ACCC Report

TARGETING SCAMS

Report of the ACCC on scam activity 2012

June 2013

Foreword

Delia Rickard

The Australian Competition and Consumer Commission's (ACCC) fourth annual scams report shows that Australians continue to be targeted by a significant level of scams activity, with nearly 84 000 scam-related contacts received by the ACCC in 2012.

The impact of scams on Australian society continues to be substantial, with consumers and businesses suffering considerable financial and non-financial losses. In 2012 just over $93 million was reported lost as a result of scams; indeed, this figure is likely to be much higher as victims often do not report their experiences for a variety of reasons, including a sense of embarrassment from being duped. They may also report their experience to the many other agencies that play an important role in helping victims. The ACCC also continues to hear devastating stories about the emotional toil that scams have on victims—an unquantifiable loss.

As with 2011, scams delivered via phone continued to be the preferred method of delivery in 2012—in total, 56 per cent of reported scams were delivered via telephone calls and text messages, with combined financial losses estimated to be nearly $25 million.

Online shopping scam reports also increased by 65 per cent to over 8000 contacts and more than $4 million in reported losses. This increase is likely to reflect the fact that more Australians are shopping online. Unfortunately, scammers like shopping online too—for victims. The Australasian Consumer Fraud Taskforce's (ACFT) 2013 Fraud Week campaign, 'Outsmart the scammers!', will focus on raising public awareness about how to buy and sell safely online without being duped.

The ACCC undertakes a range of work to protect consumers against scams activity. Both the SCAMwatch website and *Little Black Book of Scams* are regarded internationally as best practice resources, with overseas regulators linking to the site and producing their own localised versions of the book. In 2012 SCAMwatch received over 970 000 unique visitors, up 25 per cent from 2011, and over 125 000 copies of the book were distributed for free.

The ACCC also works extensively with industry, other regulators, and local and international law enforcement agencies to disrupt scams. On Valentine's Day 2012 the ACCC launched voluntary guidelines, developed in collaboration with an industry working group, to help online dating and romance service providers better protect users from scams occurring on these platforms. As chair of the ACFT, the ACCC also continues to lead a coordinated effort by government to minimise the harm arising from scams.

On the enforcement side, the ACCC successfully prosecuted individuals engaging in pyramid selling schemes, and schemes targeting small business operators to falsely sign them up to buy advertising services. The ACCC also assisted the Essex Police obtain evidence from an Australian victim of a global scam, for which some of the perpetrators were subsequently sentenced to jail and some money was returned to victims.

In a time when it can take just the click of a button to fall victim to a scam, it is more important than ever that we practice safe techniques when communicating with others—whether online, on the phone, at one's business or even at home. We hope that this report will raise awareness about the extent of scams activity in Australia, and the need for Australians to protect themselves and avoid victimisation in the first instance.

Delia Rickard

Deputy Chair, Australian Competition and Consumer Commission

Chair, Australasian Consumer Fraud Taskforce

Contents

ISBN 978 1 921973 62 8

Australian Competition and Consumer Commission
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 06/13_691

www.accc.gov.au

1 Snapshot of 2012

Scam reports

- In 2012 the ACCC continued to observe a high level of scams activity in Australia, with 83 803 scam-related contacts received from consumers and small businesses.
- Estimated scam losses reported to the ACCC totalled $93 423 030, a nine per cent increase from 2011. 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.
- Similar to 2011, the majority of consumers and small businesses contacting the ACCC about scam-related activities in 2012 (nearly 88 per cent) reported no financial loss. The most common category of loss was again between $100 to $499. This indicates the continued use of 'high volume scams', which 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 very high losses.

Most reported scams

- For the fourth consecutive year, advance fee/up-front payment scams were the most commonly reported scam type, constituting 32 per cent of all scam contacts.
- Computer hacking remained the second most reported scam type in 2012, representing just over 13 per cent of total scam reports to the ACCC. The 'Microsoft' computer virus scam continued to heavily target Australians. The public was also targeted by a scareware scam where the perpetrators pretended to be from the Australian Federal Police.
- Online shopping scams increased by 65 per cent with reported financial losses totalling $4 038 479.
- The ACCC also received a high level of contacts about banking and online account scams, false billing, job and employment scams, dating and romance, and unexpected prize scams.

Age range and location demographics

- In 2012 scams were most commonly reported by persons in the 35 to 44 age category, representing 32 per cent of contacts. This saw a shift from the previous year, where contacts were spread across a wider range of age from 25 through to 54 years.
- The greatest amounts of scam reports to the ACCC came from New South Wales (23.5 per cent), Queensland (21 per cent), Victoria (18 per cent) and South Australia (12.5 per cent).

Scam delivery method

- Scams delivered via telephone (landline and mobile) remained the preferred delivery method in 2012, with combined voice and text message scams constituting over half (56 per cent) of all reports to the ACCC. Unsolicited telephone calls represented just over 42 per cent (35 419) of contacts reported to the ACCC, accounting for $24 213 979 in reported losses. Scams delivered via SMS represented over 14 per cent (11 797) of total contacts and $759 986 in reported losses.

The ACCC's education and awareness raising activities

- The ACCC continued its efforts to help Australians protect themselves by learning how to identify and avoid scams. In 2012 the SCAMwatch website received 971 824 unique visitors, an increase of approximately 25 per cent from 2011. The SCAMwatch Twitter account increased its followers by 58 per cent.
- The 2012 Fraud Week campaign, 'Slam Scams!' (19–25 March), saw a surge in visitors to SCAMwatch and generated unprecedented media coverage as the ACCC and the Australasian Consumer Fraud Taskforce urged the public to 'slam a scam at the point of contact: press delete, throw it out, shut the door or just hang up'.
- In March 2012 the ACCC launched a pocket-sized edition of *The Little Black Book of Scams*, its most popular publication. By the end of the year 127 825 copies had been distributed.

The ACCC's collaboration, scam disruption and enforcement activities

- In 2012 the ACCC continued to work extensively with industry and government to protect the public from scams. The ACCC worked with the online dating industry to develop voluntary best practice guidelines to help dating websites and their users respond to scams occurring on these platforms. The ACCC continued to chair the Australasian Consumer Fraud Taskforce and hosted a storytelling event where representatives from the public and private sectors shared their experiences with scams.
- The ACCC also successfully prosecuted individuals engaging in pyramid selling schemes, and schemes targeting small business operators to falsely sign them up to buy advertising services. The ACCC also assisted the Essex Police in obtaining evidence from an Australian retiree who had fallen victim to a global scam. A UK court subsequently sentenced two defendants involved in money laundering aspects of the scam.

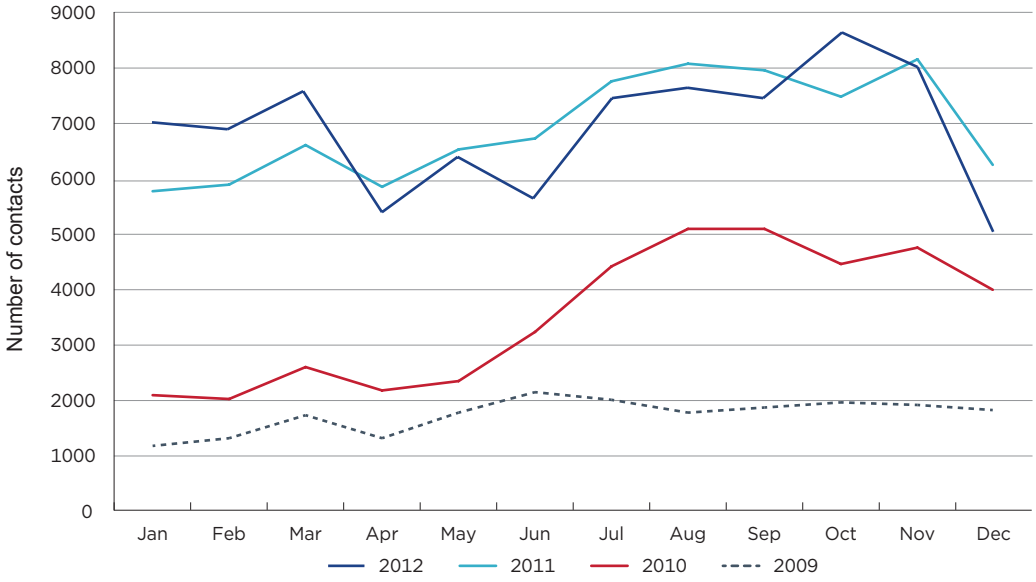
2 Contacts and trends

2.1 Scam reports and inquiries received by the ACCC

From 1 January to 31 December 2012 the ACCC received 83 803 scam-related contacts (82 549 complaints and 1254 inquiries).

This report is based solely on scam-related contacts to the ACCC and therefore provides only part of the picture in terms of the scale of scams activity in Australia. While the ACCC is one of the primary Australian government reporting agencies for scams, there are many other agencies that also play an important role in helping scam victims, including local consumer protection and law enforcement agencies. 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 occurred. Finally, many scam victims may be too embarrassed to report their experience.

Figure 1: Number of scam-related contacts to the ACCC 2009–12



Scam delivery methods

Scams are delivered in a variety of ways, with perpetrators continually adapting their method of approach to take advantage of rapid developments in technology and how communication channels are used.

Table 1 provides a comparison of all scam delivery methods reported to the ACCC in 2012 and 2011, and highlights that scams delivered by phone (telephone calls and text message) remained the most popular method of targeting the public. Online methods of delivery (internet and email) were also used more often in 2012 to target Australians compared to previous years.

Table 1: Scam delivery methods during 2012 and 2011

	2012		2011	
Scam delivery method	**Number**	**Percentage**	**Number**	**Percentage**
Telephone call	35 419	42.3%	42 977	51.7%
Email	19 478	23.2%	15 080	18.1%
Text message	11 797	14.1%	8 264	9.9%
Internet	10 003	11.9%	8 698	10.5%
Mail	5 912	7.1%	6 508	7.8%
In person	764	0.9%	580	0.7%
Fax	430	0.5%	159	0.2%
Other[1]	NA	NA	884	1.1%
Total	**83 803**	**100%**	**80 150**	**100%**

Scams delivered by phone (landline and mobile)

In 2012 unsolicited telephone calls remained the most popular scam delivery method reported to the ACCC. Just over 42 per cent of reported scams were delivered by this mode (35 419 contacts), with reported losses totalling $24 213 979. Although unsolicited telephone calls remained the most popular scam approach, reports fell by more than 17 per cent from 2011, with an associated drop in reported losses of $3 559 750.

Scams delivered via text message constituted just over 14 per cent of scam-related contacts to the ACCC, an increase of just over four per cent from 2011. Reported losses totalled $759 986, a marked decrease of 37 per cent ($447 150) from the previous year. This may be attributed to five reports in 2011 where losses were over $100 000. In 2012, no reports of mobile phone scams reached this threshold, with the largest reported loss being approximately $80 000. This increase in scams delivered via SMS corresponds to mobile phone scams entering into the top 10 reported scams for 2012.

The most prominent scams delivered via telephone calls were advanced fee/upfront payment, computer hacking, unexpected prizes, sweepstakes and lottery, and phishing and identity theft scams. The vast majority of scams delivered via text message related to premium SMS services for competitions, ringtones or games, and fake lotteries.

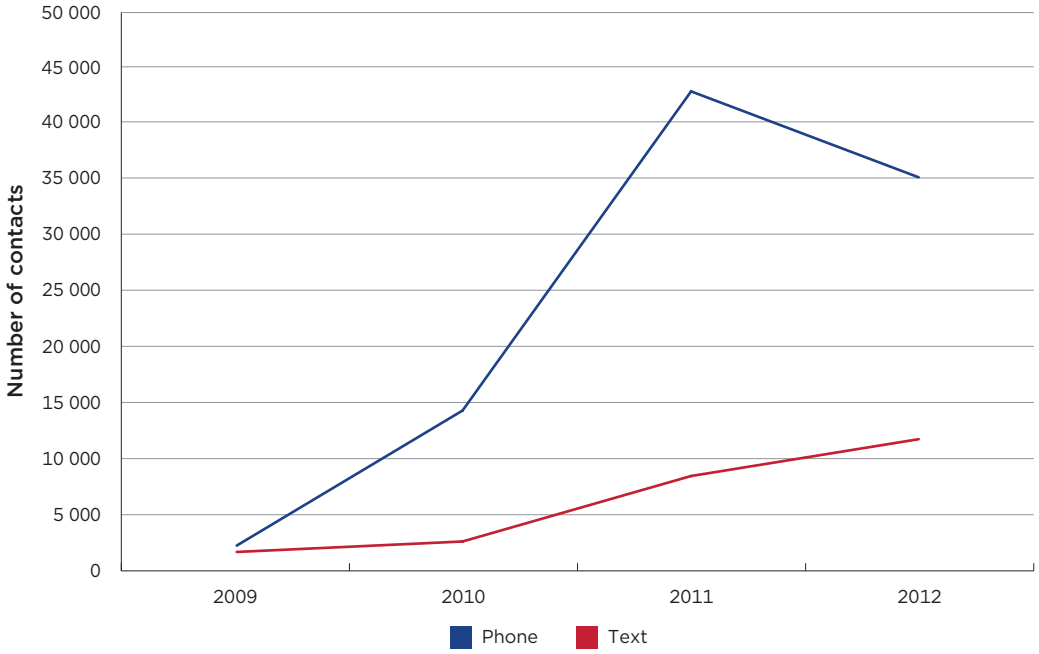
For both types of phone delivery methods, scam callers often pretended to be from government or large well-known companies including banks, computer companies, telecommunications service providers and lottery agencies.

Similar to previous years, the ACCC continued to receive reports that indicate many telephone scams may be operating through overseas call centres. This could be due to the continued outsourcing by criminal networks of unsolicited telephone activities to cheap overseas providers, as well as the growing availability of low or no-cost VoIP call services. This scam is usually directed at the home telephone and it is almost exclusively reported to the ACCC as a telephone scam. The ACCC therefore categorises scams delivered through VoIP as a telephone delivery method.

Figure 2 shows the increase in scams delivered via a telephone call or SMS since 2009.

1 In 2011 the ACCC categorised some scam contacts (1.1 per cent) as 'other'. This category was removed in 2012.

Figure 2: Scams delivered via telephone (voice and text message) 2009–12



Scams delivered online (internet and email)

The ACCC also observed an increase in scams delivered online (including via internet and email) of 6.5 per cent to represent just over 35 per cent of all scam approaches. The ACCC received 10 003 reports of scams delivered via the internet and 19 478 reports of scams delivered via email, increases of 1 and 5 per cent respectively.

Total reported losses increased by 21.5 per cent to $52 234 283, or $27 875 141 for scams delivered via the internet and $24 359 142 for scams delivered via email.

Online scams are designed to take advantage of the anonymous and instantaneous nature of the internet, with many victims only realising that they have been scammed when their credit card statement or other invoices arrive.

Scammers often take advantage of consumers' trust in popular and well-established online communications channels. For instance, scammers often pose online as legitimate sellers or buyers on auction and shopping sites, or try to 'befriend' victims on social networking forums.

As with scams delivered via phone, scammers also masquerade online as well-known organisations. A phishing email scam, where a scammer is 'fishing' for the recipient's personal details, often appears to come from a trusted entity such as a bank or financial institution. Scammers create mirror or fake websites that are effectively a copy of a legitimate website with a slightly different web address. Scammers also use emails, fake or corrupted sites and false pop-up alerts to deliver malicious software that can infect computers and allow access to information stored on the hard drive.

The ongoing and rapid evolution of mobile-enabled technology and communication channels means that new scams will continue to emerge online, increasing the need for the public to learn how to avoid victimisation. The Australasian Consumer Fraud Taskforce's 2013 Fraud Week campaign, 'Outsmart the scammers!', will focus on raising public awareness about how to buy and sell safely online without being duped (see section 6.1).

Age range and location demographics

Age range

While the provision of information on one's age is voluntary, in 2012 the ACCC received 21 116 scam-related contacts where an individual provided their age. Contrary to popular stereotypes, young people and the elderly were not overrepresented in contacts, with the under 25 and over 64 year age groups comprising only 7 and 10.5 per cent of contacts respectively.

Table 2 provides a comparison of these contacts between 2012 and 2011, which shows that the percentage of individuals contacting the ACCC under 18 and in the 55 to 64 age category remained almost stable from 2011 levels. The percentage of individuals reporting their age in the 35 to 44 years of age category increased by over 11 per cent to comprise just under one third of contacts. In all other age groups, contact levels decreased.

Table 2 also provides a comparison of scam conversion rates by age range. The conversion rate is the likelihood that a scam contact will result in the loss of money.

Whilst people under 18 years of age are less likely to report a scam to the ACCC, in 2011 they had the highest conversion rate of all groups at 40 per cent in 2012. The fact that reported losses for this group are proportionately higher than all other groups may suggest a greater level of susceptibility. This could also reflect the increasing use by scammers of communication channels popular with young people such as mobile phones and the internet, indicating a need for further efforts to educate young people on how to identify and avoid scams.

Table 2: Comparison of age ranges provided by consumers reporting scams to the ACCC in 2012 and 2011

Age range	Number	Percentage	Variance from 2011	Conversion rate
<18	180	0.9%	0.2	40%
18–24	1 203	5.7%	–2.4	26%
25–34	3 309	15.7%	–4.8	20%
35–44	6 805	32.2%	11.2	16%
45–54	4 096	19.4%	–1.8	16%
55–64	3 302	15.6%	–0.5	13%
>64	2 221	10.5%	–1.8	10%
Total	**21 116**	**100%**	**N/A**	**N/A**

Geographic location

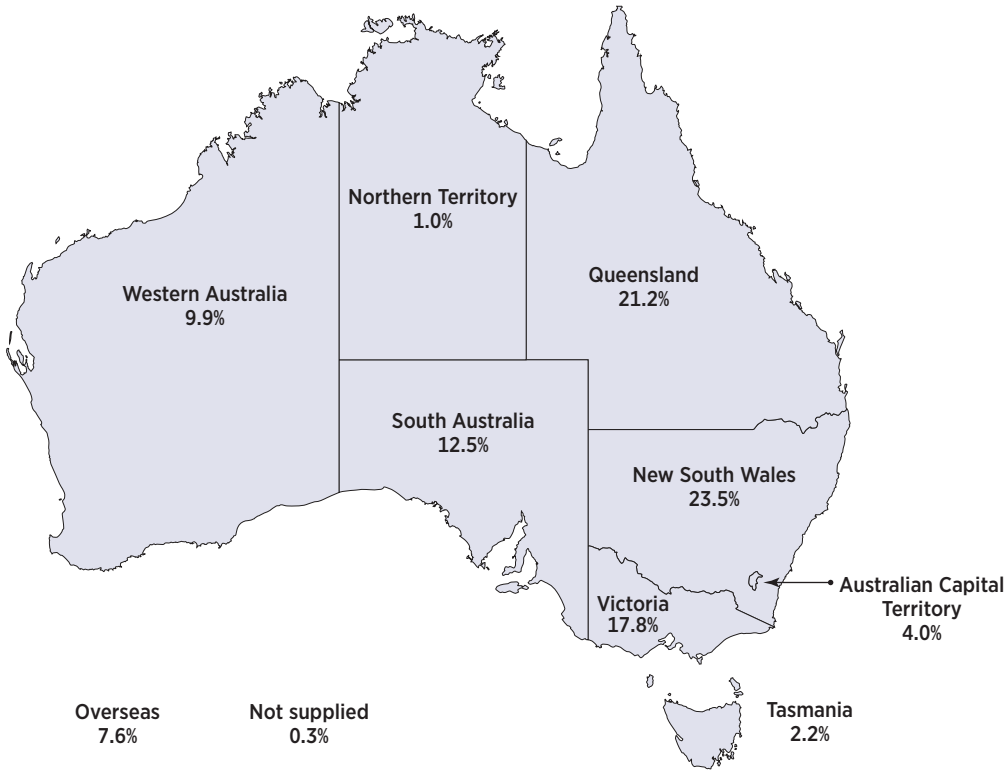
Where possible the ACCC also collects data about the geographic location of people reporting scams.

Figure 3 shows a comparison of contacts received by the ACCC in 2012 broken down by state and territory. New South Wales saw the greatest amount of scam reports (23.5 per cent), followed by Queensland (21 per cent), Victoria (18 per cent) and South Australia (12.5 per cent). Contacts received from the remaining state and territories were below 10 per cent.

The ACCC also received reports from overseas, with 8 per cent of total contacts identified as originating from individuals based outside Australia.

In 2012 the Australian Bureau of Statistics also released the results of its 2010–11 survey into personal fraud (including scams), which includes an analysis of victim exposure for personal fraud more broadly—see chapter 4.

Figure 3: Comparison of scam contacts' location by state and territory 2012



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

2.2 Financial losses reported to the ACCC

In 2012 reports of financial losses arising from scam activity totalled $93 423 030, a 9 per cent increase on the amount reported in 2011. This is a much smaller increase compared to what was seen from 2010 to 2011, where reported losses increased by 35 per cent.

It is important to note that this amount is based on information provided to the ACCC by complainants. As such, it does not represent the actual total financial loss to Australians caused by scams in 2012. The ACCC considers that the figure represents only a proportion of total losses—many scams go unreported and the ACCC is only one of many agencies that receive scam complaints.

In 2012 the number of consumers contacting the ACCC about scams who reported no financial loss remained stable at 87 per cent. The remaining 13 per cent reported losses ranging from very small amounts for unsolicited credit card deductions and 'free' online offers to $3.5 million reported lost to an inheritance scam.

Table 3 provides a breakdown and comparison of the financial losses reported in 2012 and 2011. The data shows an increase in 'high volume scams' for the second year in a row. 'High volume scams' request small amounts of money but target a large number of recipients and typically cause smaller amounts of loss per victim. Reported financial losses between $1 million and $10 million doubled from three reports in 2011 to six reports in 2012. As in 2011, the most commonly reported loss range in 2012 was from $100 to $499. The ACCC recognises that some reported losses may represent amounts that complainants believe they would have been entitled to if the offer were genuine.

Counting the costs—the tip of the iceberg

Reports of financial losses to the ACCC are just the tip of the iceberg as victims of scams are often too embarrassed to report their experience. In April 2012 the Australian Bureau of Statistics' *Personal fraud survey 2010–11* found that Australians lost an estimated $1.4 billion to personal fraud (which includes credit card fraud, identity theft, and scams).[2]

Consumer fraud comes with a high cost in both financial and non-financial terms. The financial repercussions of scams on individuals can range from a few dollars to losing one's life savings or house. Individuals may also suffer adverse effects on their mental health, work capacity, relationships and family.

Businesses can also lose significant revenue to scams activity, either directly as victims, indirectly through scammers impersonating them, or in costs associated with ongoing monitoring and security upgrades.

Scammers are also increasingly impacting on companies, organisations and government departments through the misuse of consumers' trust in brands, reputations and authority.

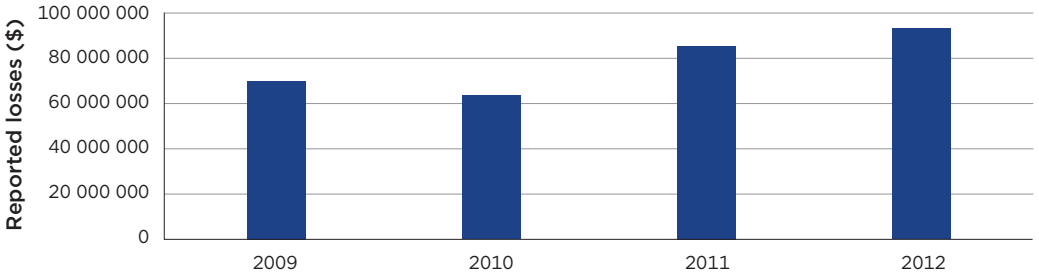
2 Australian Bureau of Statistics, *Personal fraud survey 2010–11*, Canberra, April 2012.

Table 3: Comparison of scam-related monetary losses reported to the ACCC in 2012 and 2011

Losses	Number of people reporting this loss amount in 2012	Percentage	Variance from 2011
1–99	1 761	16.7%	+426
100–499	3 390	32.1%	–96
500–999	1 574	14.9%	+264
1 000–9 999	2 640	25.0%	–56
10 000–49 999	854	8.1%	–11
50 000–499 999	327	3.1%	+8
500 000–999 999	20	0.2%	+6
1 millon–10 million	6	0.1%	+3
Total	**10 572**	**100%**	**N/A**

Figure 4 shows continued growth in scam-related losses reported to the ACCC from 2010 onwards.

Figure 4: Reported losses to the ACCC 2009–12



2.3 Most reported scams

Overview of scams reported to the ACCC in 2012

In 2012 the ACCC continued to receive contacts about a wide range of scams targeting Australians.

Table 4 (see following page) provides an overview of all scam types reported to the ACCC in 2012. The top three scam categories were the primary source of money lost, with advanced fee/up-front payment, dating and romance, and investment seminar and real estate scams accounting for over 75 per cent of reported financial losses.

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

Conversion rates

As with scam contact levels, the overall scam conversion rate remained relatively stable with a slight increase from 12 per cent in 2011 to 13 per cent in 2012. The relatively low percentage of people reporting a financial loss suggests that the public is generally alert to scam activity and how they can protect themselves, and reflects the success of the concerted efforts of the ACCC and many other agencies to engage with and educate the wider community about scam activity.

As previously noted, scam reports to the ACCC are just the tip of the iceberg as there are many other agencies where consumers report scams and seek assistance. Further, 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.

Some categories achieve very high conversion rates and may highlight a particular vulnerability of consumers to these types of scams. A high conversion rate is therefore an indicator of where the ACCC might best direct it resources.

In 2012 almost 46 per cent of people who responded to an approach by a dating and romance scammer reported a financial loss. A total of $23 311 211 was reported lost to dating and romance scams in 2012, making it the second highest category for financial losses despite representing just under three per cent of total scams reported throughout the year. The high conversion rate for dating and romance scams was a clear indicator of where efforts should be directed and in 2012 the ACCC worked with industry to develop voluntary guidelines on how to better protect users from these scams (see chapter 5).

Other scam types that have high conversion rates include computer prediction software, health and medical scams, and online auction and shopping scams. Figure 5 represents the differences in conversion rates between 2011 and 2012 and shows an increase in the conversion rates for computer prediction software, computer hacking and door to door/home maintenance scams. Categories showing a drop in the conversion rate include investment seminars and real estate scams, psychic and clairvoyant scams, and fax back scams.

Quantifying the losses

The conversion rate indicates which scam types are most likely to entrap victims. It shows the percentage of people that report a loss as opposed to those that recognise the scam and simply report it. The conversion rate may therefore indicate 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.

Table 4: Overview of scam types reported to the ACCC in 2012 in order of total reported financial losses

Scam category	Amount reported lost	Contacts	Contacts reporting loss	Less than 10k lost	Greater than 10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	$30 203 373	27 039	2 362	2 056	304	24 677	8.7%
Dating and romance (incl. adult services)	$23 311 211	2 441	1 119	773	346	1 322	45.8%
Investment seminars and real estate	$17 349 347	762	248	130	116	514	32.4%
Online auction and shopping (incl. classifieds)	$4 038 479	8 275	3 038	2 949	89	5 237	36.7%
Computer prediction software (incl. betting)	$4 033 442	733	343	211	132	390	46.8%
Job and employment	$2 704 235	2 673	294	247	47	2 379	11.0%
Lottery and sweepstakes	$2 618 835	9 337	260	214	46	9 077	2.8%
Phishing and identity theft (incl. banking and online account)	$1 503 958	8 788	494	458	40	8 294	5.6%
Computer hacking (incl. malware and viruses)	$1 312 794	10 961	1 013	1 001	12	9 948	9.2%
Unexpected prizes	$1 057 378	5 942	184	165	19	5 758	3.1%
False billing	$566 061	2 546	485	474	11	2 061	19.0%
Psychic and clairvoyant	$444 895	125	41	34	7	84	32.8%
Chain letter/pyramid scheme	$427 014	640	45	34	11	595	7.0%
Mobile phone (ringtones, competitions and missed calls)	$367 739	1 302	269	266	3	1 033	20.7%
Door-to-door and home maintenance	$192 769	364	77	71	6	287	21.2%
Health and medical	$58 076	173	77	76	1	96	44.5%
Spam and 'free' internet offers	$26 574	687	114	114	0	573	16.6%
Fax back	$1 820	64	1	1	0	63	1.6%
Other (scams that do not fit into predefined categories)	$3 205 030	951	108	91	17	843	11.4%
Total	**$93 423 030**	**83 803**	**10 572**	**9 365**	**1 207**	**73 231**	**12.6%**

Figure 5: Conversion rates by scam category 2011–12

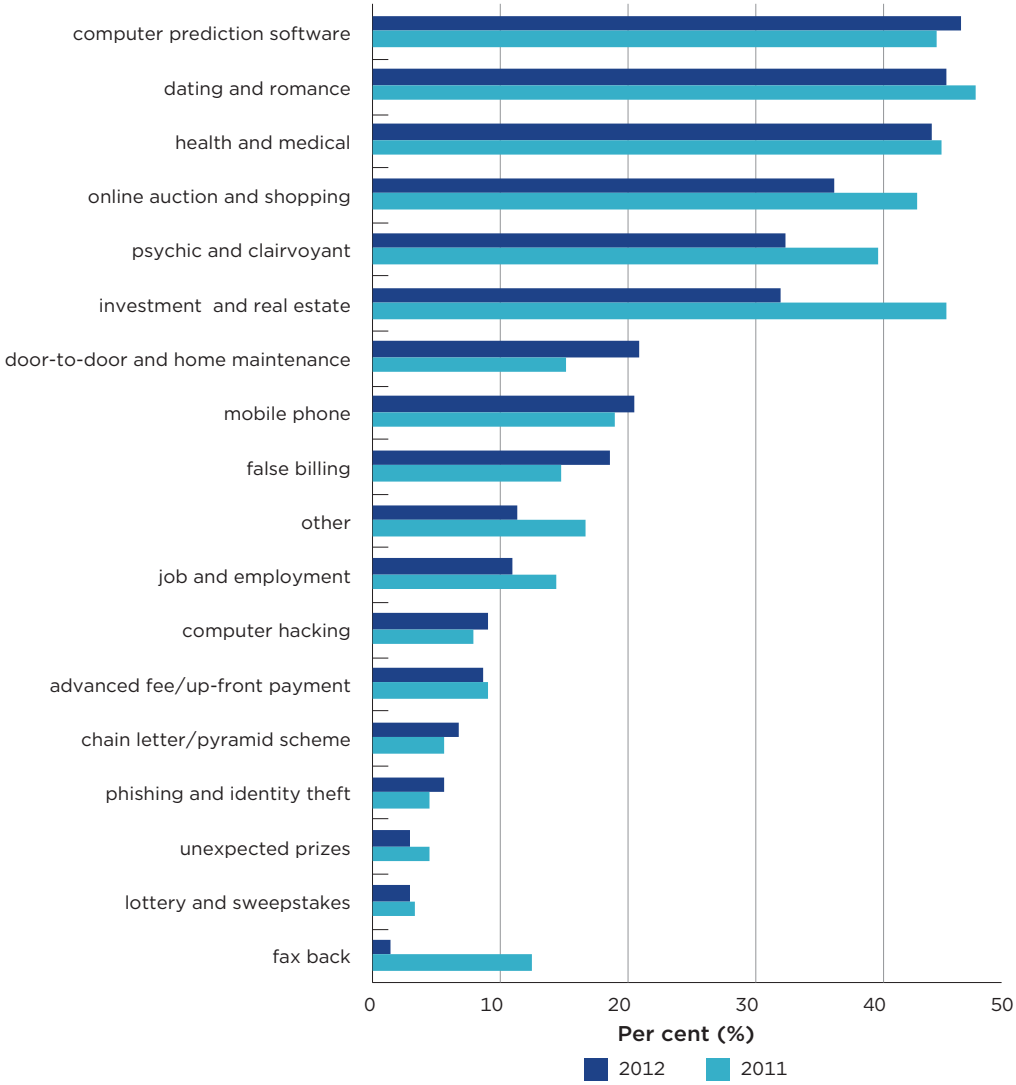
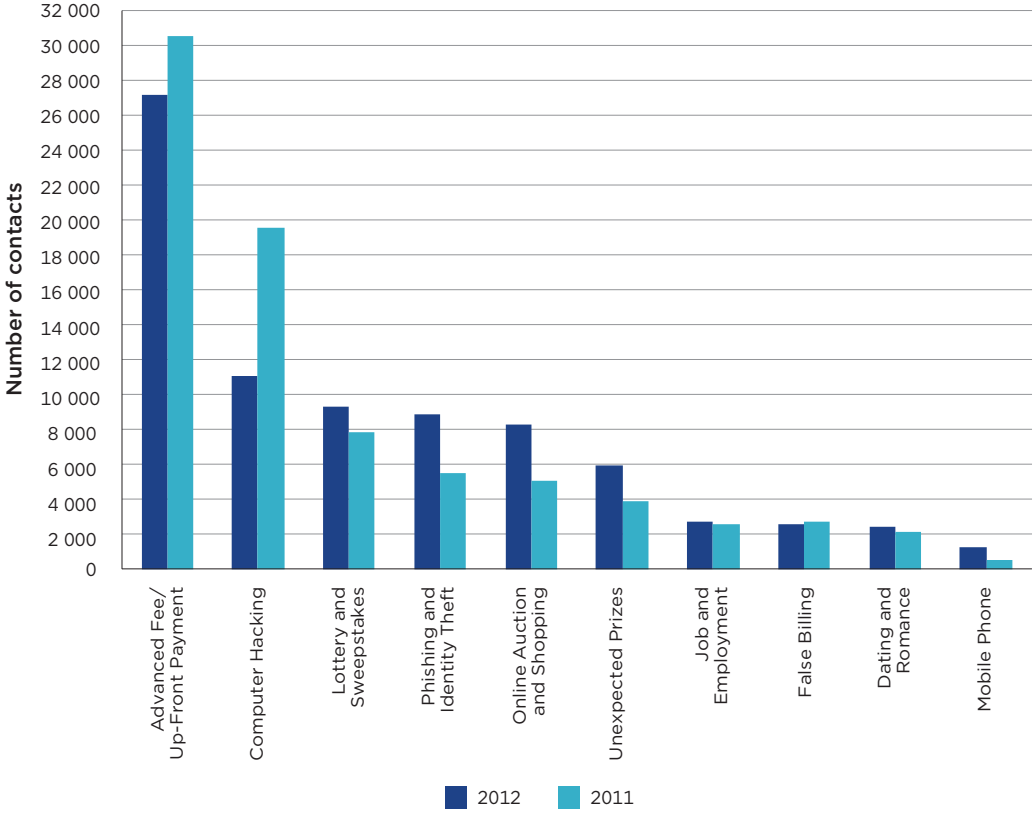


Figure 6: Comparison of the top 10 scam report levels 2011–12



The top 10 scams in 2012

The top 10 scams reported to the ACCC remained relatively similar in 2012 to that of 2011. The top five scams were identical, with some minor movement between scam categories (jobs and employment and false billing swapping to seventh and eighth ranking respectively). Mobile phone scams entered at 10 after dropping off the charts in 2009.

Figure 6 compares the number of reports between 2011 and 2012 for the 2012 top 10 reported scams. There was an increase in the number of reports to the ACCC across all top 10 scam categories except advanced fee/up-front payment scams, computer hacking, and false billing.

#1. Advance fee/up-front payment scams

Number of scam reports in 2012

27 039

Per cent of total scams reported in 2012

32 per cent

Number of consumers reporting losses

2362

Total losses reported by consumers

$30 203 373

Scam conversion rate

9 per cent

For the fourth consecutive year, advance fee/up-front payment scams were the most commonly reported scam type, constituting 32 per cent of all scam contacts.

The ACCC received 27 039 reports for this scam category, decreasing by 11 per cent from 2011 levels. At the same time, advance fee/up-front payment scams recorded the highest financial loss, with $30 203 373 reported lost. This was an increase of nearly 10 per cent compared to 2011 levels.

The advance fee/up-front payment category is broad and incorporates a range of different scams, all involving a scammer offering their victim a share in a sum of money or goods. Consumers are generally asked to provide up-front payments and/or personal information to receive their share, but the promise is never delivered.

These scams range from outlandish offers to extremely sophisticated scams that involve a gradual entrapment of consumers over many months.

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

Scammers manage to dupe Sue will-fully

"Official looking documents, logos, news articles, and even introducing you to 'bankers' or 'lawyers' are all part of inheritance scams, which often span international borders."

ACCC Deputy Chair Delia Rickard

Melbourne retiree Sue* received a letter out of the blue from a man claiming be a lawyer representing the estate of her great uncle. The letter informed her that she had been named in the long lost relative's will and could inherit a significant sum of money.

Sue excitedly contacted the lawyer and was soon provided with official looking documents showing that her relative had died overseas and that she was the heir to the multi-million dollar estate.

However, as Sue tried to access the estate, the 'lawyer' began to mention estate taxes, unpaid debts and legal fees which had to be paid via international wire transfer. Sue dutifully began to pay these fees and charges, but would discover a new fee each time she tried to access the estate.

After parting with a large sum of money, Sue contacted the embassy of the country the 'lawyer' had claimed to be from, and discovered that she had been scammed.

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

SCAMwatch radar: 'Hitman' scam resurfaces

July 2012

In July 2012 the ACCC issued a SCAMwatch radar warning Australians of the re-emergence of the 'hit man' scam, where scammers sent SMS death threats claiming to be a hired killer who would murder the recipient unless they sent cash or provided personal details.

SMS allowed scammers to quickly contact thousands of Australians.

This scam saw significant media attention in July 2012.

Read more at www.scamwatch.gov.au.

#2. Computer hacking scams

Number of scam reports in 2012

10 961

Per cent of total scams reported in 2012

13 per cent

Number of consumers reporting losses

1013

Total losses reported by consumers

$1 312 794

Scam conversion rate

9 per cent

Computer hacking was the second most reported scam type to the ACCC in 2012, contributing to just over 13 per cent of all scam reports.

The ACCC received 10 961 reports for this scam category, decreasing by 43 per cent from 2011 levels. However while contacts fell, reported losses more than doubled with an increase of almost 110 per cent to $1 312 794. This can be largely attributed to two reports received with financial losses of over $500 000 and $100 000 respectively.

In 2012 local and overseas authorities were successful in catching some of the perpetrators behind the cold calling computer virus scam (see section 5.2), one of the most commonly reported scams to the ACCC. A scareware scam where scammers claimed to be the Australian Federal Police also targeted Australians. A comparison of these scams is provided overleaf.

The ACCC also received 172 reports of social networking and email account hacking. After accessing the account, the scammer would commit identity theft, posing as the owner to gain money or personal details from friends, family, followers or contacts.

Account hacking was often initiated by a phishing scam asking the victim to enter their account password on a fake copy of their social networking site or email login page.

The anatomy of a scam: dissecting two computer hacking scams

	'Microsoft' computer virus scam	'AFP' scareware scam
How the scam works	Scammer pretending to be from Microsoft claims that the victim's computer has been infected with a virus, which needs to be fixed immediately. Their computer can be fixed for a fee.	Victim receives a computer pop-up alert claiming to be from the AFP advising that their computer has been frozen because they have visited an illegal site or broken the law. Their computer will be unlocked for a fee.
False affiliation	Microsoft (under various aliases)	Australian Federal Police
Delivery method	Telephone call	Online pop-up alert
Most commonly reported loss	$300–$400	$100–$200
Subsidiary loss	Scammer gained remote access to computer and personal information stored.	Victim has to engage the services of an IT expert to remove scareware and regain control of computer.
Scammers' tools	High pressure sales tactics to incite fear and anxiety that computer has been compromised and must be fixed immediately.	Frozen/locked computer, which strengthens scammers' claims. Emotional manipulation to induce fear and anxiety and immediate acquiescence.

SCAMwatch radar: With Halloween around the corner, beware of the scareware

October 2012

In October 2012 the ACCC issued a SCAMwatch alert to warn consumers about a particularly nasty scareware scam doing the rounds.

In this scam, the perpetrators pretended to be from the Australian Federal Police and tried to scare individuals into handing over money in order to regain control of their computer.

The scammers sent people pop-up alerts that claimed their computer had been locked down because they had visited an illegal website or breached various laws. The computer would be unlocked once a fee had been paid.

Read more at www.scamwatch.gov.au.

#3. Lottery and sweepstake scams

Number of scam reports in 2012

9337

Percentage of total scams reported in 2012

11 per cent

Number of consumers reporting losses

260

Total losses reported by consumers

$2 618 835

Scam conversion rate

3 per cent

Lottery and sweepstake scams were the third most commonly reported scam related activity to the ACCC in 2012, representing 11 per cent of all scam contacts.

The ACCC received 9337 reports for this scam category, increasing by nearly 19 per cent from 2011. At the same time, total reported losses fell by almost 35 per cent to $2 618 835. This included 12 instances of reported losses above $100 000 in 2011, whereas only eight reports reached this threshold in 2012.

In these scams, consumers are told they have won money in a lottery that they never entered. The winnings are commonly offered in currencies other than Australian dollars, for example British pounds or American dollars. These scams often pretend to be affiliated with genuine companies and brands including computer, car and mobile phone manufacturers. To claim winnings, victims are asked to provide an up-front payment and/or personal details. Victims are not able to use their 'winnings' to pay these fees and no money is ever received.

Lottery and sweepstake scams are increasingly being sent via SMS, with 5799 sent this way in 2012—an increase of 29 per cent from 2011.

This increase is likely attributable to scammers finding it more cost effective and easier to send out a large number of text messages compared to traditional postal services.

However, scammers also continue to send these scams via post and, in May 2012, the ACCC issued a SCAMwatch radar in response to an increase in contacts about scratchie scams being delivered this way.

Terry wins a one-way ticket to trouble

"A legitimate business won't ask you to pay to access your own money. If it seems too good to be true, it probably is."

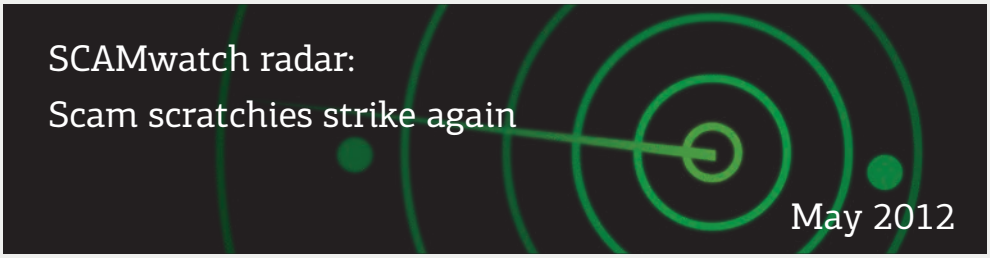
ACCC Deputy Chair Delia Rickard

Terry* was looking through his mail one morning and found two glossy brochures advertising overseas travel packages. Included with the two brochures were a number of lottery style scratch cards.

Terry scratched the first ticket, which thanked him for playing, and the second which told him that he had won a $10 000 holiday package. Never having won anything before, Terry excitedly called the number on the card to claim his prize.

Terry soon found that to claim his prize, he had to become a club member and pay a hefty membership fee via wire transfer. Having paid the fee, Terry found that he was still unable to access the holiday and that he couldn't get his money back.

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



In May the ACCC issued a SCAMwatch radar warning the public about an increase in scam scratchie cards delivered to their letterbox.

With this scam, victims were asked to pay thousands upfront in order to claim a prize that never arrived.

The package typically contained colourful travel brochures and a number of scratchie cards. One card would always be a 'winner'.

If the recipient tried to reclaim their prize by calling the number provided in the package, the scammer would ask for fees or taxes to be paid using a wire transfer service.

Read more at www.scamwatch.gov.au.

#4. Phishing and identity theft (including banking and online account)[3]

Number of scam reports in 2012

8788

Per cent of total scams reported in 2012

10 per cent

Number of consumers reporting losses

494

Total losses reported by consumers

$1 503 958

Scam conversion rate

6 per cent

Phishing and identity theft remained the fourth most commonly report scam type to the ACCC in 2012, representing approximately 10 per cent of all scam contacts.

In 2012 the ACCC received 8788 reports of phishing and identity theft scams, an increase of nearly 62 per cent compared to 2011. Associated financial losses totalled $1 503 958, an increase of almost 16 per cent from 2011. The number of contacts reporting a loss totalled 494, an increase of 95 per cent.

The most common form of phishing and identify theft scams are banking and online account scams. These scams trick people into providing their personal and banking information so that the scammers can steal their money or identity.

Scammers send emails that appear to be from legitimate businesses such as financial institutions, online payment services or telecommunications service providers, asking victims to provide account details (including usernames, unique user numbers and passwords).

Once a scammer gets access to an online bank account or social networking profile they can use it to commit identity theft, and bank account or credit card fraud.

3 The ACCC has retitled this category from 'banking and online account scams (including phishing)' to clarify that this group also covers non-banking instances of identity theft.

A dodgy logo has Steven seeing double

"Often scammers target you because they have some information about you already, which they use to gain your trust."

ACCC Deputy Chair Delia Rickard

Steven* was checking his emails when he saw a message from his mobile phone company saying that they had had trouble billing his credit card.

The email appeared legitimate as it displayed the logo of Steven's phone company. Steven clicked the link and arrived at a webpage that looked similar to his phone company's website. Steven provided the credit card details that were requested and went back to reading his emails.

A short time later, Steven received a call from his bank asking about some suspicious transactions on his credit card. It was then that Steven realised that he had been scammed.

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

Affiliation scams: who are you really dealing with?

Scammers are increasingly posing as reputable organisations to slip under people's radars. Scammers claim to represent a legitimate entity as consumers may be less cautious and more readily hand over money or personal details to a well-known and trusted source. They go to great lengths to convince their targets that they are who they claim to be, copying corporate logos, producing counterfeit and official looking documents, and even creating fake mirror websites with a slightly different web address.

These scams not only hurt the individual; they can also harm community trust in a government department or business.

Some common entities or industries used by scammers are outlined below.

Common government organisations

The Australian Government

The 'Australian Government Reclaim Department' (fictitious)

The 'Australian Council' (fictitious)

The Australian Taxation Office and Centrelink

Birth, death and marriage registries

The ACCC and SCAMwatch

Common industries

Banks and financial institutions

Online shopping services

Computer and IT security companies

Email and telecommunications services

Postal and logistics services

Social network services.

#5. Online auction and shopping scams

Number of scam reports in 2012

8275

Per cent of total scams reported in 2012

10 per cent

Number of consumers reporting losses

3038

Total losses reported by consumers

$4 038 479

Scam conversion rate

37 per cent

Online auction and shopping scams remained the fifth most reported scam type in 2012, representing 10 per cent of total scam contacts.

In 2012 the ACCC received 8275 contacts about this scam type, an increase of 65 per cent from 2011 levels. This is unsurprising given the increased take-up by Australians of online shopping. At the same time, reported financial losses totalled $4 038 479, a decrease of 3 per cent.

The conversion rate also fell in 2012 to almost 37 per cent, a decrease of 43 per cent from 2011 levels. While more people reported a loss in 2012, a greater proportion of people reported scams where they did not suffer a financial loss.

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

- **Classified ad scams**—a scammer posts a fake ad on a legitimate classifieds website for cheaply priced popular items. If a consumer shows interest in an item, the scammer will claim that the goods will be delivered following receipt of payment. If the consumer pays, they will not receive the goods or be able to contact the seller.
- **Overpayment scams**—a scammer responds to a seller's ad with a generous offer and then 'accidentally' overpays. The scammer will ask the seller to 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.

Common products that scammers target to buy or sell online include pets, used cars, boats and bikes, and electronic items such as smart phones, tablet devices and laptops.

Gemma learns this scam is a dog

"Don't trust the legitimacy of an ad just because it appears on a reputable online shopping site—make sure that the person you are dealing with, and their offer, is the real deal."

ACCC Deputy Chair Delia Rickard

Gemma* had been begging her mother for a puppy for her 13th birthday. She saw an online ad for a litter of labradors that were being sold near to her home. They contacted the owner who claimed an overseas trip prevented him from delivering the animal in person. However, they informed Gemma's mother that she could pay a fee to release the animal from the boarding kennels and arrange for the puppy to be delivered that weekend, just in time for Gemma's birthday.

Her mother transferred $750 for the labrador plus $200 for travel costs, and they excitedly prepared for its arrival. When the labrador didn't arrive, Gemma's mum repeatedly tried to contact the seller but with no luck. They realised they had been scammed and Gemma was devastated.

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

Online shopping: staying one click ahead of the scammers

Australians are increasingly going online to buy goods and services, taking advantage of benefits from increased competition, choice and convenience. The Productivity Commission estimates that in 2011 online retailing represented 6 per cent of total Australian retail sales—4 per cent domestic online ($8.4 billion) and 2 per cent from overseas ($4.2 billion).[4]

Here are five key tips to follow to avoid being scammed when shopping online:

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 send money or your financial details to a stranger, especially via money transfer—it's rare to recover money sent this way.

4 Productivity Commission, Economic Structure and Performance of the Australian Retail Industry, December 2011.

#6. Unexpected prize scams

Number of scam reports in 2012

5942

Per cent of total scams reported in 2012

7 per cent

Number of consumers reporting losses

184

Total losses reported by consumers

$1 057 378

Scam conversion rate

3 per cent

Unexpected prize scams remained the sixth most common scam type reported to the ACCC in 2012 representing 7 per cent of all scam contacts.

In 2012 the ACCC received 5942 contacts about unexpected prize scams, an increase of 55 per cent from 2011. Reported financial losses totalled $1 057 378, a decrease of 46 per cent. This large decrease is due to less people suffering substantive losses; in 2011 one victim reported losing $500 000 compared to the largest reported loss in 2012 of $140 000.

With these scams, consumers are offered a prize such as a cheap holiday, smart phone or laptop, to elicit payment or obtain personal or credit card details.

However, in order to claim the prize the 'lucky winner' must first pay a fee upfront for various charges or call a premium rate phone number. These fees and phone call rates can be very expensive.

Once the victim has paid these costs, the promised prize never arrives or is not what the scammer said it would be.

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

Janine's cold call puts her in the hot seat

"Scammers can switch from using a silver tongue to abusive language in a heartbeat. They will do anything to separate you from your money."

ACCC Deputy Chair Delia Rickard

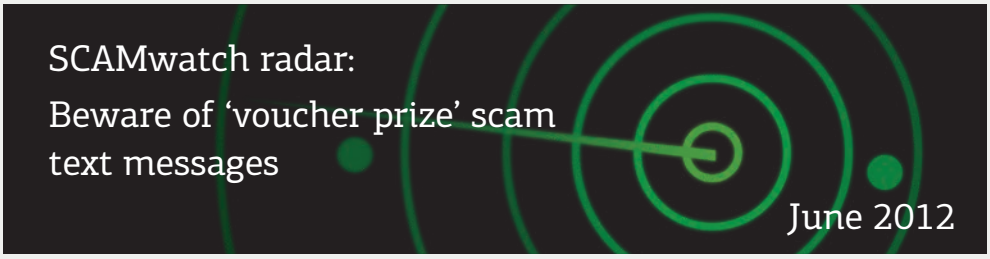
Janine* received a call out of the blue telling her she had won an overseas holiday. Assuming her husband had entered a competition without telling her, Janine accepted the offer and began to get excited about the trip.

The caller then requested credit details to put a deposit on the holiday booking. Janine was so excited that she provided her credit card details before trying to clarify the nature of the deposit. When Janine realised that the holiday was not free, she asked how she could recover her deposit. The caller then told Janine that she was 'locked in' to buying the holiday.

Now realising that the full price of the 'free' holiday would be charged to her credit card, Janine asked to cancel. But the caller refused and began to get abusive. Eventually, Janine spoke to a 'manager' who also refused to let her out of the holiday and began to threaten her with legal action if she failed to pay.

Convinced that she was the victim of a scam, Janine contacted her bank to report the fraudulent activity.

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



In June 2012 the ACCC issued a SCAMwatch alert to warn consumers about text messages doing the rounds that claimed individuals had won a voucher. If the recipient responded to the text message, they would find themselves entered into an expensive mobile premium SMS service.

This scam used (without authority) brand names and logos of well-known companies and products in order to make the prize look legitimate.

Read more at www.scamwatch.gov.au.

#7. Job and employment scams (including business opportunities)

Number of scam reports in 2012

2673

Per cent of total scams reported in 2012

3 per cent

Number of consumers reporting losses

294

Total losses reported by consumers

$2 704 235

Scam conversion rate

11 per cent

In 2012 job and employment scams moved up to the seventh (previously eighth) most commonly reported scam type to the ACCC, representing 3 per cent of total scam contacts.

The ACCC received 2673 job and employment scam reports, an increase of almost 7 per cent. At the same time, both the reported financial losses and the number of people reporting those losses fell. Total financial losses reported were $2 704 235, a decrease of 63 per cent. The number of people reporting a financial loss decreased by 20 per cent.

This large decrease is likely due to a fall in the number of employment or business opportunity scams with a significant financial loss reported. In 2011, the ACCC received reported losses of $2.5 million, $600 000 and $500 000 to this scam type, whereas in 2012 the largest reported loss was $300 000.

Job and employment scams can involve offers to work from home or to set up and/or invest in a business. Scammers promise a high 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 is sometimes used to launder money, for example a victim is paid to receive money into their bank account and then transfer it to another location or account.

Stacey learns to avoid scams the hard way

"Scammers will promise the world and then disappear before delivering anything. Be suspicious whenever you are asked for money."

ACCC Deputy Chair Delia Rickard

Stacey*, an international student studying in Australia, needed some money and answered an online ad for a company that claimed to specialise in placing international students in jobs.

Stacey was offered work as a film and TV extra, but was told that she needed to pay money for a photographic portfolio.

Stacey was later told that the company needed a payment to process her working visa and residency status before they could find her a position. But after paying the money, Stacey soon found that the scammers had disappeared.

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

Money laundering is a crime

Many people receive emails advertising easy money for working from home. These ads will describe how to open a bank account and take a commission on money being transferred through it. The scammers claim that this allows them to avoid tough tax laws in their home country.

The money being transferred is often stolen. The scammers need to transfer the money through an Australian bank account to launder it and avoid police attention.

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 unaware that they were handling the proceeds of crime can be prosecuted for money laundering in Australia.

#8. False billing scams (including advertising, directory and domain name scams)

Number of scam reports in 2012

2546

Per cent of total scams reported in 2012

3 per cent

Number of consumers reporting losses

485

Total losses reported by consumers

$566 061

Scam conversion rate

19 per cent

In 2012 false billing scams were the eighth (previously seventh) most commonly reported scam type to the ACCC, representing 3 per cent of scam contacts.

The ACCC received 2546 false billing scam contacts, a decrease of approximately 7 per cent. Likewise, reported financial losses fell with $566 061 reported, a drop of nearly 8 per cent. Despite the decrease in contact levels, the number of consumers reporting a loss from these scams increased by almost 18 per cent. As such the conversion rate increased from 15 to 19 per cent.

False billing scams are the most commonly reported scam targeting small businesses. This type of scam targets small businesses by tricking them into paying for unwanted or unauthorised listings or advertisements in magazines, journals, business registries or directories. Services often used as a ploy to target businesses 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.

In 2012 the ACCC successfully prosecuted schemes targeting small business operators to falsely sign them up to buy advertising services (see section 5.2).

Profile on small business scams

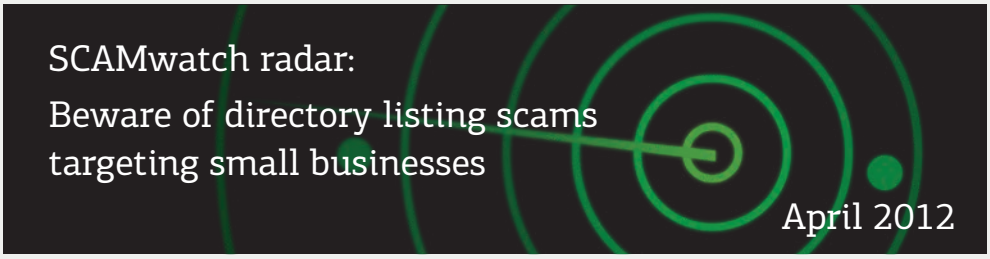
"Businesses should consider whether unsolicited offers are credible and represent value for money."

ACCC Deputy Chair Dr Michael Schaper

Whilst the majority of scam-related contacts to the ACCC are from consumers, small businesses also report scams that target them.

Apart from false billing scams, small businesses should also watch out for:

- **Domain name scams**—scammers deceive businesses through unsolicited contacts and by using high pressure tactics to purchase an internet domain registration very similar to their own. Businesses may also receive a fake renewal notice for their actual domain name and pay without realising
- **Office supply scams**—businesses receive and are charged for products that they did not order. These scams often involve products or services that businesses regularly order such as stationery and cleaning supplies. Scammers typically call businesses pretending that the service or product has already been ordered
- **Fax back scams**—scammers fax businesses an offer that requires one to accept by sending a fax back to a premium rate number (starting with '19') to accept. The scammers make sure that it takes several minutes to process the fax, resulting in a hefty phone bill.



In April 2012 the ACCC issued a SCAMwatch alert to warn businesses about an increase in unsolicited faxes offering paid listings in scam online directories.

The scam offer aimed to lock businesses into an expensive ongoing contract for periods of 12, 24 or 48 months. Sometimes the scammer sought payment 12 months in advance. Businesses reported feeling intimidated into paying after the scammer threatened legal action or debt collection.

Read more at www.scamwatch.gov.au.

#9. Dating and romance scams

Number of scam reports in 2012

2441

Per cent of total scams reported in 2012

3 per cent

Number of consumers reporting losses

1119

Total losses reported by consumers

$23 311 211

Scam conversion rate

46 per cent

In 2012 dating and romance scams remained the ninth most commonly reported scam to the ACCC, with both contact levels and reported financial losses higher than in 2011.

The ACCC received 2441 reports of dating and romance scams, up 15 per cent. Reported losses totalled $23 311 211, up 6 per cent from the previous year.

The conversion rate decreased from 52 per cent in 2010 and 48 per cent in 2011 to 45 per cent in 2012. This means that, whilst there are more people reporting victimisation as a result of dating and romance scams to the ACCC, less are losing money. Given that dating and romance scams can be carried out over a long time—in some instances, years—this may mean that victims are identifying that they have been duped and cease losing money to the scam earlier than in previous years.

Despite this conversion rate decrease, losses per victim of dating and romance scams continued to be high in comparison to most other scam categories.

On average, each victim reported a loss from dating and romance scams of almost $21 000, with over 30 per cent of reported losses being more than $100 000.

This is in comparison to nearly eight[5] of the top 10 scams reported to the ACCC having average losses below $10 000 and four reporting average losses per victim below $2000.

In these scams, which are run by experienced criminal networks—the scammer develops a strong rapport with the victim, often over weeks or months, before asking for money to help cover costs associated with illness, injury, a family crisis or to travel to see them. This scam type commonly sees the scammer trying to exploit their victim's emotions. Dating and romance scammers often approach their victims on legitimate dating websites, and then quickly attempt to move the victim away from the security of the website, communicating through other methods such as email.

Scammers also target victims through social networking platforms, using their personal information against them.

In 2012 the ACCC worked with operators of dating websites to address scams targeting their users (see section 5.1).

5 The following scam types all recorded average reported losses below $10 000: computer hacking, phishing and identity theft, online auction and shopping, unexpected prizes, job and employment, false billing, and mobile phone scams. Lottery and sweepstake scams recorded an average loss of $10 072.

Melissa's lonely hearts web scam

"Unfortunately, cupid can sometimes miss your heart and strike your wallet instead."

ACCC Deputy Chair Delia Rickard

Melissa*, a business woman in her forties living on the Gold Coast, began communicating with an attractive middle-aged man named Grant on a dating website. Grant claimed he was an American engineer working on an oil rig in the Persian Gulf, with similar interests to Melissa.

Grant suggested that they start emailing directly, away from the online dating site, and soon Melissa found herself emailing Grant several times each day.

Grant then claimed that he had been in a work accident on an oil rig and needed help to pay medical bills. Melissa transferred money to various accounts by wire transfer, as requested, with the bills mounting up.

Many months and tens of thousands of dollars later, Melissa realised she had been scammed.

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

Emotional investments

Dating and romance scammers can invest a considerable amount of time engaging with victims, sometimes spending weeks and months to build up a relationship before scamming victims out of money. Scammers employ multiple excuses for why they need financial assistance and cannot meet in person. They may claim to be ill or caring for a sick relative, unable to leave a job or even be an active duty service person posted to a war zone. These excuses are designed to elicit sympathy and a desire to help out financially. These scams rely upon the emotional connection between the scammer and the victim, and can play out for years with the scammer coming up with new reasons to ask for money.

At the same time, 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 extremely high success rate for scammers in obtaining large amounts of money.

#10. Mobile phone scams (including ringtone, competition and missed call scams)

Number of scam reports in 2012

1302

Per cent of total scams reported in 2012

2 per cent

Number of consumers reporting losses

269

Total losses reported by consumers

$367 739

Scam conversion rate

21 per cent

Mobile phone scams re-entered the top 10 most commonly reported scams activity in 2012.[6]

There was a significant increase in the number of mobile phone scams reported to the ACCC, with 1302 scams reported—more than double 2011 levels. Reported losses also increased by 809 per cent to $367 739. This included three instances of reported losses above $100 000; in 2011, no reports of mobile phone scams reached this threshold.

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 2.1, scams *delivered* via mobile phone recorded a total loss of $759 986.

Mobile phone scams can be difficult to recognise. They might come from somebody who talks as if they know you, they might come through a 'missed call' from an unknown number that you redial, or they might be upfront 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 can cost a lot of money when replied to. SMS competition and trivia scams involve an invitation to enter a competition or trivia contest over SMS for a great prize but mislead consumer about how much it will cost to take part or the chances of winning.

6 Mobile phone scams was the ninth most commonly reported scam type to the ACCC in 2009, when the *Targeting Scams* report was first published.

John flirts with danger

"Once you reply to a scammer, they will try anything to lead you along and empty your pocket."

ACCC Deputy Chair Delia Rickard

John* began getting SMS text messages from an unknown number suggesting that they should 'catch up' or 'get together for a drink'.

John began texting back thinking it was a friend with a new phone number. John soon discovered that although the SMS had been a wrong number from Jen*, they rapidly began to send flirty texts back and forth.

After sending a lot of SMS messages, John began asking to meet the woman on the other end of the phone. As soon as he did, the text messages stopped. After trying to call and not getting a response, John put the whole incident out of his mind.

Until John received his phone bill, when he discovered that all the text messages he had sent to that number had been charged at a premium rate. John had spent more than $100 on a scammer.

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

Scammers spamming via SMS

Scammers have clearly added texting to their toolbox, taking advantage of this relatively cheap delivery method to spam thousands of people 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 messages: 0429 999 888.

3 Research

Research plays an important role in helping government, business and the community better understand the scale of scams and their impact on individuals.

In 2012 a number of key research findings were released that will help inform a more effective response to scams activity.

Australian Bureau of Statistics Personal fraud survey 2010–11[7]

In April 2012 the Australian Bureau of Statistics (ABS) released the results of its *Personal fraud survey 2010–11*, which found that Australians lost $1.4 billion due to personal fraud (which includes credit card fraud, identity theft and scams).

The survey results showed that 2.9 per cent (514 500) of Australians were victims of scams, an increase from 2 per cent in 2007. The ABS defines a scam as 'a fraudulent invitation, request, notification or offer, designed to obtain personal information or money or otherwise obtain a financial benefit by deceptive means'.

In addition to scams, the survey found that 3.7 per cent (662 300) of Australians were victims of credit card fraud, and 0.3 per cent (44 700) of Australians were victims of identity theft.

The 2010–11 survey asked people aged 15 years and over about their experiences of personal fraud. The survey results estimated that three in five victims of personal fraud (713 600 persons) lost money with an average of $2000 per victim. The survey estimated that a total of 1.2 million Australians, or 6.7 per cent of the population aged 15 years and over, were a victim of at least one incident of personal fraud in the 12 months prior to interview. This is an increase from 2007 when there was an estimated 806 000 victims (5 per cent) of personal fraud.

The proportion of people exposed to a scam (but that did not necessarily respond) remained steady between 2007 and 2010–11, at 35.8 per cent of the population aged 15 years and over. At the state/territory level, the exposure rate increased in Victoria (from 32.7 per cent in 2007 to 36.2 per cent in 2010–11), and decreased in Queensland (from 39.7 per cent in 2007 to 36.8 per cent in 2010–11), Western Australia (from 38.1 per cent in 2007 to 33.5 per cent in 2010–11), and the Australian Capital Territory (from 48.5 per cent in 2007 to 39.5 per cent in 2010–11). In 2010–11, the scam exposure rate in Tasmania (40.8 per cent) and the Australian Capital Territory (39.5 per cent) were both higher than the national exposure rate (35.8 per cent).

There were no statistically significant differences in the victimisation rate for a scam between the states and territories or between the genders both at a national and state/territory level in 2010–11.

Of all persons exposed to a scam, an estimated 8.1 per cent responded to the scam invitation, request, notification, or offer by accessing a website, asking for more information, sending personal details or accepting an offer. Persons were most likely to respond to a fake notification from an established business, with 6.3 per cent of all persons exposed responding, and were least likely to respond to chain letters, with 0.9 per cent of all persons exposed responding.

7 Australian Bureau of Statistics, *Personal fraud survey 2010–11*, Canberra, April 2012.

Australasian Consumer Fraud Taskforce research (conducted by the Australian Institute of Criminology)

Since 2006 the Australian Institute of Criminology (AIC), on behalf of the Australasian Consumer Fraud Taskforce (ACFT), has conducted an annual online survey of scams to understand Australians' changing experience of this type of activity.

Consumer scams—2012[8]

The AIC's report, *Australasian Consumer Fraud Taskforce: Results of the 2012 online consumer fraud survey,* presents the results of the ACFT's annual consumer fraud survey, which in 2012 had 1576 participants. Although respondents were self-selected, making the results not representative of the Australian population as a whole, the survey results provide an indication of the experiences of a selection of individuals who have been exposed to scam invitations.

A high proportion (95 per cent) of respondents reported receiving a scam invitation in 2012, and 22 per cent responded in some way. Seven per cent of respondents sent their personal details, three per cent suffered a financial loss, and five per cent of respondents reported a financial loss as well as loss of personal information as the result of a scam in 2012. The amount that respondents indicated they had lost to scams ranged from $3 to $195 000, with a median loss of $500. Total losses reported by 108 of the victims who disclosed how much they had lost was $846 170.

In 2012, 7.1 per cent of respondents reported being exposed to an online shopping or auction site scam. Almost half of these involved the seller of a vehicle such as a car, boat, motorcycle, trailer or caravan, being contacted by someone that was believed to be posing as a potential buyer. Typically the seller was offered a higher price than what was being sought, and was asked to transfer an amount to an agent or courier company so that the transfer of goods could take place. Sellers were also sent fabricated remittance notices to make it appear that they had received a payment when they had not. Sellers of other goods were also contacted in similar ways, usually for high-value items. Relatively few respondents reported that they had been exposed to scams when attempting to purchase items, however reports did include the sale of counterfeit goods, and purchasing items that were not received.

Australian Crime Commission and Australian Institute of Criminology *Serious and organised investment fraud in Australia*[9]

In July 2012 the Australian Crime Commission (ACC) and the AIC released a report examining the nature and threat of serious and organised investment fraud in Australia.

Serious and organised investment fraud refers to the solicitation of investment in non-existent or essentially worthless shares and other securities. These scams are typically unsolicited 'cold calls' used alongside sophisticated hoax websites to try and legitimise the fraud.

The report found that more than 2600 Australians may have lost over $113 million to serious and organised investment fraud in the previous five years. Financial losses could be even higher because people tend not to report this kind of crime. The targets of this type of crime are primarily Australian men aged over 50 who may be highly educated with high levels of financial literacy. They are likely to manage their own super.

To combat this growing threat, in 2011 the ACC Board established multi-agency Task Force Galilee to disrupt and prevent serious and organised investment fraud and harden Australians against this type of organised crime. See section 6.5 for more information.

8 Jorna P & Hutchings A 2013. *Australasian Consumer Fraud Taskforce: Results of the 2012 online consumer fraud survey*. Canberra: Australian Institute of Criminology.

9 Australian Crime Commission and Australian Institute of Criminology, *Serious and organised investment fraud in Australia*, Canberra, July 2012.

Curtin University small business scams research

In 2012 Curtin University Business School undertook a national survey project to investigate the prevalence of scams committed against small businesses in Australia.

The survey explored the prevalence of scams targeting small businesses across Australia, the level of victimisation and why small businesses fall victim. Key research findings to date show that of the 192 small business survey participants, over 70 per cent may have wasted time and/or money thwarting a scam attempt, 12 per cent lost money to a scam, and the more online activity and e-commerce a firm undertakes, the higher losses are likely to be.

The research will be officially released in June 2013.

Curtin Business School anticipates that the results will help to develop strategies to reduce the level of risk faced by SMEs and disrupt scams activity. The results may also help to develop a profile of susceptible businesses, which can then be used to build a scam risk self-assessment process.

4 Awareness raising and education initiatives

Education and awareness raising is a key tool in law enforcement efforts to minimise the impact of scams on society. The increasingly online, technological and global nature of scams presents significant challenges in prosecuting the perpetrators of scams. Therefore empowering individuals with the knowledge and skills to identify and avoid being scammed in the first instance is a priority.

This chapter outlines ACCC initiatives to educate and empower Australians to avoid falling victim to scams.

4.1 SCAMwatch

The ACCC's SCAMwatch website (www.scamwatch.gov.au) provides information to consumers and small businesses about how to recognise, avoid and report scams.

SCAMwatch has significant brand awareness amongst the Australian 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 6.1.

In 2012 the SCAMwatch website received 971 824 unique visitors, an increase of 196 835 or 25 per cent from 2011. Although the majority of visitors were located in Australia, SCAMwatch was also visited by people located around the world.

Apart from the homepage, the most popular sections of the site were 'report a scam' and 'SCAMwatch radars'.

Figure 7 shows the growth of unique visitors to SCAMwatch.

Figure 7: Unique visitors to the SCAMwatch website from 2006 to 2012

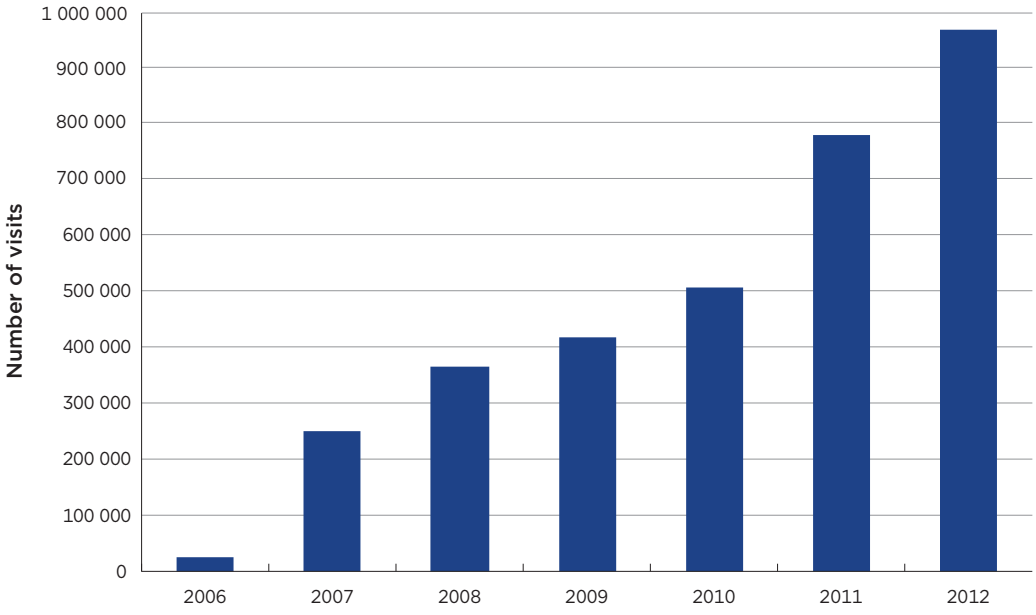
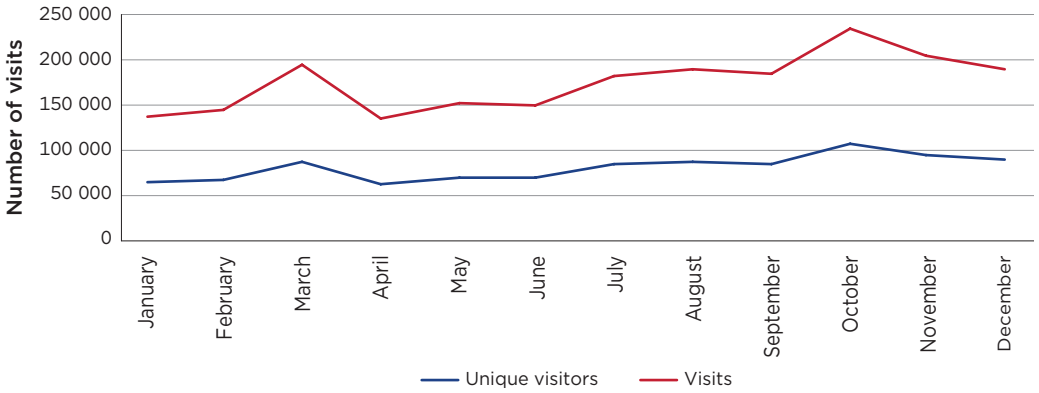


Figure 8 shows that in 2012 there were on average more unique visits to SCAMwatch per month compared to 2011. The average weekday visits to the website ranged between 2500 and 3500 visits.

Figure 8: Comparison of monthly visits to the SCAMwatch website in 2011 and 2012



Similar to previous years, visits to the SCAMwatch website were higher than average during the National Consumer Fraud Week campaign (19–26 March); between 19 and 22 March SCAMwatch received from 5500 to 6500 visits per day.

There were also two days during the year that received significant peaks, coinciding with the release of SCAMwatch radars about emerging scams. On 23 July the ACCC released a radar alert on the 'hit man' scam (see chapter 2), resulting in over 10 000 visits that day. On 4 October the ACCC released an radar on the successful prosecution by overseas regulators of scammers behind the 'Microsoft' computer virus scam (see chapter 6, which resulted in over 7000 visits that 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 2012 the email service reached 22 356 subscribers, with an additional 3690 subscribers, an increase of 20 per cent from 2011.

In 2012 the ACCC issued 19 SCAMwatch radars to warn Australians about the imminent risk of scams around current events such as the introduction of carbon pricing, spring racing, tax returns and holidays such as Christmas and Halloween.

SCAMwatch radar alerts were also issued in partnership with other organisations wishing to alert the public to scams. For example in December 2012 the ACCC and the Australian Charities and Not-for-profits Commission issued joint alerts to help consumers wishing to donate to charities during the festive season make sure that their money went to a legitimate charity and not to a scammer.

A full list of 2012 SCAMwatch radar alerts are at appendix 2.

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

4.2 SCAMwatch Twitter—@SCAMwatch_gov

The SCAMwatch Twitter account @SCAMwatch_gov has continued to prove itself popular in its second year, attracting 1531 additional followers in 2012, a 58 per cent increase in followers from 2011. Twitter allows SCAMwatch to reach consumers, businesses and the media in real time as scams emerge.

During 2012 @SCAMwatch_gov posted 539 tweets about scams targeting Australian consumers and business. Tweets covered emerging and current scams including:

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

@SCAMwatch_gov was also used to answer questions posed by followers about specific scams conduct and to support other government initiatives to protect the public from scams.

SCAMwatch
www.scamwatch.gov.au

Follow SCAMwatch on Twitter to receive timely alerts at http://twitter.com/SCAMwatch_gov or @SCAMwatch_gov.

4.3 Printed materials

The ACCC has a suite of scams-related publications that complement the information provided on the SCAMwatch website. In 2012 the ACCC distributed almost 135 000 copies of these publications.

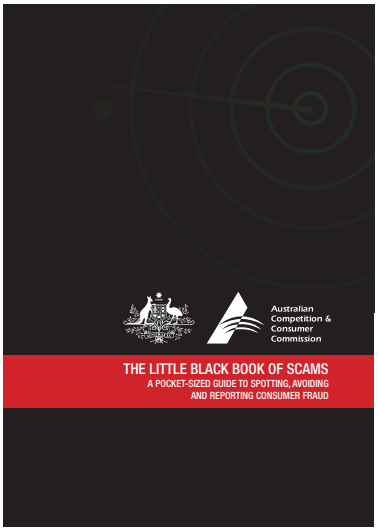
The most popular publication was *The Little Black Book of Scams,* which in 2012 was launched as a new pocket sized version. From its launch in March through to December, 127 825 copies of this free booklet distributed to consumers and businesses.

The Little Black Book of Scams highlights scams regularly used to target Australian consumers and small business, in areas such as fake lotteries, internet shopping, mobile phones, online banking, employment opportunities, and investment offers. It offers tips on how consumers can protect themselves from scams, what they can do to minimise damage if they get scammed, and how they can report a scam.

This publication is considered a best practice educational resource internationally, with several overseas regulators producing their own localised versions.

Appendix 3 provides a full list of the ACCC's scam-related resources for consumers and businesses.

Over 6500 copies of the ACCC's scam factsheets—covering lottery, sweepstakes and competition scams, money transfer scams, phishing scams, sports investment scams, and small business scams—were also distributed in 2012.



The *Little Black Book of Scams*, pocket-sized edition

Launched March 2012

4.4 Media and communications activity

The ACCC actively disseminated education and awareness messages to the media in 2012. The two main media events were Fraud Week and the release of voluntary guidelines for dating and romance websites to combat scammers.

Fraud Week 2012 received significant media attention. Highlights included multiple television and radio interviews as well as front page print coverage. While in support of the guidelines, Deputy Chair Dr Michael Schaper conducted interviews with 11 major regional and metropolitan radio programs.

The ACCC's participation in the annual International Consumer Protection Enforcement Network (ICPEN) internet sweep also received media coverage. The ICPEN internet sweep focussed upon how consumer guarantee rights are represented to consumers online and to identify the tricks used to try to fool consumers into believing such rights do not apply online.

The ACCC also pursued a strategy of providing additional media support to notable SCAMwatch radar alerts. This strategy saw increased media coverage of significant scams throughout October, November and December 2012. For instance, the ACCC undertook media activity on a dating and romance scam where consumers were being lured into purchasing a fake police check certificate, betting syndicates during the Victorian Spring Racing Carnival and fake charity scammers in the lead up to Christmas.

In addition to issuing regular media releases, the ACCC also used the media to publicise enforcement outcomes such as the penalties awarded against TVI Express and Elite Publishing.

This ongoing and extensive engagement with mass media is a crucial component of the ACCC's efforts to alert consumers and small businesses to the presence of scams.

Appendix 4 highlights the ACCC's key scam-related media and communications activities in 2012.

4.5 National education and engagement activities

During 2012 the ACCC's Education and Engagement Managers engaged with consumers and businesses about scams across Australia. Activities were conducted to raise awareness and spread ACCC scams messages widely to groups that may be vulnerable to scams, including small businesses, senior citizens and local communities.

The Education and Engagement Managers raised awareness of scams by attending meetings and giving presentations to:

- consumers attending seniors group meetings (including Probus and RSL clubs) and events such as the Office of Ageing (ACT) Seniors' Week events
- government stakeholders including NSW Office of Fair Trading Community Liaison Coordinators, staff at the Small Business Support Line, and the Department of Human Services Community Consultative Committee (WA)
- key local government and economic groups such as the Local Government and Shires Association (NSW), and the Ringwood Chamber of Commerce and Industry (Vic)
- professional associations such as the Institute of Public Accountants (NSW), Certified Practicing Accountants (NSW and WA), and the Motor Traders Association (SA)
- consumer advocacy and support groups such as the Legal Information Access Centre (NSW), Multicultural Disability Advocacy Association (NSW), St Vincent de Paul (NSW), Migrant Resource Centre (WA), and VICDeaf.

The Education and Engagement Managers also raised awareness of scams by collaborating with state/territory government agencies and co-presenting with them at the NSW Fair Trading Community Worker Forum, the Migrant Resource Centre (SA) Youth Leaders Forum, the St Albans Community Information Day (VIC), and to the Maroondah City Council (Vic) traders.

Managers also organised activities with local community groups to ensure ACCC messages penetrated to the grassroots level, including in rural community centres and local technology centres.

The ACCC also regularly engages with small businesses to raise awareness of the types of scams that target them. The ACCC provides small businesses with information on relevant enforcement action and scam-like conduct through its Small Business Information Network. The network comprises more than 1200 small businesses and small business stakeholders, including industry associations, local government and business enterprise centres.

The ACCC's 2012 enforcement activity in the area of scams also had a direct impact on scammers targeting small businesses (see chapter 5).

5 Disruption and enforcement activities

Disruption and enforcement activity is an important part of deterring, discovering and discouraging scammers. The increasingly sophisticated, overseas, and online element of scams presents considerable difficulties in identifying and prosecuting the perpetrators of scam conduct. Scammers have a great capacity to develop and adapt to growing consumer awareness of popular scam techniques. Scammers are also adept at evading prosecution through phoenix activity whereby they resume operations under a different name.

This chapter outlines action taken by the ACCC to enforce the law against scammers and to disrupt their activities.

5.1 Scam disruption activities

The ACCC and other agencies recognise that it is not possible to prosecute all scammers. This is because many are based in overseas jurisdictions and can be hard to track, especially with the increasingly sophisticated technologies used to perpetrate scams. Therefore the ACCC cooperates with agencies and private entities to disrupt and limit the harm that scams can cause to consumers and small businesses when enforcement action is inappropriate or unavailable.

In 2012 the ACCC continued to work with government and non-government parties who provided information that on closer analysis confirmed various activities as scams.

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.

One such example was the ACCC's work with dating website operators to develop voluntary industry guidelines.

Case study: ACCC works with online dating industry to better protect consumers from scams

"Online dating is an increasingly common way for people to meet each other. However, the growing number of scammers undermining the public trust in legitimate businesses like dating and romance websites is an area of concern to the ACCC."

ACCC Deputy Chair Michael Schaper

The ACCC organised a working group in 2011 of dating website operators to address scams targeting their users.

This joint project arose after the ACCC observed increasing reports of dating and romance scams in recent years and significant associated financial losses, with over $15 million reported lost in 2010. The conversion rate was also considerable at 52 per cent.

In July 2011 the ACCC held a roundtable meeting with a number of key dating website operators based in Australia to discuss measures and develop strategies to improve their response to online dating and romance scams.

The industry response was positive and website operators provided information on the measures they had already implemented to protect their users from scams. The ACCC subsequently formed a working group with nine dating website operators to develop best practice guidelines for dating websites. Before finalising the draft guidelines, the ACCC consulted with the broader online dating industry.

On Valentine's Day 2012 the ACCC launched a set of voluntary guidelines for dating websites to help operators respond to scams targeting their users. The guidelines aim to complement existing measures and to provide guidance to new entrants to the industry. The ACCC considers that they represent industry best practice, and encourages their adoption by all dating websites used by Australian consumers.

The actions detailed in the guideline fall into three areas:

1. appropriate scam warnings and information
2. internal vetting and checking procedures to detect scammers
3. effective complaint handling procedures.

5.2 Scam-related enforcement activities

The ACCC initiated proceedings or concluded action against a number of traders allegedly involved in misleading and deceptive or scam-like conduct in 2012. In particular, two court actions were finalised against traders engaging in pyramid selling schemes.

In a pyramid scheme, the only way for a member to recover any money is to convince other people to join up and to part with their money as well. In contrast, people in legitimate multi-level marketing schemes earn money by selling genuine products to consumers, not from the recruiting process. Most pyramid schemes disguise their true purpose by introducing products that are overpriced, of poor quality, difficult to sell or of little value. Making money out of recruitment is still their main aim.

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

The ACCC also took action against a group of traders that were targeting small business operators with scam-like conduct to falsely sign them up to buy advertising services. While perpetrators of this type of conduct are often based overseas, the ACCC has instituted proceedings against a number of identified traders in recent years.

Two enforcement case studies from 2012 are outlined below.

Case study: TVI Express

"Pyramid selling schemes are not legitimate businesses but scams promising the rewards of easy money that never arrives."

ACCC Chairman Rod Sims

In May 2012, following ACCC court action, the Federal Court of Australia imposed penalties totalling $200 000 on three individuals, Lualhati Jutsen (also known as Teddi Jutsen), Tina Brownlee and David Scanlon for their illegal participation in the pyramid selling scheme TVI Express.

Justice Nicholas found that the parties had breached the law by participating in the TVI Express scheme.

The TVI Express scheme was promoted through various websites including the site www.tviteamoz.com and the TVI Express Oz group on facebook.com. The TVI Express scheme extended throughout Australia and internationally.

People who wished to participate in the scheme were required to pay a membership fee of $330. Once an individual had paid the $330, they received a 'travel certificate' and the opportunity to receive commission payments for recruiting other people into the scheme.

The court found that the vouchers were of little to no value and that the only way a person could earn income from participating in the scheme was by recruiting new members.

The ACCC pursued subsequent proceedings in June 2012 against Ms Jutsen for contempt of a court order relating to bank withdrawals in circumstances where she was restrained from making withdrawals from that account beyond those required to meet her ordinary living expenses.

Case study: Elite Publishing, Wiltshire Publishers, Exclusive Media and Andrew Clifford

"This decision sends a strong message that the ACCC will use its powers to take action against companies that make a living out of deceiving small businesses."

ACCC Chairman Rod Sims

In September 2012, following ACCC court action, the Federal Court of Australia ordered three publishing companies, Elite Publishing Group Pty Ltd, Wiltshire Publishers Pty Ltd and Exclusive Media & Publishing Pty Ltd, to pay penalties totalling $400 000, and the companies' director, Mr Andrew Clifford, to pay $100 000 after they admitted that they had engaged in misleading and deceptive conduct, harassment and coercion, and unconscionable conduct in relation to advertising services that were never requested or provided.

Communications from the publishing companies led mostly small businesses to believe that they had already paid for or agreed to advertising in one of the companies' magazines, when in fact they had not. The companies would then invite the businesses to sign certain documents in order to receive complementary copies of the magazines.

The publishing companies would then claim the signed document was in fact an agreement to buy advertising services, and demand payment of around $500 for each, when in fact no such agreement was intended.

The companies admitted they used harassment and coercion and acted unconscionably when pursuing payment from some businesses. This included threatening legal proceedings, or representing that legal action had commenced against a business.

It was also admitted that while the companies represented that 500 copies of certain magazines carrying the businesses' advertisements would be distributed to various organisations, they never intended to, and never did, distribute 500 copies of the magazines for the purpose of providing advertising services.

The Court imposed injunctions by consent on all of the respondents, including a fourth company, Superior Publications Pty Ltd, restraining them from being involved in similar conduct for a period of five years. An injunction was also imposed by consent on Mr Clifford, restricting his management of corporations for five years.

6 Domestic and international collaboration

As scams commonly operate in a global environment, national and international cooperation is an essential part of effective prevention. This chapter outlines some collaborative efforts that the ACCC participated in during 2012.

6.1 The Australasian Consumer Fraud Taskforce

The Australasian Consumer Fraud Taskforce, established in 2005, comprises 23 federal and state government regulatory agencies and departments (including New Zealand) that have a responsibility for consumer protection in relation to fraudulent and scams activity.

The Taskforce's primary 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 growing number of government, business and community group partners. Partners recognise the seriousness of consumer fraud in Australasia, and play a vital role in disrupting scams activity and raising community awareness.

The Taskforce is part of the Mass-Market Global Fraud project of the International Consumer Protection Enforcement Network (ICPEN).

National Consumer Fraud Week

A key Taskforce initiative is the annual National Consumer Fraud Week, a coordinated information campaign to raise community awareness about scams. This initiative forms part of ICPEN's Global Consumer Fraud Prevention campaign.

2012 campaign—Slam scams!

The 2012 Fraud Week campaign, 'Slam scams!', ran from 19 to 25 March and raised community awareness of scam delivery methods so that Australians can identify and slam a scam at the point of contact and avoid victimisation.

'Slam scams!' highlighted the increasingly sophisticated approach by scammers in terms of how they deliver scams, taking advantage of new technology and communication methods to try and slip under one's radar. It also highlighted the fact that scammers are not afraid to adopt a personal touch such as contacting people at home, or trying to push people's buttons by playing on their emotions to evoke a sense of guilt, anxiety or fear. The key message of the campaign was to 'Slam a scam at the point of contact—press delete, throw it out, shut the door or just hang up'.

Campaign highlights included:

- Release of the ACCC's 2011 *Targeting Scams* report
- Launch of a new, pocket-sized edition of the ACCC's *Little Black Book of Scams*
- 'Slam scams!' launch evening event—Monday 19 March, the Grace Hotel Sydney (hosted by the ACCC)
- 'Consumer Fraud Offenders' forum—Monday 19 March, ASIC Sydney office (hosted by the AIC).

The campaign generated unprecedented media interest across all major metropolitan newspapers and radio stations, and several major television programs. ACCC Deputy Chair Dr Michael Schaper was interviewed on several breakfast television and current affairs programs including Channel 7 Sunrise, Channel 9 Today, ABC News Breakfast, Channel 7 News, Channel 9 News, Sky News and Channel 10 The Project. Dr Schaper was also interviewed on radio by 3AW Breakfast, ABC News Radio Breakfast, ABC Sydney 720 Mornings, 2UE Drive, ABC Ballarat Mornings, ABC Adelaide 891 Afternoons, 5AA Adelaide Afternoons, ABC Perth 720 Mornings, 2GB Ross Greenwood, and ABC Cairns. The campaign also featured on the front page of *The Age*, and was reported in all other Fairfax and News Ltd papers.

The estimated audience for the media attention generated on day one of Fraud Week 2012 was eight million people.

In 2012 the Partners Program added 20 new partners, expanding to a total of more than 120 from across the public, private and community sectors.

2013 campaign—Outsmart the scammers!

The ACFT's 2013 Fraud Week campaign, 'Outsmart the scammers!', will run from Monday 17 to Sunday 23 June and focus on helping Australians identify online shopping scams so that they can shop safely online without being duped.

Australian consumers 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.

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

Appendix 5 provides a list of ACFT members and partners.

6.2 The International Consumer Protection and Enforcement Network

The ICPEN comprises consumer protection authorities from almost 40 countries. 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 campaign is an education initiative aimed at informing consumers about fraud and raising awareness of scams through events and activities. The ACCC participates as part of its National Consumer Fraud Week campaign with the ACFT.

An important IPCEN initiative is e-consumer.gov (www.econsumer.gov), a website portal featuring a global online complaint 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 seven 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.

6.3 International Mass Marketing Fraud Working Group

Since February 2008 the ACCC has participated in the International Mass Marketing Fraud Working Group, which is comprised of a number of domestic and international law enforcement agencies. Participation assists the ACCC to combat cross-border mass-marketed fraud by:

- improving intelligence
- increasing opportunities for disruption of scam and/or fraud operations
- expanding public awareness and prevention measures
- enhancing cooperation and coordination in enforcement actions against mass marketed fraud activity.

6.4 The Cyber White Paper

In 2011 the Australian Government announced that it would release a Cyber White Paper to outline how government, industry and the community could work together to address the challenges and risks Australians will face from increased engagement in the digital economy. In 2012 the ACCC continued to work with the Department of Prime Minister and Cabinet and a range of other government departments.

A key initiative of the Cybercrime Working Group is the establishment of the Australian Cybercrime Online Reporting Network (ACORN) that would receive cybercrime reports from members of the public, allow users to access general and targeted educational advice, and refer reports to law enforcement and government agencies for further consideration.

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.

The ACORN Business Case proposes that the ACCC be represented in a Joint Management Group, which will be responsible for monitoring the ACORN's operation and resolving any issues requiring an urgent or multiagency response and/or updates to the ACORN's content or function.

6.5 Investment Scams Task Force

ACCC data: investment and real estate scams

Whilst the investment and real estate scams category was not in the top 10 scams reported to the ACCC in 2012, it recorded the third highest losses of all scam types, with $17 349 347 total reported financial losses. The conversion rate for this scam category was 32.4 per cent.

In 2012 law enforcement, regulatory and service delivery agencies across federal, state and territory governments continued to collaborate as part of 'Taskforce Galilee' to prevent and disrupt serious and organised fraudulent investment scams.

The level of superannuation and retirement savings in Australia is attractive to organised crime groups, and Australians approaching retirement who are looking to invest their savings have been urged to protect themselves.

These scams use highly sophisticated websites to trick consumers into thinking investment offers are legitimate. In many cases criminal groups contact potential victims through unsolicited cold calls.

Perpetrators of these fraudulent scams are skilled at using high-pressure sales tactics, over the phone and by email, to persuade victims to part with their money for what looks like attractive rates of return on what are actually non-existent investment opportunities.

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

The ACCC featured investment scams as part of its National Consumer Fraud Week campaign, issued a SCAMwatch radar, published a victims story, and alerted its Small Business Information Network and ACFT partners to the issue.

Led by the Australian Crime Commission, the Taskforce includes the ACCC, all Australian Crime Commission Board agencies, the Department of Broadband, Communications and the Digital Economy, the Department of Immigration and Citizenship, the Department of Human Services, representatives from Commonwealth, State and Territory Police and the Australian Transaction Reports and Analysis Centre.

6.6 Australian Transaction Reports and Analysis Centre partnership

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

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 below $10 000.

The ACCC uses this information to provide targeted education to affected consumers. More information about AUSTRAC can be found at: www.austrac.gov.au.

6.7 Organisation for Economic Co-operation and Development Committee on Consumer Policy

The Organisation for Economic Co-operation and Development Committee on Consumer Policy enhances the development and enforcement of effective consumer policies through research and analysis, exchange of information and development of guidelines to address problematic areas. Secure cross-border e-commerce remains a focus area with relevance to enforcement work and protection of consumers from scam activity. The ACCC participates as a member of the Australian delegation.

6.8 Support of overseas law enforcement efforts

Wherever possible the ACCC also supports the efforts of overseas law enforcement agencies to investigate and prosecute scam offenders.

In 2012 the ACCC assisted the Essex Police in obtaining evidence from an Australian retiree who had fallen victim to a scam committed by UK citizens. A UK court subsequently sentenced two defendants for their conduct against the individual.

In October 2012 the ACCC issued a SCAMwatch radar to support an announcement issued by several international agencies of the successful prosecution of scammers behind the most popular scam targeting Australians in 2011: the computer cold calling virus scam.

Case studies are provided on the following pages.

Case study: ACCC helps inheritance scam victim in UK prosecution

"Scammers are able to spin a complex web of lies to convince you that their story is true. Don't get caught up by slick tricks such as sophisticated websites and authentic looking documentation as they may not be the real deal."

ACCC Deputy Chair Delia Rickard

In 2012 a UK court sentenced two defendants for defrauding an Australian retiree of approximately $800 000. The ACCC assisted the victim in providing her testimony, which held significant weight in the case's proceedings.

The ACCC originally approached the victim after identifying that she was sending significant amounts of money overseas. The ACCC then advised her of its concerns that she had been targeted by a scam. It was subsequently revealed that the retiree had been the victim of a sophisticated scam. Following listing a home for sale, the retiree received an email purporting to be from a reputable organisation 'Hong Kong and Shanghai Banking Corporation' (HSBC) via a UK email address. The email, allegedly directed to this retiree only, was from a Mr Vincent Cheng. Mr Cheng had identified $US22.5 million deposited in his UK bank branch by an Iraqi Brigadier and his son. The father and son had both been killed leaving no relatives. Mr Cheng proposed sharing the funds in a business proposition with the co operation of the retiree. The retiree would then 'legally' facilitate transaction of the funds.

The retiree responded to Mr Cheng, taking care to assess the legitimacy of the offer. Mr Cheng emailed detailed information including links to seemingly genuine documentation such as Mr Cheng's biography, a website and telephone numbers. Further emails convinced the consumer of the proposal's authenticity including contact with a barrister, a confidentiality agreement, telephone contact with various individuals in the UK, creation of a UK financial account and finally, an email confirming $US 22.5 million deposited into the retiree's account.

The retiree was then asked to pay funds to facilitate access to the inheritance including charges for administration, a diligence certificate, an indemnity bond, and revenue and conversion charges.

Following delays accessing the money the consumer visited the UK to meet with the individuals involved. After the second visit, the realisation hit that this was a fraud. In retrospect, the victim acknowledged that 'Mr Cheng' had identified the retiree following the listing of the family home for sale.

The scam had a severe impact on the retiree who lost approximately $800 000 funded by savings, selling the family home and through loans from family members. In addition to financial difficulty, the retiree faced family difficulties and significant health issues.

The UK police involved in the case contacted the Australian victim who verified the loss in a witness statement. The retiree, with the support of the ACCC, gave evidence to the UK court from Australia.

The Court ultimately sentenced two defendants for money laundering as follows:

- Kevin Amadin—four and a half years' imprisonment
- Irene Edeigba—12 months' imprisonment suspended for 18 months (her sentence was more lenient due to her pleading guilty earlier as well as giving evidence against her co-defendant).

The Court has since awarded compensation of £47 634 to be paid to the Australian victim.

Case study: computer cold virus scammers caught

In October 2012 US authorities won court orders to close down and freeze funds of scammers connected to the Microsoft scam after international collaboration between authorities in targeted nations (see chapter 6); the Australian Communications and Media Authority, the US Federal Trade Commission (FTC), the Canadian Radio-television and Telecommunications Commission and the UK's Serious Organised Crime Agency. The FTC also received assistance from Microsoft and other computer companies.

A US District Court Judge ordered a to halt six alleged tech support scams mostly based in India targeting English-speaking consumers using telemarketing boiler rooms or placing ads with Google which appeared when searching for the consumer's computer company's tech support telephone number. Scammers hoped to avoid detection by consumers and law enforcers by using virtual offices and using 80 different domain names and 130 different phone numbers but were charged with violating the Federal Trade Commission Act. Fourteen corporate defendants and 17 individuals were targeted in the FTC case.

In October the ACCC issued a SCAMwatch alert about the outcome but also urged Australians to continue to be alert to this scam, as this action caught just a handful of the perpetrators behind a global scheme.

SCAMwatch advised Australians to follow these 'protect yourself' messages:

- **Suspect**: Don't accept anything at face value—if it sounds unlikely or too good to be true, it probably is.
- **Think**: Recognise the signs—if you're being pressured to act, disclose personal details or send money to a stranger, it's almost certainly a scam. For example, Microsoft never makes unsolicited phone calls about its products.
- **Report**: Act quickly—tell SCAMwatch and stop scammers in their tracks.
- **Ignore**: Never respond. Just hang up, or delete the SMS or email after reporting.

7 Conclusions and future challenges

While the ACCC undertakes considerable efforts to educate and empower consumers, such as through the SCAMwatch website, the importance of raising community awareness about the need to remain vigilant against scams activity will always remain a high priority. With over $93 million reported lost to scams in 2012, as well as the unquantifiable and devastating non-financial costs experienced by many victims, it is crucial that Australian consumers and businesses are able to identify scams and avoid victimisation in the first instance.

In addition to helping the individual, the ACCC also recognises the importance of working with industry, other regulators, and local and international law enforcement agencies to disrupt scams. Building upon its successful collaboration with the online dating and romance industry in 2012, the ACCC will continue to work with key industries where consumer detriment arises. In line with the fact that more Australians are shopping online and scam reports continue to increase, in 2013 the ACCC will focus its efforts on the online retail industry. The ACCC will also continue to work with members and partners of the Australasian Consumer Fraud Taskforce to deliver a coordinated response to scams in Australia and New Zealand.

Where possible the ACCC will take enforcement action against the perpetrators of scams. In 2012 the ACCC took successful court action against individuals involved in the TVI Express pyramid selling scheme, and against traders falsely signing up small businesses to advertising services. It also provided assistance to the Essex Police in its case against a global scam that saw some defendants sentenced and an Australian victim awarded compensation. These efforts show that scammers cannot always evade prosecution.

The scams landscape will continue to evolve in line with developments in technology and how communication channels are used. For many Australians, mobile technology, smart phone devices, connecting with family and friends online, and shopping or banking over the internet is now a daily part of life. It is therefore unsurprising that in 2012 the ACCC saw an increase in reports and associated losses of scams sent via mobile phones as a way of delivering scams direct to people's pockets.

At the same time scammers are also increasingly sophisticated in their operations, using professional business models such as call centres, virtual offices, sophisticated or mirror websites and even their own version of clients lists—'victims lists'—to dupe people. Scams are also now regularly committed overseas and on a global scale, with the potential to reach millions of potential victims at the click of a button.

The speed in which developments in technology and communications occur, and the modus operandi used by scammers, presents considerable challenges to law enforcement agencies. The ACCC and international law enforcement agencies will continue in their efforts to stay one step ahead of scammers.

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 2012 scam categories by state and territory.

Overall New South Wales saw the greatest amount of scam reports (23.5 per cent), followed by Queensland (21 per cent), Victoria (18 per cent) and South Australia (12.5 per cent). Contacts received from the remaining state and territories were below 10 per cent.

The ACCC also received reports from overseas, with 8 per cent of total contacts identified as originating from individuals based outside Australia.

Australian Capital Territory

Scam category	Amount reported lost	Contacts	Contacts reporting loss	Less than 10k lost	Greater than 10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	$1 647 635	1 069	74	64	10	995	6.9%
Dating and romance (incl. adult services)	$438 904	79	34	23	11	45	43.0%
Lottery and sweepstakes	$394 082	425	13	8	5	412	3.1%
Unexpected prizes	$234 562	242	7	5	2	235	2.9%
Investment seminars and real estate	$145 988	30	13	8	5	17	43.3%
Job and employment	$134 949	77	10	7	3	67	13.0%
Online auction and shopping (incl. classifieds)	$115 973	305	99	97	2	206	32.5%
Phishing and identity theft (incl. banking and online account)	$91 508	392	22	17	5	370	5.6%
Computer prediction software (incl. betting)	$43 750	26	7	6	1	19	26.9%
Computer hacking (incl. malware and viruses)	$15 874	462	47	47	0	415	10.2%
False billing	$13 550	104	15	14	1	89	14.4%
Health and medical	$2 899	10	4	4	0	6	40.0%
Mobile phone (ringtones, competitions and missed calls)	$1 147	66	14	14	0	52	21.2%
Chain letter/pyramid scheme	$600	28	2	2	0	26	7.1%
Door-to-door and home maintenance	$450	16	1	1	0	15	6.3%
Spam and ‘free’ internet offers	$360	32	6	6	0	26	18.8%
Fax back	$0	3	0	0	0	3	0.0%
Psychic and clairvoyant	$0	1	0	0	0	1	0.0%
Other (scams which do not fit into predefined categories)	$600	24	1	1	0	23	4.2%
Total	**$3 282 831**	**3 391**	**369**	**324**	**45**	**3 022**	**10.9%**

New South Wales

Scam category	Amount reported lost	Contacts	Contacts reporting loss	Less than 10k lost	Greater than 10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	$7 170 379	6 637	554	481	73	6 083	8.3%
Dating and romance (incl. adult services)	$5 650 123	521	234	159	75	287	44.9%
Investment seminars and real estate	$5 126 382	160	45	23	22	115	28.1%
Online auction and shopping (incl. classifieds)	$1 104 586	1 913	752	730	22	1 161	39.3%
Computer prediction software (incl. betting)	$1 088 004	199	100	57	43	99	50.3%
Computer hacking (incl. malware and viruses)	$762 654	2 788	260	258	2	2 528	9.3%
Lottery and sweepstakes	$475 868	1 936	55	44	11	1 881	2.8%
Phishing and identity theft (incl. banking and online account)	$449 889	2 126	112	102	10	2 014	5.3%
Job and employment	$430 537	586	49	38	11	537	8.4%
Unexpected prizes	$365 557	1 298	42	35	7	1 256	3.2%
False billing	$107 140	626	128	126	2	498	20.4%
Chain letter/pyramid scheme	$64 880	105	7	5	2	98	6.7%
Door-to-door and home maintenance	$49 992	66	16	14	2	50	24.2%
Spam and ‘free’ internet offers	$6 743	148	29	29	0	119	19.6%
Mobile phone (ringtones, competitions and missed calls)	$6 069	320	78	78	0	242	24.4%
Health and medical	$5 281	31	10	10	0	21	32.3%
Psychic and clairvoyant	$2 642	18	3	3	0	15	16.7%
Fax back	$0	15	0	0	0	15	0.0%
Other (scams which do not fit into predefined categories)	$1 736 955	201	21	16	5	180	10.4%
Total	**$24 603 681**	**19 694**	**2 495**	**2 208**	**287**	**17 199**	**12.7%**

Northern Territory

Scam category	Amount reported lost	Contacts	Contacts reporting loss	Less than 10k lost	Greater than 10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	$308 657	272	26	21	5	246	9.6%
Lottery and sweepstakes	$67 601	99	6	4	2	93	6.1%
Computer prediction software (incl. betting)	$55 120	13	7	6	1	6	53.8%
Online auction and shopping (incl. classifieds)	$42 323	78	23	22	1	55	29.5%
Dating and romance (incl. adult services)	$37 469	12	9	8	1	3	75.0%
Phishing and identity theft (incl. banking and online account)	$28 444	71	5	4	1	66	7.0%
Unexpected prizes	$3 400	100	1	1	0	99	1.0%
Spam and ‘free’ internet offers	$1 773	7	3	3	0	4	42.9%
False billing	$1 750	23	2	2	0	21	8.7%
Computer hacking (incl. malware and viruses)	$1 398	92	5	5	0	87	5.4%
Chain letter/pyramid scheme	$1 200	6	1	1	0	5	16.7%
Psychic and clairvoyant	$306	2	1	1	0	1	50.0%
Investment seminars and real estate	$0	4	0	0	0	4	0.0%
Job and employment	$0	23	0	0	0	23	0.0%
Mobile phone (ringtones, competitions and missed calls)	$0	12	0	0	0	12	0.0%
Door-to-door and home maintenance	$0	0	0	0	0	0	0.0%
Fax back	$0	0	0	0	0	0	0.0%
Health and medical	$0	0	0	0	0	0	0.0%
Other (scams which do not fit into predefined categories)	$1 800	9	3	3	0	6	33.3%
Total	**$551 241**	**823**	**92**	**81**	**11**	**731**	**11.2%**

Queensland

Scam category	Amount reported lost	Contacts	Contacts reporting loss	Less than 10k lost	Greater than 10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	$7 784 360	5 981	501	418	83	5 480	8.4%
Dating and romance (incl. adult services)	$4 347 930	532	241	171	70	291	45.3%
Investment seminars and real estate	$3 502 938	151	53	29	24	98	35.1%
Online auction and shopping (incl. classifieds)	$840 249	1 819	564	541	23	1 255	31.0%
Computer prediction software (incl. betting)	$698 856	162	75	50	25	87	46.3%
Job and employment	$543 222	518	61	54	7	457	11.8%
Lottery and sweepstakes	$539 960	1 935	44	34	10	1 891	2.3%
Phishing and identity theft (incl. banking and online account)	$216 538	1 846	100	94	6	1 746	5.4%
False billing	$155 746	515	88	84	4	427	17.1%
Computer hacking (incl. malware and viruses)	$140 254	2 273	189	186	3	2 084	8.3%
Unexpected prizes	$62 459	1 203	29	28	1	1 174	2.4%
Door-to-door and home maintenance	$27 693	72	15	14	1	57	20.8%
Mobile phone (ringtones, competitions and missed calls)	$14 628	226	48	47	1	178	21.2%
Spam and ‘free’ internet offers	$5 438	141	20	20	0	121	14.2%
Chain letter/pyramid scheme	$4 550	119	6	6	0	113	5.0%
Psychic and clairvoyant	$3 198	33	4	4	0	29	12.1%
Fax back	$1 820	15	1	1	0	14	6.7%
Health and medical	$849	27	11	11	0	16	40.7%
Other (scams which do not fit into predefined categories)	$33 782	190	18	17	1	172	9.5%
Total	**$18 924 470**	**17 758**	**2 068**	**1 809**	**259**	**15 690**	**11.6%**

South Australia

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 (incl. adult services)	$2 951 377	359	157	112	45	202	43.7%
Advanced fee/up-front payment	$2 876 540	3 073	269	235	34	2 804	8.8%
Investment seminars and real estate	$2 181 281	101	30	16	14	71	29.7%
Online auction and shopping (incl. classifieds)	$368 626	1 094	371	361	10	723	33.9%
Computer prediction software (incl. betting)	$329 555	69	32	21	11	37	46.4%
Unexpected prizes	$218 795	818	29	24	5	789	3.5%
Lottery and sweepstakes	$207 721	1 348	30	26	4	1 318	2.2%
Job and employment	$201 131	418	38	34	4	380	9.1%
Phishing and identity theft (incl. banking and online account)	$109 273	1 047	53	51	2	994	5.1%
Psychic and clairvoyant	$94 349	20	13	12	1	7	65.0%
Computer hacking (incl. malware and viruses)	$48 666	1 236	95	94	1	1 141	7.7%
False billing	$39 184	293	59	59	0	234	20.1%
Door-to-door and home maintenance	$25 466	51	10	9	1	41	19.6%
Chain letter/pyramid scheme	$23 690	82	9	8	1	73	11.0%
Health and medical	$6 581	18	7	7	0	11	38.9%
Spam and ‘free’ internet offers	$2 957	115	18	18	0	97	15.7%
Mobile phone (ringtones, competitions and missed calls)	$1 000	173	27	27	0	146	15.6%
Fax back	$0	12	0	0	0	12	0.0%
Other (scams which do not fit into predefined categories)	$37 062	158	16	14	2	142	10.1%
Total	**$9 723 254**	**10 485**	**1 263**	**1 128**	**135**	**9 222**	**12.0%**

Tasmania

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 (incl. adult services)	$1 269 931	40	15	11	4	25	37.5%
Computer prediction software (incl. betting)	$60 400	12	7	4	3	5	58.3%
Lottery and sweepstakes	$49 064	245	6	5	1	239	2.4%
Online auction and shopping (incl. classifieds)	$49 062	161	45	45	0	116	28.0%
Advanced fee/up-front payment	$48 940	600	31	29	2	569	5.2%
Computer hacking (incl. malware and viruses)	$16 832	249	18	18	0	231	7.2%
Investment seminars and real estate	$15 950	15	3	2	1	12	20.0%
Unexpected prizes	$9 491	152	7	7	0	145	4.6%
False billing	$9 289	48	13	13	0	35	27.1%
Job and employment	$4 575	26	2	2	0	24	7.7%
Phishing and identity theft (incl. banking and online account)	$3 860	192	9	9	0	183	4.7%
Spam and ‘free’ internet offers	$437	13	2	2	0	11	15.4%
Door-to-door and home maintenance	$250	4	1	1	0	3	25.0%
Health and medical	$151	2	2	2	0	0	100.0%
Psychic and clairvoyant	$120	1	1	1	0	0	100.0%
Mobile phone (ringtones, competitions and missed calls)	$118	26	3	3	0	23	11.5%
Chain letter/pyramid scheme	$0	15	0	0	0	15	0.0%
Fax back	$0	0	0	0	0	0	0.0%
Other (scams which do not fit into predefined categories)	$900	12	1	1	0	11	8.3%
Total	**$1 539 370**	**1 813**	**166**	**155**	**11**	**1 647**	**9.2%**

Victoria

Scam category	Amount reported lost	Contacts	Contacts reporting loss	Less than 10k lost	Greater than 10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	$4 734 784	4 942	421	378	43	4 521	8.5%
Dating and romance (incl. adult services)	$4 152 758	403	195	128	67	208	48.4%
Investment seminars and real estate	$3 206 267	107	38	19	19	69	35.5%
Computer prediction software (incl. betting)	$1 050 880	128	70	48	22	58	54.7%
Online auction and shopping (incl. classifieds)	$903 641	1 482	629	607	22	853	42.4%
Job and employment	$798 709	476	47	39	8	429	9.9%
Phishing and identity theft (incl. banking and online account)	$324 507	1 475	100	95	5	1 375	6.8%
Computer hacking (incl. malware and viruses)	$145 184	2 166	235	233	2	1 931	10.8%
Psychic and clairvoyant	$140 702	22	6	4	2	16	27.3%
False billing	$112 436	490	73	72	1	417	14.9%
Chain letter/pyramid scheme	$103 250	117	6	4	2	111	5.1%
Lottery and sweepstakes	$90 127	1 501	54	50	4	1 447	3.6%
Unexpected prizes	$73 944	959	43	41	2	916	4.5%
Mobile phone (ringtones, competitions and missed calls)	$37 979	217	55	54	1	162	25.3%
Health and medical	$26 074	23	8	7	1	15	34.8%
Door-to-door and home maintenance	$11 548	90	14	14	0	76	15.6%
Spam and ‘free’ internet offers	$3 555	119	22	22	0	97	18.5%
Fax back	$0	9	0	0	0	9	0.0%
Other (scams which do not fit into predefined categories)	$933 728	179	18	14	4	161	10.1%
Total	**$16 850 073**	**14 905**	**2 034**	**1 829**	**205**	**12 871**	**13.6%**

Western Australia

Scam category	Amount reported lost	Contacts	Contacts reporting loss	Less than 10k lost	Greater than 10k lost	Contacts reporting no loss	Conversion rate
Advanced fee/up-front payment	$2 368 059	2 859	267	243	24	2 592	9.3%
Dating and romance (incl. adult services)	$2 269 015	214	99	61	38	115	46.3%
Investment seminars and real estate	$755 070	85	22	11	11	63	25.9%
Online auction and shopping (incl. classifieds)	$393 043	823	300	294	6	523	36.5%
Computer prediction software (incl. betting)	$366 088	62	22	10	12	40	35.5%
Phishing and identity theft (incl. banking and online account)	$298 695	830	32	31	1	798	3.9%
Job and employment	$288 986	226	34	27	7	192	15.0%
Computer hacking (incl. malware and viruses)	$138 978	1 092	110	107	3	982	10.1%
False billing	$94 881	254	62	59	3	192	24.4%
Unexpected prizes	$72 021	648	12	10	2	636	1.9%
Chain letter/pyramid scheme	$52 399	63	4	2	2	59	6.3%
Lottery and sweepstakes	$43 652	784	16	15	1	768	2.0%
Door-to-door and home maintenance	$6 561	32	6	6	0	26	18.8%
Health and medical	$5 076	8	3	3	0	5	37.5%
Spam and ‘free’ internet offers	$3 250	61	8	8	0	53	13.1%
Mobile phone (ringtones, competitions and missed calls)	$2 239	122	24	24	0	98	19.7%
Fax back	$0	5	0	0	0	5	0.0%
Psychic and clairvoyant	$0	5	0	0	0	5	0.0%
Other (scams which do not fit into predefined categories)	$32 656	93	12	11	1	81	12.9%
Total	**$7 190 669**	**8 266**	**1 033**	**922**	**111**	**7 233**	**12.5%**

Appendix 2: 2012 SCAMwatch radars

Beware of distress emails targeting the APY lands

January 2012: SCAMwatch and Consumer and Business Services in South Australia are warning people throughout the Anangu Pitjantjatjara Yankunytjatjara (APY) lands to beware of scam distress emails targeting the area.

Beware of phone scams—2011 Targeting Scams report

March 2012: SCAMwatch is continuing to warn Australians to beware of scams delivered by phone with the ACCC receiving over 43 000 reports of scams perpetrated this way in 2011.

Beware of directory listing scams targeting small businesses

April 2012: SCAMwatch is advising businesses to beware of unsolicited faxes offering paid listings in scam online directories.

Beware of native language call scams

May 2012: SCAMwatch is advising consumers to beware of scammers who call, speaking in the consumer's native language and requesting money.

Scam scratchies strike again

May 2012: SCAMwatch is advising consumers to continue to be on the look out for scam scratchie cards in their letterbox. You may think you're a big winner but scammers will ask you for thousands to claim a prize that never arrives.

Update—Beware of carbon price scams

Updated June 2012: SCAMwatch is warning consumers and businesses to be on the look out for carbon price scams, particularly calls asking for personal information in order to receive compensation.

Beware of 'voucher prize' scam text messages

June 2012: SCAMwatch is warning consumers not to respond to text messages which claim you have won a voucher, when in fact you are entering into an expensive mobile premium SMS service.

Protect your retirement savings from investment scammers

July 2012: SCAMwatch and the Australian Crime Commission Board are urging Australians to protect themselves from the growing threat of investment scams. Investment scammers are commonly based offshore and target Australia because of high levels of superannuation and retirement savings.

'Hitman' scam resurfaces

July 2012: SCAMwatch is warning Australians to beware of SMS death threats from scammers claiming to be 'hitmen' hired to kill the SMS recipient unless they send cash.

Beware of reclaim scams

July 2012: SCAMwatch is warning you to be aware of scam calls or emails claiming that you are entitled to reclaim fees or rebates.

Update—Beware of carbon price scams

August 2012: SCAMwatch is warning consumers and businesses to be on the look out for carbon price scams, particularly calls asking for personal information in order to receive compensation.

With one month left to lodge your tax return, beware of tax time scams

September 2012: SCAMwatch and the Australian Taxation Office (ATO) are urging consumers and small businesses to be aware of scam calls or emails around tax time.

Computer cold call virus scam—scammers outsmarted!

October 2012: Joint action between three international regulators has thwarted a massive global phone scam, with US authorities winning court orders to close down and freeze funds of imposters posing as Microsoft employees offering to fix PC viruses.

With Halloween around the corner, beware of scareware

October 2012: With Halloween around the corner, SCAMwatch urges you to be alert to a new type of scareware doing the rounds where scammers try and scare you into handing over money in order to regain control of your computer.

Scammers continue to impersonate government officials

October 2012: SCAMwatch is warning consumers to remain vigilant against scammers impersonating government officials with false claims of owed money.

Don't be horsed around by scammers this spring racing season

November 2012: SCAMwatch is warning punters not to be fooled by scammers pedalling sports investment scams this spring racing season.

Beware of scam surveys and offers misusing household names

November 2012: SCAMwatch is warning 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.

Watch out for fake flight itineraries landing in your inbox

SCAMwatch is warning travellers to watch out for scam emails with fake flight itineraries attached—these attachments may harbour malicious software.

Don't be fooled by scams this festive season

December 2012: SCAMwatch is warning people to be on the lookout this festive season not just for flying reindeer and bargain gifts but also scam surprises wrapped up as the real deal.

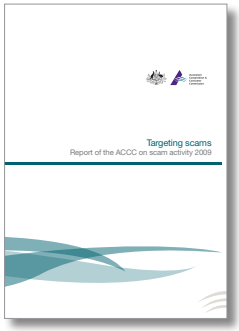
Appendix 3: ACCC scam-related resources for consumers and businesses

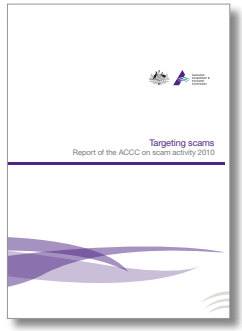
SCAMwatch

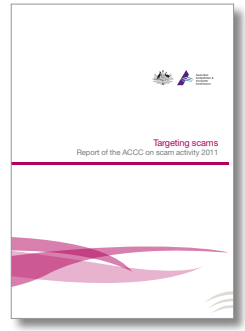
SCAMwatch website (www.scamwatch.gov.au)

SCAMwatch Twitter profile (@SCAMwatch_gov)

Annual reports



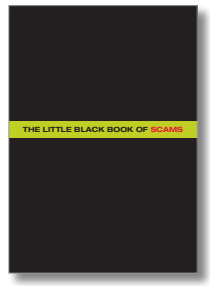




Targeting scams: Report of the ACCC on scam activity—2009, 2010 and 2011 editions

Publications

The Little Black Book of Scams
(pocket-sized edition)



The Little Black Book of Scams
(comprehensive version)

Factsheets

'Small business scams' factsheet

'Phishing scams' factsheet

'Money transfer scams' factsheet

'Sports investment scams' factsheet

'Lotteries, sweepstakes and competition scams' factsheet

2012 Fraud Week campaign resources

Campaign image and postcard design

Campaign web button

Campaign web banner

Appendix 4: Key ACCC media releases and communications initiatives

2012 ACCC scam media releases

ACCC and ACNC provide tips on how to donate safely this festive season—14 December

ACCC Deputy Chair Michael Schaper updates WA community on carbon price claims and small business scams—18 October

Publishing companies and director to pay $500 000 in penalties for unconscionable conduct and harassment—20 September

'I Bought What' ACCC internet sweep focuses on consumers' repair, replace, refund rights online—18 September

ACCC takes action against pyramid scheme operator—20 July

$200 000 penalty for TVI Express pyramid selling scam—21 May

ACCC and telco ombudsman tackle phone and SMS scam—22 March

ACCC: Small business must be alert to scams—20 March

Phone No. 1 choice for scam delivery: 'Slam Scams!' Fraud Week campaign—19 March

Scam reports almost double for second consecutive year: ACCC launches targeting scams report—19 March

ACCC launches guidelines to help dating websites protect consumers from scams—14 February

2012 Scam Survey now online—17 January

2012 ACCC speeches containing scam messages

Deputy Chair, Michael Schaper—SME Regulation: Building Better Policy Symposium, Wellington, New Zealand—20 September

Chairman, Rod Sims—Law Council of Australia

Chairman, Rod Sims —Committee for Economic Development of Australia, Sydney—14 June

Chairman, Rod Sims—National Consumer Fraud Week, Sydney—19 March

Commissioner, Sarah Court—Australian Council on Children and the Media conference, Melbourne—9 March

Chairman, Rod Sims—Australia-Israel Chamber of Commerce, Melbourne—20 February

Appendix 5: 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 Broadband, Communications and the Digital Economy

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 Northern Territory
Consumer Affairs Victoria
Fair Trading New South Wales
Queensland Office of Fair Trading
South Australia Office of Consumer and Business Affairs
Tasmanian Office of Consumer Affairs and Fair Trading
Western Australia Department of Commerce

Representatives of the state and territory police

New South Wales Police Service
Queensland Police Service
Northern Territory Police Force
State and Territory Police Commissioners

2012 Taskforce partners

Principal partners

Australian Communications Consumer Action Network
BankWest
CarsGuide
Commonwealth Bank
Consumer Action Law Centre
Facebook
Fairfax Media
Gumtree
Holiday Coast Credit Union
Horseyard.com.au
Microsoft
PayPal
Telstra
The Westpac Group (including Westpac Bank, St.George Bank and BankSA)
Trading Post
Western Union
Yahoo

Partners

Consumer advocacy (general)

CHOICE
Public Interest Advocacy Centre

Legal centres

National Association of Community Legal Centres
Peninsula Community Legal Centres

Ombudsman services

Commonwealth Ombudsman
Energy and Water Ombudsman of NSW
Fair Work Ombudsman
Telecommunications Industry Ombudsman

Financial institutions and services

Abacus—Australian Mutuals
Adelaide Bank
ANZ Bank
Australian Bankers' Association
Australian National Audit Office
Bendigo Bank
ComSuper
Financial and Consumer Rights Council
Police Credit Union
Suncorp Metway
Visa

Social/welfare/community bodies

Alexandra District Hospital
Australian Association of Social Workers
Australian Federation of Disability Organisations
Australian Financial Counselling and Credit Reform Association
Better Hearing Australia Vic Inc.
Brotherhood of St Laurence
Comcare
Country Women's Association of Australia
Cranbourne Information and Support Service
CRS Australia
Department of Human Services
Diamond Valley Community Support
Indigenous Consumer Assistance Network
Laverton Community Centre
Mental Health Council of Australia
Neighbourhood Watch
Sane Australia
Social Securities Appeal Tribunal
Western Australia Council of Social Services Inc.
Whittlesea Community Connections

Online shopping, security and computer bodies

Ailean
auDA
AusCERT
Australian Computer Society
Australian Mobile Telco Association
Australian Telecommunications Users Group

Communications Alliance

Community Technology Centres Association

eBay

Internet Industry Association

Optus

Surete Group

Symantec

Seniors associations

Australian Seniors Computer Club Association

Council on the Ageing—Australian Capital Territory

Council on the Ageing—Northern Territory

Council on the Ageing—Queensland

Council on the Ageing—South Australia

Council on the Ageing—Tasmania

Council on the Ageing—Western Australia

RSL NSW

RSL SA

RSL TAS and Vic

Seniors Information Victoria

Gaming bodies

Australian Casino Association

BetFair

Sportsalive.com

Tabcorp

Miscellaneous

Australia Post

Australian Trade Commission

Cootamundra Police Station

Crime Stoppers

Migration Review Tribunal and Refugee Review

National Archives of Australia

National Measurement Institute

Office of the Australian Information Commissioner

Tenants Union of Victoria

Victoria Police Service

2013 Taskforce Partners

As at 1 June 2012 the following entities have confirmed their partnership with the Taskforce for 2013.

Consumer advocacy (general)

CHOICE

Consumers Federation of Australia

Indigenous Consumer Assistance Network

Public Interest Advocacy Centre

Legal centres

Consumer Action Law Centre

National Association of Community Legal Centres

Peninsula Community Legal Centre

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

Real Estate Institute Australia

Tasmanian Small Business Council

The Institute of Chartered Accountants of Australia

The Pharmacy Guild Australia

Ombudsman services

Commonwealth Ombudsman

Energy & Water Ombudsman of NSW

Energy & Water Ombudsman of Victoria

Fair Work Ombudsman

Telecommunications Industry Ombudsman

Financial institutions and services

Abacus—Australian Mutuals

Adelaide Bank

ANZ

Association of Independent Retirees

Association of Superannuation Funds Australia

Australian Bankers' Association
Australian Super
Bankwest
Bendigo Bank
Commonwealth Bank
ComSuper
Financial & Consumer Rights Council Victoria
MoneyGram International
National Australia Bank
PayPal Australia
SunCorp-Metway
The Westpac Group
Western Union

Social/welfare/community bodies

Alexandra District Hospital
Australian Charities and Not-for-profits Commission
Australian Council of Social Services
Brotherhood of St Laurence
Child Support Agency
Citizens Advice Bureau (ACT)
Comcare
Country Women's Association of Australia
CRS Australia
Dept of Human Services (VIC)
Diamond Valley Community Support
Federation of Ethnic Communities Council of Australia
Financial Counselling Australia
Mental Health Council of Australia
Neighbourhood Watch Victoria
Social Securities Appeal Tribunal
Wesley Mission
Western Australia Council of Social Services Inc
Whittlesea Community Connections

Online classifieds and auction shopping service providers

Cars Guide

Carsales.com.au

Deals Direct

eBay Australia

GraysOnline

Gumtree

Trading Post

Online dating services

3H Group Pty Ltd—OasisActive.com

eHarmony Australia

Slinky Dating Australia Ltd

Internet security and computer bodies

Ailean

AusCERT

Australian Computer Society

Centre for Internet Safety (University of Canberra)

Community Technology Centres Association

Internet Industry Association

Microsoft

Norton by Symantec

Sophos

Surete Group

Trustedwebsites.com.au

Yahoo

Telecommunications service providers (including (VoIP)

Australian Communications Consumer Action Network

Australian Mobile Telecommunications Association

Communications Alliance

Department of Broadband, Communications and the Digital Economy

Optus

Telstra

Seniors associations

Australian Seniors Computer Clubs Association

Council on the Ageing Australia

Council on the Ageing—SA

Council on the Ageing—VIC

Council on the Ageing—WA

RSL NSW

RSL SA

Seniors Information Victoria

Gaming bodies

Australian Casino Association

Australian Gaming Council

Betfair

Miscellaneous

Australia Post

Crime Stoppers Australia

Curtin University of Technology

Migration Review Tribunal & Refugee Review Tribunal

NSW Department of Attorney General & Justice

Office of the Australian Information Commissioner

Qantas

The Newspaper Works

Victoria Police

Australian
Competition &
Consumer
Commission

www.accc.gov.au