targeting customers or particular community groups. For example, in July 2013 the ACCC and the Department of Immigration and Citizenship issued a joint alert to warn visa holders about scammers calling to demand payment to resolve issues with their visa, or risk deportation.

A full list of SCAMwatch radar alerts issued in 2013 is provided at appendix 2.

Don't let scams slip under your radar! Sign up to the SCAMwatch alert service

The ACCC has a free SCAMwatch subscription service where you can sign up to receive email alerts on new scams doing the rounds.

Sign up to receive SCAMwatch radar alerts at www.scamwatch.gov.au.

SCAMwatch Twitter—@SCAMwatch_gov

The ACCC also communicates with the public via its SCAMwatch Twitter profile—@SCAMwatch_gov. This social media platform allows SCAMwatch to reach consumers, small businesses and the media in real time as scams emerge.

In 2013 SCAMwatch Twitter posted 583 tweets to its 4374 followers on the following topics:

- alerts on emerging and current scams
- information exposing scammers' tactics
- tips to outsmart scammers and protect oneself
- how to report a scam
- what to do after being scammed.

Join the SCAMwatch Twitter community

Follow SCAMwatch on Twitter to receive timely alerts on scams targeting Australians

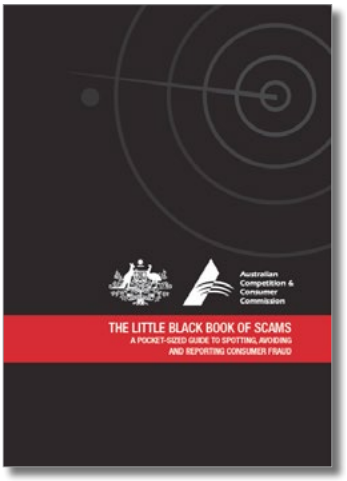
Visit https://twitter.com/SCAMwatch_gov or @SCAMwatch_gov.

5.2 Other scams educational resources

The ACCC has also produced a range of educational resources to educate consumers and small businesses about how to identify a scam and avoid being duped.

The Little Black Book of Scams

The ACCC's *Little Black Book of Scams* is its primary educational resource, and the ACCC's most popular publication. In 2013 over 91 000 copies of the book were distributed throughout the community.



This publication highlights the most commons scams that target Australians such as advance fee fraud, fake lotteries and sweepstakes, dating and romance scams, computer hacking and online shopping scams. It also explains scam delivery methods, tools used by scammers to trick people, personalised scam approaches, and golden rules on how to protect oneself.

The *Little Black Book of Scams* is considered a best practice educational resource internationally, with several overseas regulators producing their own localised versions.

Small business scams factsheet launched

In April 2013 the ACCC released *What you need to know about: small business scams*, a factsheet for small businesses on common business scams and how to avoid them.

The factsheet explains overpayments scams, directory entry or unauthorised advertising scams, investment scams, office supply scams, domain name scams, and email intercept and ransomware scams. It also provides a list of steps that businesses can take to help prevent being scammed.

The factsheet was downloaded over 450 times between April and December 2013.

5.3 Media and communications activity

The ACCC recognises the important role of the media in helping to raise community awareness about scams activity. In 2013 the ACCC continued to proactively generate media interest in scams targeting Australians.

The Australasian Consumer Fraud Taskforce's National Consumer Fraud Week campaign is the key annual public awareness raising initiative for the ACCC. As with previous years, the release of the *Targeting scams* report during Fraud Week received significant media coverage in 2013.

Throughout the year ACCC spokespeople engaged in over 200 scam-related interviews for print, radio and TV reaching a wide audience across the capital cities, remote Indigenous communities, and rural and regional Australia. This activity was supported at the local level by the inclusion of scams information in a number of community and business presentations.

The ACCC also continued to raise community awareness of scams activity through the 'Scam of the month' initiative (see highlight box).

ACCC 'Scam of the month' initiative puts scams under the media spotlight

In 2013 the ACCC continued to develop its 'Scam of the month' initiative as a key part of its strategy to raise the profile of scams amongst the Australian community by way of media activity.

Each month, the ACCC selected a scam of particular concern to warn the public about and developed newsworthy and timely content to maximise media coverage. For example, Valentine's Day saw a warning to those looking for love online to watch out for dating and romance scams. May provided a caution about holiday scams for people booking winter getaways. In November, the public was alerted to sports betting scams in the lead-up to the Melbourne Cup.

The ACCC worked with news outlets to generate media coverage of this initiative. This media engagement helped the ACCC to reach a broad cross-section of the community with scam warnings.

6. Disruption and enforcement activities

Disruption and enforcement activity are both important elements of the ACCC's strategy to tackle scams.

Where appropriate, the ACCC will undertake enforcement activity against scammers to stop the conduct and send a deterrence message to others. However, the increasingly sophisticated, overseas and anonymous nature of scams presents considerable difficulties in identifying and prosecuting the perpetrators behind these schemes. Enforcement action is also not always the most effective way of dealing with scams as it is a costly exercise that fails to meet the immediate need of scam victims—that is, intervention to cease further interaction with the perpetrator. Further, traditional litigation is difficult against scammers who are quick to strike and morph into a new scheme to target other victims.

In this context, disruption activity—that is, initiatives aimed at intercepting, interrupting and impeding scams—is a key element in minimising and, in some cases, preventing further harm.

This chapter outlines efforts undertaken by the ACCC, the police services in Queensland and Western Australia, and business enablers to deter, discourage and disable scammers targeting Australians.

6.1 Scam disruption activities

The ACCC recognises that, in addition to education and awareness raising, disruption activity is one of the primary tools to effectively respond to scams given that traditional law enforcement is often not possible.

Disruption activities may allow law enforcement agencies to restrict or even discontinue the activities of a scammer and to prevent the harm that they may otherwise cause, often without having to identify or locate the scammer. Disruption activity typically involves collaboration between government and industry to identify intervention opportunities that might:

- minimise reputable platforms and services from enabling scams activity
- prevent scammers from communicating with their targets
- provide timely warnings to better educate consumers that utilise legitimate services
- interrupt the sending of funds.

In 2013 the ACCC's disruption activities focused on examining online shopping scams, tackling a re-emerging small business scam, and planning for a disruption project on relationship scams to be launched in 2014.

Online shopping scams—industry engagement

In 2013 the ACCC initiated discussions with the online shopping industry to explore possible ways to disrupt scams activity targeting Australians shopping or selling online.

This project arose after the ACCC observed an increase of 65 per cent in reports of online shopping scams from 2011 to 2012, with associated financial losses reaching over $4 million.

In June 2013, as part of National Consumer Fraud Week, the ACCC held a workshop in Melbourne, which was attended by representatives from online shopping businesses and platforms, industry associations, financial institutions, security software companies and government stakeholders. During the workshop, participants discussed their perspectives on how to prevent scams occurring in the online retail environment.

A follow-up meeting was held in Sydney in August 2013, with key representatives from the online shopping and money transmitter sector exploring opportunities to better protect consumers from these scams.

'Yellow Pages' small business scam

In September 2013 the ACCC identified the re-emergence of a business directory scam targeting Australian small businesses. After receiving a surge in reports from small businesses who had received a fax claiming to be from 'Yellow Page Australia' and 'Open Business Directory Ltd', the ACCC quickly worked to minimise the harm arising out of this scam.

This scam aimed to trick businesses into thinking that it was affiliated with Sensis' Yellow Pages® directory by using this well-known Australian company's name and a deceptively similar depiction of the 'Walking Fingers' logo. The perpetrators behind the scheme sent a fax en masse to small businesses, which appeared to be

seeking confirmation of their contact details. However, on closer inspection, the fax was a solicitation for an agreement to sign up to an online business directory service that charged $99 per month for a minimum two-year period.

The scam was supported by a website that looked like a business directory and strongly suggested an affiliation with Sensis' Yellow Pages®, when this was not the case.

The ACCC suspected that the scammers deliberately chose to target small businesses during the busy time of the new financial year period when they were more vulnerable to fall victim.

The ACCC previously took successful court action against the perpetrators behind another 'Yellow Pages' scam targeting Australian businesses and, in April 2011, the Federal Court imposed penalties totalling $2.7 million against two overseas companies for similar conduct. Authorities in the United States and Canada have also successfully prosecuted scammers behind this global scheme. Whilst the perpetrators from this round of faxes appeared to be different, the conduct was nearly identical.

In 2013 the ACCC adopted a disruption approach to tackle the scam given that it had re-emerged despite the strong deterrence message arising out of the previous court outcome. Working closely with Sensis, the ACCC promptly sought to raise community awareness of the scam. On 1 August the ACCC issued a SCAMwatch radar alert, media release and circulated information through its small business networks.

The ACCC also worked with Australia Post to arrange for the seizure of letters containing invoices for unsolicited services, with reports indicating that the scammers were sending these invoices after the initial fax was circulated. Under section 90UA(3) of the *Australian Postal Corporations Act 1989,* Australia Post may remove batches of articles from the normal course of carriage if a consumer protection agency gives notice of articles which may contain scam mail. Where other opportunities arise, the ACCC will continue to avail itself of this important disruption tool.

Sensis was also successful in taking action to shut down the scam website 'www.yellow-page-australia.com'. However, the perpetrators then moved the scam website to 'www.yellow-page-australia.at', a site registered in Austria. This transfer prompted the ACCC and Sensis to issue further alerts in early 2014.

Relationship scams and upcoming national disruption project

In 2013 the ACCC commenced planning for a national disruption project focused on relationship scams, building upon previous work undertaken to disrupt this scams activity.

Relationship scams are acts of fraud that are premised on the scammer building a deceptive connection with an individual or business in order to secure their personal details or money.

The most common and destructive type of this fraud is dating and romance scams, which in 2013 moved to number one position in terms of financial losses reported to the ACCC. However, relationship scams can cross over any scam type where the perpetrator invests time and effort into convincing the victim that some form of relationship exists and then manipulates this to secure a personal gain. For instance, complex small business and investment scams are based on a relationship of trust where, over time, the victim becomes so heavily invested in the scheme from an emotional, time and financial perspective that it is difficult to break through the web of deceit.

In recent years the ACCC has prioritised efforts aimed at minimising consumer harm arising out of relationship scams.

In 2011–12 the ACCC prioritised compliance work aimed at dating and romance scams after observing a rising trend in report levels and significant associated financial losses. Of particular concern was the ongoing high conversion rate reported against dating and romance scams, which indicates a particular vulnerability of consumers to these types of scams. The ACCC initiated a working group with dating website operators to address scams targeting their users, with participants collaborating to identify disruption measures to improve responses to these scams. On Valentine's Day 2012 the ACCC launched a set of voluntary guidelines to help the industry as a whole protect consumers from these scams.

The ACCC has also previously taken steps to disrupt relationship scams more broadly through the analysis of financial intelligence on money sent overseas to identify and then reach out to suspected victims. This approach proved to be reasonably successful in ceasing financial transactions to scammers and limiting further exposure.

Other government authorities, most notably in Queensland and Western Australia, have also adopted a similar approach to tackle relationship scams targeting their citizens (see highlight box on page 51).

In 2013 the ACCC decided to bolster its work in this area and commenced planning for a national disruption project to tackle relationship scams.

Building on its previous work and that currently underway in Queensland and Western Australia, the ACCC will work with other government members of the Australasian Consumer Fraud Taskforce to analyse financial intelligence on a larger scale in order to identify potential victims. This project involves alerting all identified victims that it is likely they are being defrauded. Where appropriate, this engagement may involve face-to-face intervention with the victim to convince them that they have been scammed.

The ACCC will also work with industry to identify other opportunities to implement measures that may provide cost effective scams disruption. For instance, the ACCC will revisit its collaboration with dating website operators to see what further preventative steps can be taken. The ACCC will also engage with money transmitter agencies and financial institutions to examine options for blocking funds transfers where it can be established that scammers are engaging in fraudulent conduct.

Disruption—it makes good business sense

Most scams activity today cannot occur without scammers utilising the legitimate services that people use to communicate, connect and transact. Online dating websites, email and telecommunications services, social networking platforms, money transmitter and payment services—all of these are essential elements in enabling scammers to target people.

Scammers are good at using them, too—often more so than the general public—as they have experience with using these mediums to create scams that can appear to the average person as a legitimate scheme.

The ACCC recognises the important role that enabler businesses have to play in disrupting scams, many of whom have realised that it makes good business sense to invest in fraud prevention systems. A collaborative effort between government and industry can help to create more widespread improvement across particular sectors and thereby reduce scammers targeting enablers with less robust systems in place.

Following on from the ACCC's work with the dating and romance industry in 2011–12, which culminated in the release of best practice guidelines, some online dating service providers reported that improvements to their fraud prevention systems significantly reduced scams occurring through their services.

Scammers will continue to adapt and move to other platforms or mediums where consumers are vulnerable to an approach. This therefore means that government and industry alike must be adaptive too.

In the end, those enablers that have systems in place to protect their customers also reap the benefits as consumers feel safer using their services.

Case study: Queensland and West Australian authorities help scam victims

Other government authorities have also adopted a proactive approach to disrupting scams and protecting local citizens. In particular, authorities in Queensland and Western Australia (WA) have implemented measures to intervene scam victims and cease further financial losses.

Gold Coast scams disruption

The Queensland Police Service's Fraud and Corporate Crime Group has led the way in Australia in tackling scams head on, with scam victim intervention a long-standing priority area of their work.

The analysis of financial intelligence data is the primary means by which the Queensland Police Service identifies possible scam victims. This is then followed by victim intervention, which can range from a phone call through to intercepting victims about to board a plane to meet the scammer overseas.

In 2010 Queensland Police Service set up Australia's first ever scam victims support group, whereby victims work through their experiences in a supportive environment. The Victims of Fraud Support Group meets once a month, and is open to any victim of fraud, friend or family member in need of support.

In 2013 Detective Superintendent Brian Hay was featured on SBS' *Head First* series' 'Social Monster' episode, which focused on victims of dating and romance scams. The show highlighted the lengths that authorities have to go to convince people that they have fallen victim to a relationship scam.

The Fraud and Corporate Crime Group has also commenced working with Griffith University to conduct research into developing more effective communications scripts for the intervention process when working with victims.

West Australian scams disruption

In 2013 the WA Police Major Fraud Squad and the WA Department of Commerce (Consumer Protection) initiated a joint disruption project, 'Operation Sunbird', to identify and prevent consumer fraud originating from specific West African countries against WA citizens.

Together, WA Police and the Department of Commerce identified that between 2011 and 2013 organised criminals defrauded locals out of over $11 million. Many of these losses were the result of relationship fraud.

After identifying potential scam victims through financial intelligence data, WA Police and the Department of Commerce approach victims. In the first instance, victims are sent a letter advising that they had been identified as a potential victim of fraud and to cease contact with the scammer and stop sending any further funds overseas. Where financial intelligence reveals that the victim is continuing to send money, a further more specific and targeted letter is sent and then followed up with face-to-face engagement where significant detriment continues.

To date, after a personal visit by police or contact with Department of Commerce officers, almost all victims have acknowledged that they were defrauded and subsequently stopped sending money.

WA Police and the Department of Commerce also help scam victims access support services to overcome their experience.

6.2 Scam-related enforcement activities

ACCC enforcement activity

Where appropriate the ACCC will undertake enforcement action against the perpetrators of scams, particularly where it is likely to have the potential to deter others who may be considering engaging in unscrupulous conduct.

In 2013 the ACCC initiated proceedings or concluded action against a number of traders allegedly involved in misleading and deceptive or scam-like conduct.

Operator of Crimeguard pyramid selling scheme banned for five years

In February 2013 the Federal Court made declarations by consent that Mr Leslie Forsyth Stott, a former director of Crimeguard International Security Systems Pty Ltd, was knowingly concerned and a party to Crimeguard's participation in a pyramid selling scheme.

Mr Stott also engaged in false, misleading and/or deceptive conduct concerning representations about the profitability of the Crimeguard business.

As a result of Mr Stott's involvement, the court made an order by consent banning him from managing a company for five years.

This outcome followed enforcement action by the ACCC, with the order significant as it was only the second time that the ACCC had obtained orders disqualifying an individual from managing companies.

As well as disqualifying Mr Stott for five years, the Court imposed a permanent injunction restraining him from engaging in future pyramid schemes and from promoting business activities or opportunities where representations are made as to potential earnings without reasonable grounds.

Pyramid selling schemes—how they work

In a pyramid scheme, the only way for a member to recover any money is to convince other people to join up and part with their money as well.

Pyramid selling schemes can be highly sophisticated and hard to tell apart from genuine offers. Most of these schemes disguise their true purpose by introducing products that are overpriced, of poor quality, difficult to sell or of little value.

The tell-tale sign of a pyramid selling scheme is that they recruit people rather than selling a legitimate product or service.

In Australia, it is against the law not only to promote a pyramid scheme, but even to participate in one.

Adepto Publications, director and manager penalised for charity scam

In March 2013, following ACCC court action, the Federal Court in Sydney ordered Adepto Publications Pty Ltd (Adepto), its sole owner and director, Craig Mitchell, and a former manager, Danielle McKay, to pay penalties totalling $750 000 after they admitted that they had made false and misleading representations in relation to advertising services that were never requested.

The operators also falsely claimed that the advertising services were for publications with a philanthropic slant including the National Emergency Relief Guide, Underprivileged Childrens Guide and Volunteer Organisations Guide.

Representatives of Adepto made unsolicited phone calls to Australian businesses about advertising in these publications. After the call, even if the business did not agree to take out an advertisement, Adepto posted them a copy of the published advertisement and an invoice seeking payment. If the business did not pay, Adepto representatives made follow-up calls demanding payment.

Adepto admitted that it had no affiliation with any charitable or non-profit organisations. Adepto also admitted that while it represented that 2000 copies of the publications carrying the businesses' advertisements would be distributed to various organisations in the same postcode as the advertiser, actual distribution was significantly less being, at most, limited to 2000 copies nationwide.

The Court made declarations, ordered costs and imposed injunctions by consent upon all of the respondents, restraining them from being involved in similar conduct. A specific injunction was also imposed by consent restricting the respondents from requesting payment for advertisements in its publications without prior written confirmation from consumers, and from pursuing payment from businesses who had previously been invoiced.

The Court found that the conduct, which took place over several years, would probably have continued but for the intervention of the ACCC. Justice Cowdroy found that the conduct was 'blatantly and knowingly deceitful'.

How these scams work

- You receive a call out of the blue from someone claiming to represent a business directory or other publication you've never heard of. The caller offers to place an advertisement for your business in the publication for a fee.
- The caller may refer to a publication with a philanthropic purpose in the hopes of appealing to your charitable side. Alternatively, they may claim to have affiliation with government or a well-known business. They may even claim to represent a business through which you currently advertise.
- If you accept the offer, you find that when the ad is published, the actual distribution number and geographic reach is significantly less than what you signed up for.
- If you decline the offer, you subsequently receive an invoice in the mail along with a copy of the ad.
- If you do not pay, you receive follow-up calls or official-looking letters demanding payment.

Artorios Ink director and manager penalised for ink cartridge scams

In December 2013 the Federal Court ordered Tuan Nguyen, the sole director, and Thuan Nguyen, the sales manager, of Artorios Ink to pay a penalty of $50 000 each after they admitted to deliberately misleading and deceiving small businesses to generate ink cartridge sales.

Artorios Ink was a telemarketing company that sold printer cartridges to businesses from 2008 to 2012. The company was placed into voluntary liquidation on 25 February 2013 after the ACCC instituted proceedings in September 2012.

The Federal Court found that, during 2011 and 2012, Artorios Ink engaged in conduct that was misleading or deceptive and made false or misleading representations to five small businesses including that the businesses had agreed to purchase printer cartridges, that Artorios Ink was an approved, regular or current supplier, and that Artorios Ink had instituted court proceedings against the businesses to obtain payment.

The Federal Court also found that Artorios Ink asserted a right to payment for unsolicited goods, by sending demands for payments for ink cartridges which the small businesses had never agreed to purchase.

The Court made declarations by consent, and accepted undertakings from the respondents that they would not manage or be a director of a corporation for five years.

In her findings, Justice Mortimer stated: "The most serious aspect of the conduct was its premeditated character, the implementation of a system of deceiving unsuspecting employees and owners of small businesses into believing that they had ordered printer cartridges and were obliged to pay for them."

ACCC Deputy Chair Dr Michael Schaper noted that this court decision was important as it sent "a warning to traders that dishonest business practices can result in substantial penalties being imposed against the individuals responsible."

Scammers' strategies—office supply scam

Scammers running office supply scams use a range of tools to trick employees into confirming orders that were never placed including:

- **Background research**: Scammers call businesses to gather information, such as names of other employees and printer models, which they then later use to trick staff into thinking that they are a regular supplier.
- **Recordings**: Scammers will make a follow-up call where they trick a staff member using information gathered in the initial call to 'confirm' an order. This call is recorded to use as proof that business signed up to them.
- **Enticements**: Scammers may offer gifts, such as vouchers, discounts or cameras, to entice staff members to orally agree to receiving those gifts. Again, this call is recorded with the conversation later used out of context to corner the business into paying for goods.

7. Domestic and international collaboration

The ACCC recognises that scams require a coordinated response between the public and private sectors, with collaboration between local and overseas entities essential to effectively deal with the global reach of scams.

These days, law enforcement agencies in both Australia and overseas face the same challenges that arise from scam operations having the capacity to reach consumers across jurisdictions with just the click of a button. Scammers often rely on legitimate platforms or communications channels to achieve a global reach, taking advantage of popular and trusted mediums to deliver the scam. As such, in addition to working with overseas law enforcement agencies, collaboration with business enablers to disrupt or disable scams activity is a critical component of disruption activity.

This chapter outlines ACCC efforts to collaborate with domestic and international agencies, and industry stakeholders, to prevent or minimise scams.

7.1 The Australasian Consumer Fraud Taskforce

The Australasian Consumer Fraud Taskforce was established in 2005 and comprises of 23 government member agencies across Australia and New Zealand that share a responsibility for consumer protection in relation to fraud and scams activity.

The Taskforce's main functions are to:

- enhance the Australian and New Zealand governments' enforcement activity against fraud and scams
- share information and research on consumer fraud and scams
- develop coordinated consumer education initiatives to raise community awareness about scams.

The ACCC's Deputy Chair, Delia Rickard, is the Chair of the Taskforce. The ACCC also provides secretariat services to the Taskforce.

The Taskforce's work is assisted by a number of government, business and community group partners. Partners recognise the seriousness of consumer fraud in Australasia, and play an important role in disrupting scams activity and raising community awareness.

A list of Taskforce member agencies and partners is provided at appendix 4.

National Consumer Fraud Week

A key initiative of the Taskforce is the annual National Consumer Fraud Week campaign, a coordinated effort by the Taskforce and its partners to raise community awareness about scams. Fraud Week supports the International Consumer Protection Enforcement Network's Global Fraud Prevention initiative.

2013 campaign—'Outsmart the scammers!'

The 2013 Fraud Week campaign, 'Outsmart the scammers!', ran from 17 to 23 June and focused on helping Australians identify online shopping scams so that they can shop safely online without being duped.

The key message of the campaign was to stay one click ahead of scammers by being a smart and safe shopper online.

Campaign highlights included:

- release of the ACCC's 2012 *Targeting scams* annual report
- 'Outsmart the scammers!' video launch (produced by ABC's *The Checkout* team)
- 'Outsmart the scammers!' conference 18 June, The Arts Centre Melbourne (hosted by the ACCC)
- online shopping scams industry workshop 18 June, The Arts Centre Melbourne (hosted by the ACCC)
- Consumer Affairs Victoria's 'Stevie's Scams School' consumer video launch 17 June, Small Business Victoria office (launched by the Hon. Heidi Victoria MP, Minister for Consumer Affairs)
- Australasian Consumer Fraud Taskforce 2012 consumer survey results release 17 June (compiled by the Australian Institute of Criminology).

- Small business scams forum 21 June, WA Small Business Development Corporation (SBDC) office, Perth (hosted by the ACCC and WA SBDC).
- 'Stay one click ahead' mouse pad and calendar (distributed by partners and at major events).

The launch of the ACCC's fourth *Targeting scams* report generated significant media interest, which was used to promote Fraud Week. In the first two days of the campaign, Fraud Week was covered by nearly every major newspaper and radio station, focusing on the financial losses and increase in the number of online shopping scams reported to the ACCC. Further media focusing on small business scams also received coverage.

A social media coordination group was also formed with 35 organisations, companies and agencies tweeting and blogging about the campaign. One ACCC Facebook blog received over 4200 views.

The 2013 Fraud Week 'Outsmart the scammers!' video, produced by ABC's *The Checkout* team, also proved to be popular, with around 3500 views during the campaign period.

'Outsmart the scammers!' was supported by over 140 partners from a diverse range of backgrounds including government, business, community groups and industry bodies. Key areas relating to the theme were targeted including online shopping service providers, online and computer bodies, and the financial industry.

Figure 10 provides an outline of the 'Outsmart the scammers!' campaign messaging.

Figure 10: 2013 National Consumer Fraud Week campaign messaging

Outsmart the Scammers!

National Consumer Fraud Week 17–23 June 2013

Have you ever bought or sold something online, only to find that the person at the other end isn't the real deal?

National Consumer Fraud Week 2013 is all about outsmarting scammers online by learning how to buy and sell safely online without being duped.

Australians are increasingly going online to buy goods and services, taking advantage of the speed, convenience and greater choice that the internet can offer. Unfortunately scammers like shopping online for their victims too.

Stay one click ahead—follow the **Top 5 tips to Outsmart the Scammers**:

1. **Think twice**—if a deal looks too good to be true, it probably is.
2. **Find out what other shoppers say—**make sure the person that you are dealing with, and their offer, is the real deal.
3. **Protect your identity**—your personal details are private and invaluable; keep them that way and away from scammers.
4. **Keep your computer secure**—Install software that protects your computer from viruses and unwanted programs, and make sure it is kept up-to-date.
5. **Only pay via secure payment methods**—look for a web address starting with 'https' and a closed padlock symbol. Never use a wire transfer service to send money to anyone you do not know and trust, and do not share your financial details with anyone.

Visit SCAMwatch to find out how scams work, how to protect yourself and what to do if you've been scammed:
www.scamwatch.gov.au

Outsmart the Scammers!
National Consumer Fraud Week 2013
An initiative of the Australasian Consumer Fraud Taskforce

2014 campaign—'Know who you're dealing with'

The Taskforce's 2014 Fraud Week campaign, 'Know who you're dealing with', will run from Monday 16 to Sunday 22 June and focus on relationship scams. The 2014 campaign will be asking Australians to take a step back and think about whether someone they met online is the real deal, particularly if they ask for money.

These days, scammers are highly skilled at developing a relationship with people, using all sorts of tricks to connect with them and convince them to part with their personal details or money. Is the person on the other side a friend or foe, lover or liar, money maker or taker? Fraud Week 2014 will help Australian consumers and small businesses learn how to identify a scammer and avoid losing money.

The key message of the campaign is: 'think twice before transferring money—if someone asks for money, but you've never met them in person, they're more than likely trying to scam you'.

Fraud Week 2014 will support the ACCC-led national disruption project—see section 6.1 for more information.

7.2 The International Consumer Protection and Enforcement Network

The International Consumer Protection and Enforcement Network (ICPEN) is a network comprised of over 50 governmental consumer protection authorities around the globe. It is a network through which authorities can cooperatively share information and look at combating consumer problems arising with cross-border transactions in goods and services, such as e-commerce fraud and international scams. ICPEN encourages international cooperation among law enforcement agencies.

ICPEN's Global Fraud Prevention education initiative aims to inform consumers about fraud and raise awareness of scams through targeted events and activities. The ACCC participates as part of its national Fraud Week campaign with the Australasian Consumer Fraud Taskforce.

An important ICPEN initiative is e-consumer.gov (www.econsumer.gov), a website portal featuring a global online complaints mechanism, which consumers can use to report complaints about online and related transactions with foreign companies. The site was developed in 2001 as a response to the challenges of multinational internet fraud. It is available in eight languages. The portal also provides consumers with tips on how they may be able to resolve issues and provides contacts for alternative dispute resolution services in ICPEN member jurisdictions, including Australia.

Collaboration with overseas law enforcement agencies to disrupt scams

Queensland and Western Australia (WA) Police work closely with overseas law enforcement agencies to disrupt scams targeting locals.

In 2013 WA authorities worked closely with the Nigerian Economic and Financial Crimes Commission (NEFCC) following the tragic circumstances that befell a WA woman. The woman was found dead after travelling overseas to meet a Nigerian admirer that she met online. Before her death, the victim had lost more than $100 000 to the scammer.

The NEFCC recognises the prevalence of scams activity that originates out of Nigeria and is committed to working with other law enforcement agencies, including Australian authorities, to identify and prosecute local perpetrators.

In January 2014 this collaborative effort culminated in the Nigerian admirer being arrested on fraud charges in relation to this crime.

In 2013 Queensland Police Service's Fraud and Corporate Crime Group continued its long-standing and close collaboration with overseas authorities to tackle cross-border fraud. Detective Superintendent Brian Hay, a leading figure in Australia in fighting consumer fraud, highlighted the importance of this cooperative approach in ABC's *Head First* series. In this program, which aired in May 2013, Brian travelled to Ghana where he worked with the Ghanaian authorities to catch criminals who had scammed Australians out of money after building deceptive relationships with them.

Queensland Police Service's collaboration with Nigerian and Ghanaian authorities has resulted in nearly 30 prosecutions for fraud offences. This work has occasionally also proved successful in recovering funds for the victims.

7.3 Australian Transaction Reports and Analysis Centre partnership

Since 2006 the ACCC has been a partner agency with the Australian Transaction Reports and Analysis Centre (AUSTRAC) as authorised under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Clth).

AUSTRAC is Australia's anti-money laundering and counter-terrorism financing regulator and specialist financial intelligence unit. It works with domestic partners including law enforcement, revenue, regulatory and social justice agencies, and their international counterparts.

From time to time the ACCC examines information provided by AUSTRAC for certain patterns of conduct that mirror known advance fee fraud schemes. Indicators of potential advance fee fraud can include:

- international funds transfers to a country or jurisdiction of interest
- multiple customers conducting international funds transfers to the same overseas beneficiary
- multiple international funds transfers structured in an attempt to avoid reporting obligations.

More information about AUSTRAC can be found at: www.austrac.gov.au.

Case study: reports of money lost to investment scams decrease after collaborative effort

In 2011 and 2012 the ACCC, along with other law enforcement, regulatory and service delivery agencies across federal, state and territory governments, collaborated on a scams-related initiative led by the Australian Crime Commission. Code-named 'Taskforce Galilee', these entities worked together to prevent and disrupt serious and organised fraudulent investment scams.

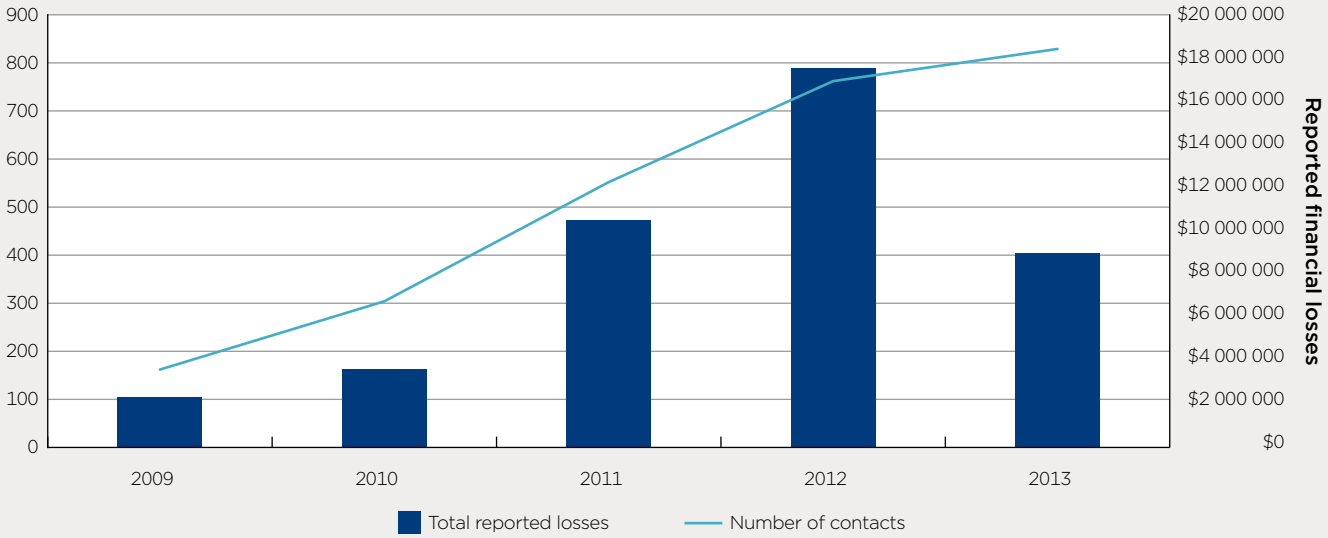
This collaborative effort arose after it was identified that millions of dollars were being lost by Australians to these schemes, in particular by individuals approaching retirement who were looking to invest their superannuation and retirement savings. These highly sophisticated scam operations where victims sign up for non-existent investment opportunities are typically initiated through an unsolicited phone call, with victims then directed to professional looking sites that appear to be legitimate. The perpetrators are skilled at using high-pressure sales tactics to persuade victims to part with their money.

As part of this joint effort, in July 2012 the Taskforce implemented a national campaign to warn and educate Australians about this type of fraud. The Australian Crime Commission report, *Serious and Organised Fraud in Australia*, attracted significant national media coverage across all major metropolitan news outlets, radio and online media channels. The Taskforce also coordinated, in collaboration with Australia Post, the largest mail-out by law enforcement agencies in Australia's history to warn Australian households about this activity.

Following this awareness raising activity, in 2013 the ACCC observed a change in contacts about investment schemes.

Figure 11 provides a comparison of investment scam contacts to the ACCC over the past five years in terms of both contact levels and reported financial losses. While contact levels rose by nearly 14 per cent from 2012 levels to 829 contacts, reported losses almost halved (48 per cent) from $17 349 347 to $9 083 512. The conversion rate, that is, the number of people who received a scam of this type and subsequently lost money, fell from 32 per cent in 2012 to 28 per cent in 2013.

Figure 11: Investment scams—total financial losses and contacts reported 2009–13



The increase in contacts to the ACCC with a concomitant decrease in reported financial losses could indicate that Taskforce Galilee was successful in raising awareness in the Australian community about these scams, with people therefore better able to protect themselves and avoid being scammed when approached by the perpetrators behind these schemes.

7.4 Upcoming Australian Cybercrime Online Reporting Network (ACORN)

As part of its response to cybercrime, in 2013 the Australian Government commenced developing a national online reporting facility for cybercrime—the Australian Cybercrime Online Reporting Network (ACORN).

ACORN represents a potentially vital tool in combating cybercrime in Australia. While there are no comprehensive figures currently available, the best available assessments suggest that cybercrime costs the Australian community billions of dollars a year and that the scale and impact of online offending is likely to increase as the internet is further integrated into the everyday lives of Australian citizens. In this context, the reporting, gathering and analysis of data and intelligence are important elements of national and international efforts to combat cybercrime.

ACORN will provide an internet-based capability that will allow members of the public to report instances of cybercrime, and access general and targeted educational advice. ACORN will also help government agencies respond quickly to acts of cybercrime.

Intelligence and threat assessments on ACORN data will be assessed by the Australian Crime Commission to assist in the development of a clearer national cybercrime picture. The system will also refer cybercrime reports to law enforcement and government agencies for further analysis.

It is anticipated that ACORN will be operational in the second half of 2014.

The ACCC continues to work with ACORN to ensure that contacts about online scams received through SCAMwatch form part of the national data set of cybercrime. SCAMwatch will continue to receive contacts from the public and to provide educational information and advice to the public on online scams.

8. Conclusions and future challenges

As highlighted by this report, scams continue to cause significant financial and non-financial harm to the Australian community. With over 92 000 contacts and nearly $90 million reported lost, we can start to grasp the scale of scams activity in Australia. However, these statistics give us just one part of the picture, with the emotional toll on victims, and broader societal and economic costs, impossible to accurately quantify.

In the face of this activity, it is imperative that we help ourselves, and those who are more vulnerable, to identify scams and avoid falling victim.

In 2014 the ACCC will direct its efforts at those scams that cause the most harm to victims: relationship scams. Unfortunately scammers appear to have a higher success rate when they invest the time and effort into developing a relationship with their victims—with over $25 million reported lost in 2013 to dating and romance scams, this approach is clearly paying dividends. Relationship scams are the most insidious in that victims are heavily invested not just with their wallets, but often with their heads and hearts, too.

Building on work currently underway by law enforcement agencies in Queensland and Western Australia, the ACCC is commencing a national disruption project for relationship scams. This project will have at its primary objective helping Australians caught up in relationship scams to identify that they are a victim and cease any further engagement with the scammer. This victim intervention approach will not only help the individual, but also reduce the significant economic losses that arise out of money flowing offshore and into the hands of scammers.

The ACCC will also continue to look at innovative ways to disrupt scams, in particular working with business enablers who can directly intervene and help prevent their customers from falling victim in the first instance or prevent funds being transferred to scammers. It really does make good business sense for corporations to invest time and effort into minimising fraud occurring through their services or platforms. At the ACCC, we see a lot of potential and value in working with industry as a whole where it is identified that scammers are taking advantage of a particular sector or market to connect with targets and/or secure the transfer of funds. As shown by this year's report, that increasingly means tackling scams in the online environment, with the internet fast on track to become the number one method of scams delivery.

In addition to this work, the ACCC will continue its efforts to help Australians protect themselves against scams through educational initiatives. The ACCC will work closely with other government agencies and private entities to realise the common goal of protecting the Australian community from scams, with the SCAMwatch radar alert service and the Australasian Consumer Fraud Taskforce's annual Fraud Week campaign important collaborative efforts in raising the profile of scams. In the case of scams, prevention really is better than cure.

Appendix 1: Scam categories by state and territory

Where possible the ACCC collects data about the geographic location of people reporting scams. Appendix 1 provides a breakdown of 2013 scam categories by state and territory.

Overall New South Wales saw the greatest number of scam contacts (31.5 per cent), followed by Victoria (21.5 per cent) and Queensland (20 per cent). Contacts received from the remaining states and territories were below 10 per cent.

The ACCC also received 3959 scam contacts from people based overseas, and a further 170 where their location was not provided.

Australian Capital Territory

Scam contact report levels for the Australian Capital Territory were artificially inflated in 2013 due to it being the default state or territory listed in the SCAMwatch online reporting form. This default option was removed when the ACCC updated the SCAMwatch reporting form at the end of 2013.

Scam category	Contacts	Amount reported lost	Contacts reporting loss	Less than $10k lost	Greater than $10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	1 413	$444 053	121	114	7	1 292	8.6%
Phishing and identity theft	786	$164 665	33	28	5	753	4.2%
Lottery and sweepstakes	631	$643 073	50	43	7	581	7.9%
Computer hacking	530	$38 291	54	54	0	476	10.2%
Online shopping	439	$195 269	174	168	6	265	39.6%
Unexpected prizes	268	$4 965	9	9	0	259	3.4%
Dating and romance	165	$1 641 819	68	47	21	97	41.2%
Job and employment	160	$46 411	14	12	2	146	8.8%
False billing	154	$50 539	11	10	1	143	7.1%
Mobile phone	74	$979	11	11	0	63	14.9%
Spam and 'free' internet offers	61	$2 185	6	6	0	55	9.8%
Computer prediction software	55	$222 825	16	11	5	39	29.1%
Investment	45	$949 362	13	5	8	32	28.9%
Other—scams outside predefined categories	41	$21 308	2	1	1	39	4.9%
Health and medical	31	$3 971	20	20	0	11	64.5%
Door-to-door and home maintenance	19	$114 200	8	7	1	11	42.1%
Chain letter/pyramid scheme	17	$2 600	1	1	0	16	5.9%
Fax back	14	$0	0	0	0	14	0.0%
Psychic and clairvoyant	6	$80 000	1	0	1	5	16.7%
Total	**4 909**	**$4 626 515**	**612**	**547**	**65**	**4297**	**12.5%**

New South Wales

Scam category	Contacts	Amount reported lost	Contacts reporting loss	Less than $10k lost	Greater than $10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	9 317	$7 707 720	871	758	113	8 446	9.3%
Phishing and identity theft	4 836	$532 451	185	175	10	4 651	3.8%
Computer hacking	3 265	$492 011	341	332	9	2 924	10.4%
Online shopping	2 399	$1 385 558	1 100	1 081	19	1 299	45.9%
Lottery and sweepstakes	2 320	$1 801 837	136	108	28	2 184	5.9%
False billing	1 083	$172 159	118	114	4	965	10.9%
Unexpected prizes	1 061	$209 503	53	48	5	1 008	5.0%
Job and employment	826	$444 908	84	75	9	742	10.2%
Dating and romance	721	$7 396 687	321	200	121	400	44.5%
Mobile phone	410	$16 009	91	91	0	319	22.2%
Spam and 'free' internet offers	309	$13 628	37	37	0	272	12.0%
Computer prediction software	259	$1 178 830	86	60	26	173	33.2%
Investment	219	$1 777 392	56	35	21	163	25.6%
Health and medical	178	$22 303	90	90	0	88	50.6%
Other—scams outside predefined categories	141	$52 406	7	6	1	134	5.0%
Chain letter/pyramid scheme	107	$37 326	19	19	0	88	17.8%
Door-to-door and home maintenance	83	$132 176	37	34	3	46	44.6%
Fax back	47	$1 717	1	1	0	46	2.1%
Psychic and clairvoyant	34	$80 974	18	16	2	16	52.9%
Total	**27 615**	**$23 455 595**	**3 651**	**3 280**	**371**	**23 964**	**13.2%**

Northern Territory

Scam category	Contacts	Amount reported lost	Contacts reporting loss	Less than $10k lost	Greater than $10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	208	$104 581	37	34	3	171	17.8%
Phishing and identity theft	118	$30 384	7	6	1	111	5.9%
Online shopping	108	$67 774	53	53	0	55	49.1%
Lottery and sweepstakes	86	$22 607	6	5	1	80	7.0%
Computer hacking	65	$6 040	4	4	0	61	6.2%
False billing	44	$9 767	5	5	0	39	11.4%
Dating and romance	27	$68 847	9	5	4	18	33.3%
Job and employment	23	$53 338	4	3	1	19	17.4%
Unexpected prizes	20	$2 168	2	2	0	18	10.0%
Investment	10	$135 220	5	3	2	5	50.0%
Mobile phone	8	$0	0	0	0	8	0.0%
Health and medical	6	$954	4	4	0	2	66.7%
Computer prediction software	5	$7 500	1	1	0	4	20.0%
Spam and ‘free’ internet offers	5	$0	0	0	0	5	0.0%
Fax back	3	$0	0	0	0	3	0.0%
Other—scams outside predefined categories	3	$0	0	0	0	3	0.0%
Chain letter/pyramid scheme	1	$0	0	0	0	1	0.0%
Door-to-door and home maintenance	1	$0	0	0	0	1	0.0%
Total	**741**	**$509 180**	**137**	**125**	**12**	**604**	**18.5%**

Queensland

Scam category	Contacts	Amount reported lost	Contacts reporting loss	Less than $10k lost	Greater than $10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	5 379	$4 901 196	560	489	71	4 819	10.4%
Phishing and identity theft	2 960	$472 659	111	107	4	2 849	3.8%
Computer hacking	2 274	$138 161	169	167	2	2 105	7.4%
Lottery and sweepstakes	1 827	$505 134	107	99	8	1 720	5.9%
Online shopping	1 780	$1 250 844	703	674	29	1 077	39.5%
False billing	699	$99 060	95	94	1	604	13.6%
Unexpected prizes	674	$154 416	33	30	3	641	4.9%
Dating and romance	551	$4 372 940	221	155	66	330	40.1%
Job and employment	527	$561 420	82	74	8	445	15.6%
Mobile phone	262	$3 347	49	49	0	213	18.7%
Computer prediction software	213	$1 146 343	83	64	19	130	39.0%
Spam and 'free' internet offers	185	$16 465	29	29	0	156	15.7%
Investment	130	$1 447 807	35	25	10	95	26.9%
Other—scams outside predefined categories	98	$558 604	11	9	2	87	11.2%
Health and medical	93	$15 647	55	55	0	38	59.1%
Chain letter/pyramid scheme	69	$58 565	15	14	1	54	21.7%
Door-to-door and home maintenance	59	$36 927	18	17	1	41	30.5%
Fax back	34	$22 000	1	0	1	33	2.9%
Psychic and clairvoyant	29	$43 630	12	11	1	17	41.4%
Total	**17 843**	**$15 805 165**	**2 389**	**2 162**	**227**	**15 454**	**13.4%**

South Australia

Scam category	Contacts	Amount reported lost	Contacts reporting loss	Less than $10k lost	Greater than $10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	1 960	$1 616 493	181	158	23	1 779	9.2%
Phishing and identity theft	1 245	$112 245	52	50	2	1 193	4.2%
Computer hacking	882	$74 972	79	78	1	803	9.0%
Lottery and sweepstakes	791	$522 530	36	31	5	755	4.6%
Online shopping	579	$220 037	243	242	1	336	42.0%
Unexpected prizes	387	$82 664	14	11	3	373	3.6%
False billing	335	$19 697	43	43	0	292	12.8%
Dating and romance	216	$1 565 006	100	77	23	116	46.3%
Job and employment	177	$285 119	23	21	2	154	13.0%
Computer prediction software	90	$316 436	33	25	8	57	36.7%
Mobile phone	85	$2 790	16	16	0	69	18.8%
Spam and 'free' internet offers	81	$3 728	10	10	0	71	12.3%
Investment	65	$86 673	10	8	2	55	15.4%
Other—scams outside predefined categories	41	$967	2	2	0	39	4.9%
Chain letter/pyramid scheme	33	$65 800	1	0	1	32	3.0%
Health and medical	30	$4 299	14	14	0	16	46.7%
Door-to-door and home maintenance	24	$3 349	5	5	0	19	20.8%
Fax back	22	$354	1	1	0	21	4.5%
Psychic and clairvoyant	12	$427	4	4	0	8	33.3%
Total	**7 055**	**$4 983 586**	**867**	**796**	**71**	**6 188**	**12.3%**

Tasmania

Scam category	Contacts	Amount reported lost	Contacts reporting loss	Less than $10k lost	Greater than $10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	606	$198 327	43	36	7	563	7.1%
Phishing and identity theft	348	$2 218	6	6	0	342	1.7%
Computer hacking	302	$11 192	15	15	0	287	5.0%
Lottery and sweepstakes	264	$137 490	20	13	7	244	7.6%
Online shopping	152	$274 533	77	76	1	75	50.7%
Unexpected prizes	128	$1 195	1	1	0	127	0.8%
False billing	92	$13 036	10	10	0	82	10.9%
Dating and romance	62	$337 835	23	16	7	39	37.1%
Job and employment	47	$13 063	11	11	0	36	23.4%
Computer prediction software	31	$56 404	12	12	0	19	38.7%
Spam and 'free' internet offers	26	$825	7	7	0	19	26.9%
Mobile phone	24	$825	5	5	0	19	20.8%
Investment	11	$6 950	4	4	0	7	36.4%
Health and medical	10	$1 267	5	5	0	5	50.0%
Other—scams outside predefined categories	9	$0	0	0	0	9	0.0%
Chain letter/pyramid scheme	9	$3 526	2	2	0	7	22.2%
Fax back	6	$0	0	0	0	6	0.0%
Door-to-door and home maintenance	4	$840	1	1	0	3	25.0%
Psychic and clairvoyant	2	$0	0	0	0	2	0.0%
Total	**2 133**	**$1 059 526**	**242**	**220**	**22**	**1 891**	**11.3%**

Victoria

Scam category	Contacts	Amount reported lost	Contacts reporting loss	Less than $10k lost	Greater than $10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	6 841	$5 656 030	679	599	80	6162	9.9%
Phishing and identity theft	3 013	$535 632	149	133	16	2 864	4.9%
Computer hacking	2 040	$159 214	185	182	3	1 855	9.1%
Lottery and sweepstakes	1 780	$898 549	137	110	27	1 643	7.7%
Online shopping	1 676	$933 098	798	779	19	878	47.6%
Unexpected prizes	826	$235 014	41	34	7	785	5.0%
False billing	752	$226 076	96	90	6	656	12.8%
Job and employment	650	$415 243	71	62	9	579	10.9%
Dating and romance	474	$5 517 085	209	131	78	265	44.1%
Mobile phone	279	$4 618	58	58	0	221	20.8%
Computer prediction software	225	$5 352 428	93	61	32	132	41.3%
Spam and 'free' internet offers	213	$13 272	21	21	0	192	9.9%
Investment	160	$1 464 794	49	28	21	111	30.6%
Other—scams outside predefined categories	123	$45 188	7	6	1	116	5.7%
Door-to-door and home maintenance	117	$22 154	29	29	0	88	24.8%
Health and medical	94	$21 312	55	54	1	39	58.5%
Chain letter/pyramid scheme	79	$8 481	9	9	0	70	11.4%
Fax back	34	$0	0	0	0	34	0.0%
Psychic and clairvoyant	26	$263 078	11	9	2	15	42.3%
Total	**19 402**	**$21 771 266**	**2 697**	**2 395**	**302**	**16 705**	**13.9%**

Western Australia

Scam category	Contacts	Amount reported lost	Contacts reporting loss	Less than $10k lost	Greater than $10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	2 158	$1 491 150	253	233	20	1 905	11.7%
Phishing and identity theft	1 472	$336 564	70	63	7	1 402	4.8%
Lottery and sweepstakes	917	$202 519	41	38	3	876	4.5%
Computer hacking	842	$116 239	71	69	2	771	8.4%
Online shopping	833	$388 064	384	379	5	449	46.1%
False billing	385	$43 597	35	35	0	350	9.1%
Unexpected prizes	347	$84 733	24	23	1	323	6.9%
Job and employment	263	$609 230	39	34	5	224	14.8%
Dating and romance	241	$2 280 828	97	62	35	144	40.2%
Mobile phone	138	$3 120	23	23	0	115	16.7%
Investment	107	$1 421 243	28	17	11	79	26.2%
Spam and 'free' internet offers	102	$6 956	17	17	0	85	16.7%
Computer prediction software	99	$758 091	47	32	15	52	47.5%
Health and medical	72	$13 426	40	40	0	32	55.6%
Other—scams outside predefined categories	48	$10 950	6	6	0	42	12.5%
Chain letter/pyramid scheme	37	$3 617	4	4	0	33	10.8%
Door-to-door and home maintenance	19	$7 139	10	10	0	9	52.6%
Fax back	11	$0	0	0	0	11	0.0%
Psychic and clairvoyant	9	$5 589	2	2	0	7	22.2%
Total	**8 100**	**$7 783 055**	**1 191**	**1 087**	**104**	**6 909**	**14.7%**

Appendix 2: 2013 SCAMwatch radars

Beware bogus bushfire appeals—scammers also appeal to your generous side

January 2013: SCAMwatch is urging consumers considering donating to help those affected by the summer bushfires to make sure that their money goes to a legitimate charity, cause or appeal.

Protect your wallet and your heart this Valentine's Day

February 2013: SCAMwatch is warning those looking for love online not to fall for scammers this Valentine's Day.

Think carefully about unsolicited offers to register domain names overseas

February 2013: SCAMwatch is warning businesses to treat with caution unsolicited invitations to register or renew internet domain names in China and other countries.

Police scareware scam continues to target Australians

March 2013: SCAMwatch is urging people to continue to be alert to a scareware scam where scammers posing as the Australian Federal Police (AFP) try to scare you into handing over money to regain control of your computer.

Penalties handed down against operators of charity publications scam targeting small businesses

March 2013: The operators behind a scam targeting small businesses with false claims about advertising services for publications with a philanthropic slant have been ordered to pay $75 0000 in penalties following court action by the Australian Competition and Consumer Commission (ACCC).

Beware of scammers taking advantage of the Boston marathon tragedy

April 2013: SCAMwatch is warning consumers to be alert to scammers looking to take advantage of the Boston marathon explosions with malware or donation scams.

Pause to avoid a puppy scam

April 2013: Looking for a furry friend? Watch out—scammers continue to use cute and cuddly canines to pull on people's heart strings and get them to part with their money.

Watch out when booking your winter getaway

May 2013: SCAMwatch is warning consumers to be wary when making plans for a holiday escape this winter.

Don't let your heart be blackmailed

July 2013: SCAMwatch is again warning those looking for love online to stay on the lookout for scammers.

Beware of immigration scams

July 2013: SCAMwatch and the Department of Immigration and Citizenship are warning people who have migrated to Australia or are currently temporary visa holders to be cautious of immigration-related scams.

Small businesses beware—'Yellow Pages' directory scam strikes again

August 2013: SCAMwatch is warning small businesses to be alert as the fake 'Yellow Pages' business directory scam has resurfaced in Australia.

This end of financial year, look out for tax refund phishing scams

August 2013: SCAMwatch and the Australian Taxation Office (ATO) are urging consumers and small businesses to be aware of tax refund email scams, with scammers taking advantage of the busy nature of tax time to target you.

Beware of scam surveys and fake free offers

September 2013: SCAMwatch is reminding people to beware of online scams—surveys, emails and social-media posts—offering fake gift vouchers or other bogus inducements in return for disclosing credit card and other personal information.

Beware of fake charities

October 2013: SCAMwatch and the Australian Charities and Not-for-profits Commission (ACNC) are reminding people to beware of scammers pretending to represent a charity or not-for-profit organisation.

Don't back a scammer this spring racing season

October 2013: SCAMwatch is reminding punters not to be fooled by con artists pushing sports investment scams this spring racing season.

Beware fake websites when shopping online for Christmas

November 2013: SCAMwatch is warning consumers shopping online for Christmas to watch out for fake websites selling bogus gifts.

Don't let scammers take advantage of the Anzac spirit

November 2013: With 2015 marking the 100th anniversary of the Gallipoli campaign, the Australian and New Zealand governments have launched a ballot for attendance at Anzac Day commemorations at Gallipoli.

Don't let scammers ruin your Christmas

December 2013: With only days until Christmas, SCAMwatch is warning consumers to watch out for fake delivery scams arriving in your inbox or letter box.

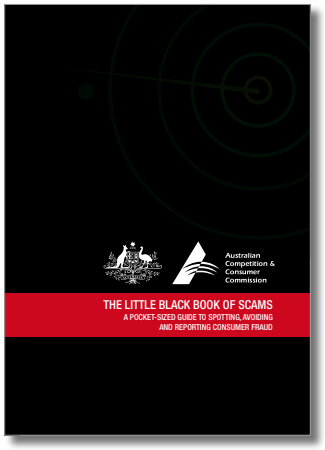
Appendix 3: ACCC scam-related resources for consumers and businesses

SCAMwatch

SCAMwatch website (www.scamwatch.gov.au)

SCAMwatch Twitter profile (@SCAMwatch_gov)

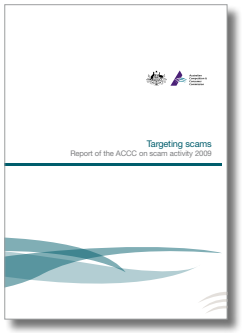
Publications

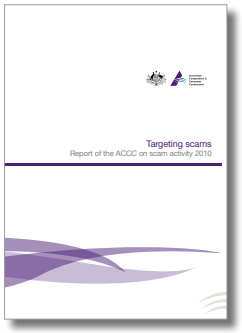


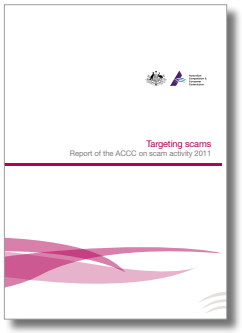
The *Little Black Book of Scams*

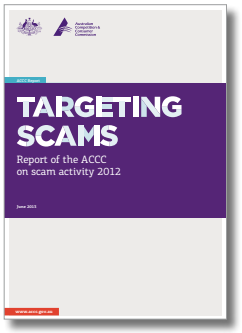
ACCC Small business scams factsheet

Annual reports









Targeting scams: Report of the ACCC on scam activity—2009, 2010 and 2011 editions

2013 Fraud Week campaign resources

Campaign web button

Campaign image

Campaign web banner

Appendix 4: Australasian Consumer Fraud Taskforce members and partners

Taskforce members

Australian Government

Attorney-General's Department

Australian Bureau of Statistics

Australian Communications and Media Authority

Australian Competition and Consumer Commission (Chair)

Australian Federal Police

Australian Institute of Criminology

Australian Securities and Investments Commission

Australian Taxation Office

Department of Communications

New Zealand Government

New Zealand Commerce Commission

New Zealand Ministry of Consumer Affairs

State and territory governments

Australian Capital Territory Office of Fair Trading

Consumer Affairs and Fair Trading, Department of Justice Tasmania

Consumer Affairs Victoria

Department of Commerce Western Australia

Fair Trading Queensland

Northern Territory Consumer Affairs

New South Wales Fair Trading

Office of Consumer and Business Affairs SA

Representatives of the state and territory police

New South Wales Police Service

Queensland Police Service

Northern Territory Police Force

State and Territory Police Commissioners

2013 Taskforce partners

Consumer advocacy (general)

CHOICE

Consumers Federation of Australia

Public Interest Advocacy Centre

Legal centres/associations

Consumer Action Law Centre

Indigenous Consumer Assistance Network

National Association of Community Legal Centres

Peninsula Community Legal Centre

Financial institutions and services

Abacus—Australian Mutuals

Adelaide Bank

Altura Financial Planning

ANZ

Association of Independent Retirees

Association of Superannuation Funds Australia

Australian Bankers' Association

Australian National Audit Office

Australian Super

Bankwest

Bendigo Bank

Commonwealth Bank

ComSuper

Financial and Consumer Rights Council Victoria

Financial Services Council

MoneyGram International

National Australia Bank

PayPal Australia

SunCorp-Metway

The Westpac Group

Western Union

Online shopping service providers

Cars Guide

Carsales.com.au

Deals Direct

eBay Australia

GraysOnline

Gumtree

National Online Retailers Association

Trading Post

Trustedwebsites.com.au

Small business bodies/associations

Australian Motor Industry Federation

Australian Retailers Association

Business Enterprise Centres Australia

Chamber of Commerce Northern Territory

Council of Small Business of Australia

Institute of Public Accountants

Liquor Retailers Australia

Master Builders Australia

Master Grocers Australia

National Independent Retailers Association

Real Estate Institute Australia

Tasmanian Small Business Council

The Institute of Chartered Accountants of Australia

The Pharmacy Guild Australia

Gaming bodies

Australian Casino Association

Australian Gaming Council

Betfair

Tabcorp

Ombudsman services

Commonwealth Ombudsman

Energy and Water Ombudsman of NSW

Energy and Water Ombudsman of Victoria

Fair Work Ombudsman

Financial Ombudsman Service

Insurance Ombudsman Service

Telecommunications Industry Ombudsman

Social/welfare/community bodies

Alexandra District Hospital

Australian Charities and Not-for-profits Commission

Australian Federation of Disability Organisations

Banyule Community Health

Better Hearing Australia Victoria Incorporated

Brotherhood of St Laurence

Citizens Advice Bureau (ACT)

Comcare

Community Connections Victoria

Country Women's Association of Australia

Cranbourne Information and Support Service

CRS Australia

Department of Human Services

Diamond Valley Community Support

Federation of Ethnic Communities Council of Australia

Financial Counselling Australia

Laverton Community Centre

Mental Health Council of Australia

Neighbourhood Watch Victoria

Otway Health and Community Services

Sane Australia

Social Securities Appeal Tribunal

Wesley Mission

Western Australia Council of Social Services Incorporated

Whittlesea Community Connections

Online dating services

3H Group Pty Ltd—OasisActive.com

eHarmony Australia

Slinky Dating Australia Ltd

Seniors associations

Australian Council of Social Services

Australian Seniors Computer Clubs Association

Council on the Ageing—ACT

Council on the Ageing—NT

Council on the Ageing—Qld

Council on the Ageing—SA

Council on the Ageing—Tas

Council on the Ageing—Vic

Council on the Ageing—WA

Council on the Ageing Australia

RSL NSW

RSL SA

RSL Tas

RSL Vic

RSL WA

Seniors Information Victoria

Internet security and computer bodies

auDA

AusCERT

Australian Computer Society

AVG Technologies AU

Centre for Internet Safety at the University of Canberra

Community Technology Centres Association

Internet Industry Association

Internet Society of Australia

Microsoft

National Online Retailers Association

Norton by Symantec

Sophos

Surete Group

Yahoo

Telecommunications service providers (including VOIP)

Australian Communications Consumer Action Network

Australian Mobile Telecommunications Association

Communications Alliance

Optus

Telstra

Miscellaneous

Ailean

Australia Post

Australian Federal Police

Australian Trade Commission

Crime Stoppers Australia

Curtin University of Technology

Migration Review Tribunal

National Archives of Australia

Office of the Australian Information Commissioner

Qantas

REA Consultancy

Refugee Review Tribunal (RRT)

SettleBox

Tenants Union of Victoria

The Newspaper Works

The Strategy Helix