Australian Competition & Consumer Commission

Targeting scams

Report of the ACCC on scam activity 2010

Peter Kell, Chairman, Australasian Consumer Fraud Taskforce

Foreword

The Australian Competition and Consumer Commission's (ACCC) second annual report on cyber crime and scam activity highlights the significant growth we continue to see in this area, with the number of scams reported in 2010 more than double that in 2009. Coming into contact with a scam is one of the fastest growing reasons why consumers contact the ACCC, and the ACCC is strongly committed to dealing with consumer fraud and scams.

This report is designed to raise awareness of the nature and extent of the problem of cyber crime and scams targeted at consumers and small businesses. We believe that more consumers and small businesses are now willing to report scams, which allows the ACCC to issue more timely warnings. The report explains the key trends the ACCC observed in 2010. It documents the year's successes in responding to scams, and discusses the difficulties and challenges for law enforcement.

This year we have sought to provide more information about the effects of cyber crime and scams on the lives of individuals. Consumers and small businesses are often reluctant to come forward with their story, so the report sets out several case studies that illustrate the impact that scams can have. This theme will be expanded upon in the Australasian Consumer Fraud Taskforce (ACFT) 2011 Fraud Week campaign, *Scams: It's Personal*.

One challenge in 2010 was the continual evolution in the use of technologies by cyber criminals and scam operators. An example was the unexpected resurgence of scams being delivered by telephone—while unsolicited telephone calls have long been a part of scam operations, they have received less attention in recent years. The increasing popularity of inexpensive voice-over-internet services is a likely cause of the 23.5 per cent increase in scams delivered by phone compared to 2009. This will be an area of focus for the ACCC in 2011.

This report also highlights the broad ranging cooperative work undertaken by the ACCC with other regulators and law enforcement agencies, as well as consumer bodies and private industry. Both domestic and international networks and partnerships are crucial to tackling the increasing sophistication and global nature of cyber crime and scams. Through my role as Chair of the ACFT, the ACCC is heavily involved in working with other consumer protection agencies to disrupt scams, enforce the law and educate consumers, and their support is critical in all these activities.

Peter Kell
Deputy Chairman, ACCC
Chairman, Australasian Consumer Fraud Taskforce

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

First published by the ACCC 2011

ACCC 02/11_40522_226

www.accc.gov.au

Contents

1 Snapshot of 2010

- In 2010, the ACCC received more than 42 000 reports of scams, more than double that in 2009. Reporting a scam is one of the fastest growing reasons for contacting the ACCC. The ACCC believes that while scam activity is increasing, a positive development is the growth in the number of people reporting these scams.
- Scam losses reported to the ACCC from cyber crime and scams totalled more than $63 million in 2010. This is slightly less than reported losses in 2009. This amount is based solely on information provided by consumers reporting scams to the ACCC. Actual losses are likely to be higher as many scams go unreported and the ACCC is only one of several agencies that receive scam reports.
- Most consumers reported no financial loss, however 16 per cent of consumers who reported a scam reported losses between $1.00 and $4 million.
- Just over half of the scams reported to the ACCC concerned mass marketed advance fee fraud (MMAFF), the most reported scam category in 2010. This category includes advance fee/up-front payment, lottery and sweepstakes, unexpected prizes, and dating and romance scams (including adult services).
- The reports of scams delivered online (including internet and email) increased, from 14 101 reports in 2009 to 19 074 in 2010. The online delivery method was used in 45 per cent of scams reported in 2010.
- There was a steep increase in the reporting of scams initiated by unsolicited telephone calls from 2036 reports in 2009 to 14 144 in 2010. Scams delivered by telephone represented 33.4 per cent of the total reported in 2010. Reports indicate that calls may have originated from overseas call centres, likely taking advantage of cheap or free voice-over-internet services. This will remain a major area of focus for the ACCC in 2011, including for consumer education.
- Many unsolicited scam telephone calls misled consumers to believe their computer had a virus, and in some cases the call facilitated computer hacking by convincing consumers to provide scammers with remote access.
- In 2010 the ACCC observed increases in scammers impersonating representatives from well-known government departments and private companies. Many of these scams were also delivered through unsolicited telephone calls.
- The ACCC continued to receive complaints about online auction and shopping scams, false billing, banking and online account scams, job and employment scams, dating and romance scams, and computer prediction software scams.
- Personally targeted scams increased in 2010. Victims were particularly vulnerable to these scams if they had made their personal details readily available online, for example through social networking websites.
- Scams continued to target people of all ages but the majority who provided their age when contacting the ACCC were between 35 and 44 years of age.
- In 2010 law enforcement intelligence reports increasingly showed that scam operators ranged from opportunistic individuals undertaking relatively small actions through to major international criminal networks. Recently the latter category has grown, generating greater risks for consumers both within Australia and overseas, exploiting new technologies and global opportunities.
- The ACCC's SCAMwatch website (www.scamwatch.gov.au) received more than 500 000 unique visitors and in excess of 5.3 million hits during 2010. SCAMwatch issued 38 radar alerts warning consumers about specific scams. The ACCC also distributed more than 102 000 copies of its scam-related publications in 2010.
- The ACCC worked extensively with a wide range of domestic and international agencies in 2010 to educate and protect consumers and small business from scams and enforce consumer laws. The ACCC, for example, chaired the International Consumer Protection Enforcement Network through to July 2010 and continued to chair the Australasian Consumer Fraud Taskforce. The ACCC also coordinated the International Internet Sweep Day in 2010, which targeted potential cyber crime activity.

2 Contacts and trends

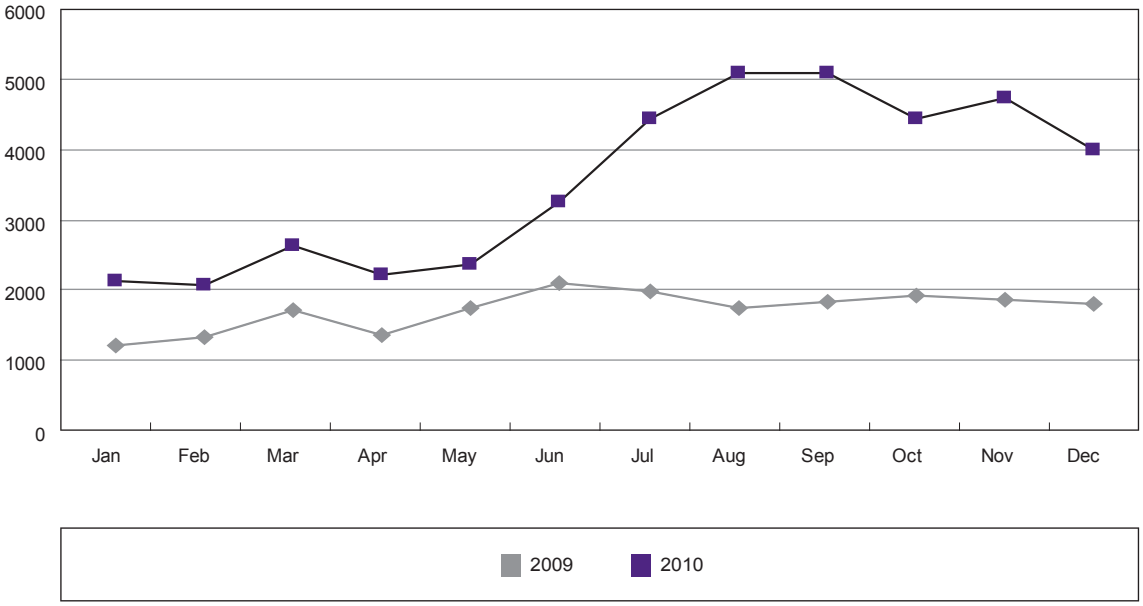
2.1 Scam and cyber crime reports and inquiries received by the ACCC

From 1 January to 31 December 2010 the ACCC received 42 385 scam-related contacts (41 582 scam reports and 803 inquiries). This represented an increased contact level of 106 per cent in comparison to 2009 when 20 554 contacts were received (19 886 scam reports and 668 inquiries).

The ACCC believes this increase can be partly attributed to raised consumer awareness of the option to report scams to organisations such as the ACCC.

In 2010 increased complaints were received across most scams types. However, the largest increase was in scams delivered by unsolicited telephone calls, particularly in the second half of 2010, as illustrated in figure 1.

Figure 1: Number of scam-related contacts made with the ACCC in 2009 and 2010



Method of communication of scams

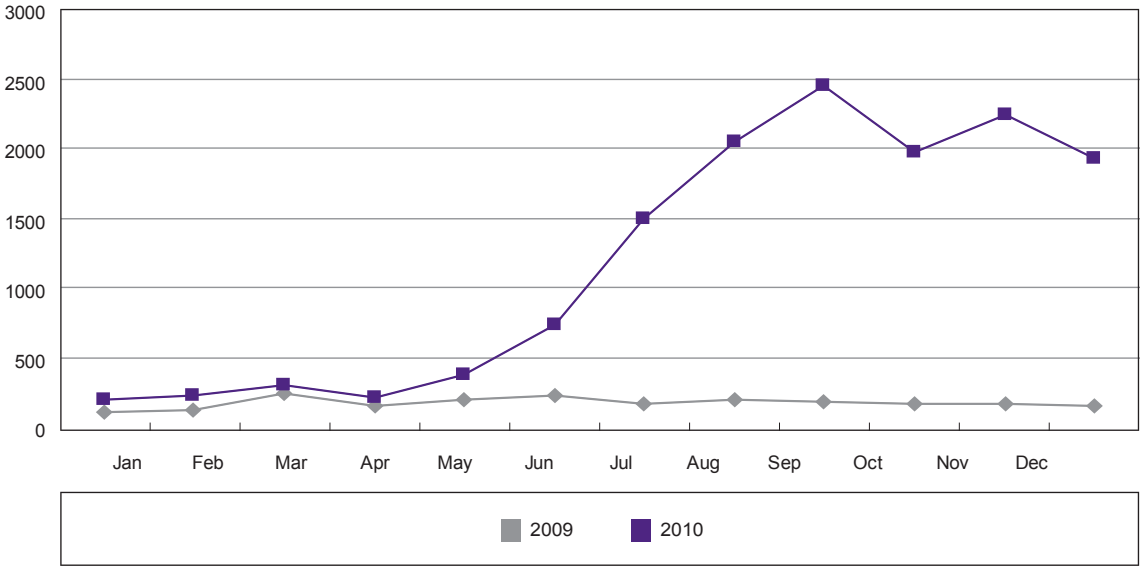
In 2010 consumers were most commonly approached by scammers online, making up 45 per cent of reported scams—25.6 per cent by internet and 19.4 per cent by email. The number of reports of online scams increased from 14 101 in 2009 to 19 074 in 2010.

There was also a steep increase in the reporting of scams initiated by unsolicited telephone calls, from 2036 reports in 2009 to 14 144 in 2010. Scams delivered by telephone represented 33.4 per cent of the total reported. In some cases there was a secondary contact through the computer—see page 13 for a description of such scams.

Other forms of contact included postal mail (10.9 per cent), text message (6.2 per cent), facsimile (2.3 per cent), other—for example newspaper advertisements (1.4 per cent) and in person (0.9 per cent).

In 2010 the ACCC observed a marked increase in consumer reports indicating that many telephone scams were operating out of overseas call centres. While many legitimate business operations use overseas call centres, the rise in unsolicited telephone scams may be attributed to the outsourcing by criminal networks of various telemarketing activities to cheap overseas providers and also the availability of low-cost or free voice-over-internet international calls services.

Figure 2: Comparison between number of consumers who reported being contacted by telephone in 2009 and 2010



Scams delivered by phone varied from calls offering:

- fake government grants
- false energy rebates
- ineffective energy saving devices
- to list the consumer's phone number on the Australian Government's Do Not Call Register[1] for a fee (when the register is a free government service)
- refunds for overpaid taxes or bank fees.

A particularly significant example of scams delivered by phone involved claiming that a consumer's computer was infected with a virus and demanding payment to fix it.

Calls targeted both numbers registered and unregistered on the Do Not Call Register. In October 2010 the ACCC and the Australian Communications and Media Authority initiated an awareness-raising activity to address the steep increase in scam telephone calls, including a joint media release and a number of media interviews.

Age range

While the provision of age data when contacting the ACCC is voluntary, the majority who provided these details fell into the 35 to 44 age bracket (24 per cent). In 2010, 67 per cent of people who contacted the ACCC about scams were between 25 and 54 years of age. As shown in Table 1, between 2009 and 2010 there was no change in the proportion of individuals under 18 years of age and increases for individuals between 55 and 64 and those over 65 years of age.

1 The Do Not Call Register is an Australian Government initiative providing Australians with the opportunity to opt out of receiving most telemarketing calls or marketing faxes. It is a free service.

Table 1: Comparison of age ranges provided by consumers when they contacted the ACCC in 2009 and 2010

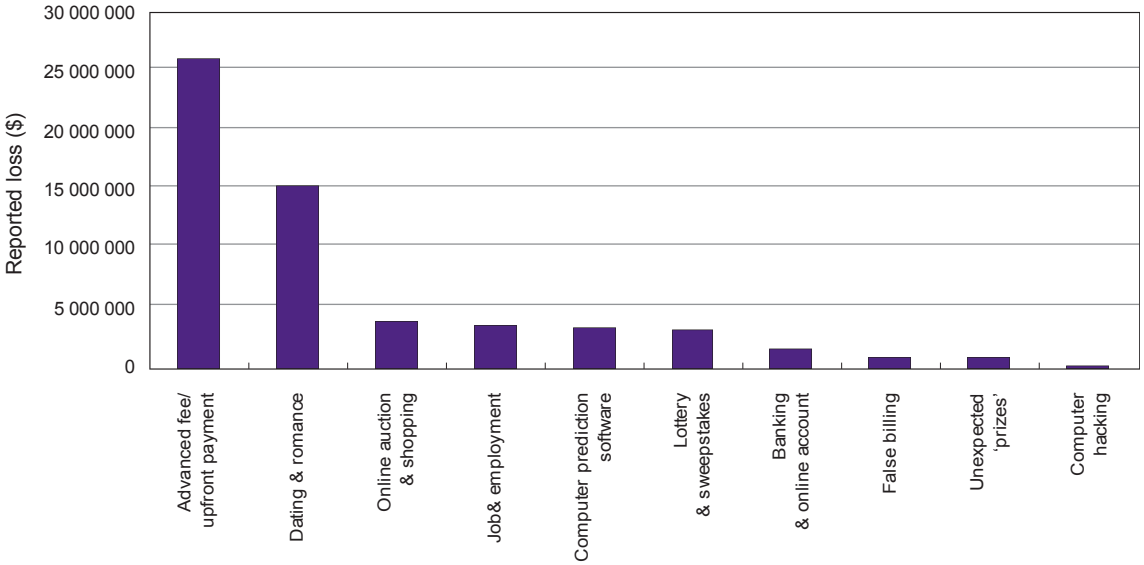
Age range	Number	Percentage	Variance from 2009
<18	89	1	No change
18–24	1083	9	– 2%
25–34	2510	21	– 2%
35–44	2876	24	– 5%
45–54	2522	21	+ 2%
55–64	1501	13	+ 3%
> 65	1168	10	+ 5%

2.2 Financial losses reported to the ACCC

Between 1 January and 31 December 2010 consumers reported to the ACCC losses of $63 436 348 to scam activity. This is slightly less than that reported in 2009 and is based solely on information provided to the ACCC by complainants. As such, this figure does not represent actual total financial losses by Australians caused by scams in 2010. Indeed, the ACCC considers that the figure represents only a small proportion of total losses—many scams are unreported and the ACCC is only one of many agencies that receive scam complaints.

More than 84 per cent of consumers who contacted the ACCC about scams in 2010 reported no financial loss. Sixteen per cent of consumers reporting scam activity to the ACCC accounted for the total money lost. Reported losses ranged from $1 (for an automatic deduction to charity) to almost $4 million (for an advance fee fraud). Figure 3 provides an overview of the monetary losses reported by consumers for each of the top 10 scam categories. Each scam type has varying success in extracting money from consumers. This is known as the scam's *conversion rate*[2] and is discussed in the next section.

Figure 3: Monetary losses reported by consumers to ACCC in 2010 for top 10 scams



2 A scam conversion rate is the percentage of consumers who receive a scam approach and then lose money.

Table 2 provides a further breakdown and comparison of the financial losses reported by consumers in 2009 as compared to 2010. Increases were recorded across all ranges except the $10 million plus category with two reports in 2009 and zero in 2010. This is consistent with the increase in overall contacts made by consumers on scams to the ACCC.

Table 2: Comparison of monetary losses reported by consumers because of scams in 2009 and 2010

Monetary range ($)	Number of people reporting this loss amount	Variance from 2009
1 to 99	734	+ 135
100 to 499	1978	+ 1160
500 to 999	805	+ 371
1000 to 9999	2204	+ 966
10 000 to 49 999	624	+ 275
50 000 to 499 999	204	+ 113
500 000 to 999 999	15	+ 5
1 million to 10 million	4	+ 1
10 million +	0	– 2

2.3 Most reported scams

Overview of cyber crime and scams reported to the ACCC in 2010

Table 3 provides an overview of all scam types reported to the ACCC in 2010, including how many had associated losses and the total losses attributed to each type of loss.

Detriment caused by scams can be measured in a number of ways. One measure is the conversion rate of a scam—that is the percentage of consumers who receive a scam approach and then lose money. Some scams, such as dating and romance as well as health and medical, have comparatively low numbers of reports but achieve very high conversion rates (above 50 per cent).

Table 3: Overview of scams types reported to the ACCC in 2010 including scam conversion rates

Scam type	Total reported loss	Number of reported scams	Number who report loss	Number with loss more than $10 000	Number with loss less than $10 000	Number without loss	% losing money (conversion rate)
Advanced fee/up-front payment	$25 787 755	14 739	1563	232	1331	13 176	10.6
Dating and romance (including adult services)	$15 157 360	1149	598	232	366	551	52.0
Online auction and shopping	$3 922 665	5527	1902	74	1828	3625	34.4
Job and employment (including business opportunity)	$3 567 619	1322	265	54	211	1057	20.0
Investment seminars and real estate	$3 471 697	304	119	46	73	185	39.1
Computer prediction software (including betting)	$3 426 288	604	278	84	194	326	46.0
Lottery and sweepstakes	$3 102 933	3468	256	52	204	3212	7.4
Banking and online account (including Phishing)	$1 606 450	2692	175	19	156	2517	6.5
False billing (including advertising, directory and domain name)	$966 844	2740	357	10	347	2383	13.0
Unexpected prizes	$934 282	2813	185	17	168	2628	6.6
Other (scams which do not fit into predefined categories)	$533 161	554	56	5	51	498	10.1
Chain letter or pyramid scheme	$338 779	189	26	7	19	163	13.8
Computer hacking	$225 483	4983	441	6	435	4542	8.9
Health and medical	$125 089	269	140	3	137	129	52.0

For more information on the broad variety of scams operating visit the SCAMwatch website at *www.scamwatch.gov.au*.

The top 10 scams most commonly reported to the ACCC in 2010

For the second consecutive year, MMAFF recorded the highest complaints, contributing to just over half (22 169) of the total scams reported to the ACCC. MMAFF consists of four of the scam types listed in Table 4—advance fee/up-front payment, lottery and sweepstakes, unexpected prizes, and dating and romance.

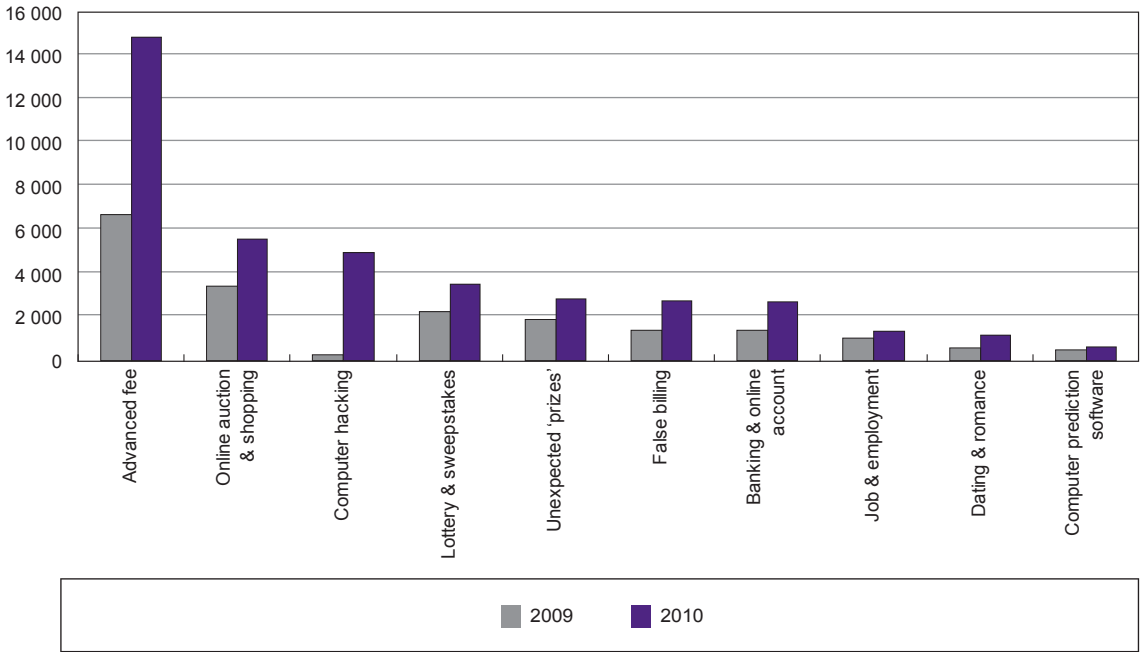
The ACCC also continued to receive high levels of complaints about the other types of scams listed in Table 4, including online auction and shopping, false billing, banking and online account, and dating and romance. In 2010 computer hacking became the third most commonly reported scam type due to the emergence of a non-traditional hacking scam in which scammers used telemarketing calls to request remote access to the consumer's computer. This is classified as a computer hacking scam despite the initial contact being a scam telemarketing call.

Table 4: Top 10 scam types complained about to the ACCC in 2010

Type	Total scams reported to ACCC in 2010	% of total reports
Advanced fee/up-front payment	14 739	34.8
Online auction and shopping	5527	13.0
Computer hacking	4983	11.8
Lottery and sweepstakes	3468	8.2
Unexpected prizes	2813	6.6
False billing (including advertising, directory and domain name)	2740	6.5
Banking and online account (including phishing)	2692	6.4
Job and employment (including business opportunity)	1322	3.1
Dating and romance (including adult services)	1149	2.7
Computer prediction software (including betting)	604	1.4

Figure 4 compares reports of the top 10 scam types in 2009 and 2010.

Figure 4: Comparison of top 10 scam types in 2009 and 2010



Mass marketed advance fee fraud

The ACCC defines MMAFF as scams that involve requesting fees up-front for goods, services or rewards that are never supplied. It includes four types of scams:

- advance fee/up-front payment
- lottery and sweepstakes
- unexpected prizes
- dating and romance.

MMAFF characteristically tricks consumers into sending money by using inventive and seemingly legitimate reasons for requesting payment, for example, to claim a prize, reward or other benefit.

Details on these four types of scams are provided below.

Advance fee/up-front payment scams

Number of scam reports in 2010: 14 739

Number of consumers reporting losses: 1563

Total losses reported by consumers: $25 787 755

Scam conversion rate: 10.6 per cent

The proportion of advance fee fraud scam reports made during 2010 increased by 2.4 per cent over 2009.

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 sums 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 on.

These scams range from seemingly outlandish offers to extremely sophisticated scams that can involve a gradual entrapment of consumers over many months. Some examples include: inheritance offers; promises of goods or profits from commodities such as gold, gemstones and oil; rental scams such as advance payment for rental accommodation; fake accommodation vouchers; and promises of guaranteed visas.

In 2010 the ACCC saw an increase in advance fee scams being initiated through scam telephone calls. Many involved scammers posing as representatives from government departments. These scams are of particular concern as they trick people into believing they have received a legitimate offer from a trustworthy source. Consumers may therefore be less cautious when judging the authenticity of the offer and may more readily provide payments and personal details.

Some examples of departments and/or services falsely represented in 2010 included the Australian Taxation Office, Medicare Australia, Centrelink, the Department of Veterans' Affairs, the Department of Immigration and Citizenship, the Do Not Call Register, and a fictitious Australian Government Grants Department. Scammers also posed as representatives of large private companies, such as banks and telecommunications providers, to lull victims into a false sense of security.

Another key growth area in recent years has been the emergence of advance fee scams on online classified websites. Consumers have reported buying pets, used cars, boats, bikes, caravans and other goods advertised online and often at very low prices. Consumers are frequently told the item is in Australia but because the owner is travelling or has moved overseas an agent will deliver the goods following receipt of payment. However, once the money is sent, the purchaser does not receive the goods and is unable to contact the seller. Many consumers reported they were required to send funds by wire transfer.

The ACCC continues to work with a range of traders operating online classified websites to ensure that when these types of advertisements are identified, they are removed as soon as possible.

The ACCC has also received reports of scammers targeting consumers who sell goods online through auction and classified websites. This scam involves elements of advance fee fraud. In several cases, the scammer (buyer) made an excuse for their inability to pay up-front costs (such as for transportation) and asked the seller to pay these costs first with a promised reimbursement. However, once the seller paid, there was no reimbursement and it was often too late to recover the money and/or contact the 'buyer'.

Observation: Reports to the ACCC show that classified scams are commonly initiated through fake ads placed on legitimate online auction and classifieds websites. Payments are made outside of the websites' secure payment systems, however victims may not realise this as scammers often impersonate legitimate payment providers.

Victim story: university student loses $10 000 responding to a fake car ad

In a typical advance fee scam, a university student found a car advertised on an online classified website at a very good price. The student expressed an interest in the car and was told that the owner was holidaying overseas. The student was asked to wire transfer the money overseas to the owner and told that an agent would then deliver the car.

The student sent $10 000 but never received the vehicle.

From the SCAMwatch radar: fake grants from a fake government department

One prominent advance fee scam from 2010 involved scammers calling victims to offer fake government grants. They said they were from the Australian Government Grants Department (this department does not exist).

The scammers claimed that their victims had received a government grant and requested a fee of $199 to release the grant funds. They also requested $4000 to contribute to charities and pay off government debt.

The scammers maintained that they managed the Government GrantsLINK directory website (www.grantslink.gov.au). This site is a legitimate Australian Government site run by the Department of Infrastructure, Transport, Regional Development and Local Government. It does not provide grants funding, however, and is not affiliated with the scammers.

www.scamwatch.gov.au

Lottery and sweepstakes scams

Number of scam reports in 2010: 3468

Number of consumers reporting losses: 256

Total losses reported by consumers: $3 102 933

Scam conversion rate: 7.4 per cent

Lottery and sweepstake scams were again quite prominent in 2010. Consumers reported receiving a notice either by post, email or SMS, stating they had won money in a lottery they never entered. To claim their winnings consumers were first asked to provide money and/or personal information, however no winnings were ever received.

In 2010 these scams coincided with major sporting events such as the Fédération Internationale de Football Association (FIFA) World Cup, and also involved scammers impersonating organisations such as the United Nations, telecommunications companies, car companies and well-known beverage companies.

Observation: Scammers can be identified by the fact that they will not let their victim use the 'winnings' to pay the required fees.

Victim story: consumer loses almost $60 000 claiming lottery win

An Australian consumer received an email notifying them of a multi-million dollar lottery win. While they were initially sceptical as they had not bought a lottery ticket, they conducted some research and found that the bank where the winnings were supposedly being held was a legitimate overseas bank. Over a series of months, the victim paid almost $60 000 for various transfer fees and certificates but never received the expected winnings.

Unexpected prizes scams

Number of scam reports in 2010: 2813

Number of consumers reporting losses: 185

Total losses reported by consumers: $934 282

Scam conversion rate: 6.6 per cent

In this scam, scammers offer consumers a prize, such as a cheap holiday or mobile phone, to elicit a payment or obtain personal or credit card details. Often the promised prize does not exist or is not what it seems.

Observation: Unexpected prizes scams are similar to lottery and sweepstakes scams, however the scammer offers a good or service rather than money.

Outsmarting scammers: answering a survey and winning a prize

A consumer was contacted by phone to answer a simple survey. Following the survey, they were advised they had won an electronic good and that their name had gone into the draw for the major prize. The consumer was called back and told they had won second place in the major prize draw—around $60 000. To collect the prize they had to fill in a claim form with their personal details and send a fee. The consumer realised that the number on the cheque did not belong to the bank that supposedly issued it and so did not send their money or personal information.

From the SCAMwatch radar: beware of scam scratchie cards in your letterbox

A common unexpected prize scam from 2010 was a scratch card travel scam in which the Aviats Travelling Group (among others) posted colourful travel brochures and scratch cards to consumers. When consumers scratched a winning card (one was included in every envelope) they were directed to call the scammers who then requested various up-front fees and copies of personal identity documents.

Further details of this scam and the ACCC's actions in dealing with it are in section 4.1 of this report.

www.scamwatch.gov.au

Dating and romance scams

Number of scam reports in 2010: 1149

Number of consumers reporting losses: 598

Total losses reported by consumers: $15 157 360

Scam conversion rate: 52 per cent

Dating and romance scams recorded high losses in 2010. Seeking to exploit consumer emotions is a feature of this type of cyber crime.

In these scams, which may be 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 or a family crisis.

Dating and romance scammers often approach their victims on legitimate dating websites, then quickly move away from the security of the website, communicating with their victim through other methods such as email.

Victims may be specifically targeted as they make their personal details readily available to scammers through online dating websites and other social media networks.

Observation: Romance scam losses per victim continued to be high in comparison to other scam categories. Just over 17 per cent of consumers (almost one-in-five) who reported a loss to this type of scam in 2010 had lost more than $100 000.

Victim story: retiree loses 'true love' and $200 000 to romance scam

In a typical romance scam, a retiree found someone who they believed to be their true love on a reputable online dating website. They had sent photos to each other and spoken on the phone but had not yet met in person. The scammer claimed to be temporarily overseas for work and therefore could not meet up.

The scammer professed their love but required some financial assistance, claiming that both they and their child had experienced a series of unfortunate events including accidents and illnesses. They also requested money for a phone and computer so they could stay in touch with the victim.

After several months, the scammer mentioned they had inherited a large quantity of gemstones and required some assistance in paying the taxes on these so they could leave the country they were in and come back to Australia to be with the victim.

The victim sent approximately $200 000 over a four-month period to support the scammer. The love interest never arrived in Australia.

Online auction and shopping scams

Number of scam reports in 2010: 5527

Number of consumers reporting losses: 1902

Total losses reported by consumers: $3 922 665

Scam conversion rate: 34.4 per cent

For the second consecutive year the online auction and shopping scam category was the second most reported type, contributing 13 per cent to total scam contacts.

In this scam category, scammers typically advertise products on popular online auction websites, however when the consumer buys the product, it is never sent or is of an inferior quality to what was promised. This category does not include the online classified scams mentioned earlier in this chapter in the advance fee/up-front payment category.

Observation: Some common reports in 2010 involved jewellery and hair straighteners which were advertised as authentic products from popular brands, however the goods provided were imitations.

Victim story: internet purchases paid for but never arrive

A consumer tried to buy new mobile phones from the website of an overseas-based company. While they promptly paid for the goods and received a tracking number, the items never arrived. The overseas-based company refused to provide a refund for the items, leaving the victim $1500 out of pocket.

Computer hacking scams

Number of scam reports in 2010: 4983

Number of consumers reporting losses: 441

Total losses reported by consumers: $225 483

Scam conversion rate: 8.9 per cent

Computer hacking was the third most common scam type reported to the ACCC in 2010. However rather than computers being hacked directly, this was predominantly due to a surge in hacking scams initiated by way of the telephone. In these scams, victims were tricked into providing remote access to their computer to fix a non-existent virus. This scam is explained in more detail in the 'Your computer has a virus' case study from SCAMwatch.

Other scams in this category involved computers, modems, and email or social networking accounts being hacked by scammers, most commonly resulting in lost data, passwords and personal details.

Observation: Computer hacking scams have evolved since 2009 when they were most commonly an internet-based scam in which the victim had no contact with the scammer. The trend of telephone-initiated computer hacking scams in 2010 was much more personalised with victims speaking directly to their scammer. The victim was present when the scam was being committed and was directed by the scammer to compromise the security of their own computer and their personal details.

Victim story: a friend in need

A consumer received emails from her friend travelling overseas to say that she had been injured during a mugging and was unable to pay her hotel or hospital bills as her purse was stolen. The friend said she was unable to leave the country until she had paid the bills and desperately needed help. The consumer knew her friend was travelling and sent $18 000 to help out. The friend's distress emails were fake as her email account had been hacked by a scammer. In reality she had not been mugged and was uninjured, however the consumer lost her $18 000.

From the SCAMwatch radar: your computer has a virus!

In the latter half of 2010 scammers made wide-ranging scam telephone calls to consumers to trick them into believing their computer was infected with a virus or was sending out error messages. Scammers claimed to representat Microsoft or another genuine service provider and asked for remote access to scan consumers' computers for the (non-existent) virus.

The scammers pretended to run scans and then tried to convince their victims to buy anti-virus software, either through a one-off payment or an ongoing subscription. While this approach may be seen to be more of a telemarketing scam—as the scammer tries to sell an unnecessary product—it has strong elements of computer hacking because scammers gain remote access to their victim's computer.

In some instances scammers also asked the unsuspecting victim to follow a link to a website. In doing so, some victims unwittingly loaded a virus onto their computer.

www.scamwatch.gov.au

False billing (advertising, directory and domain name) scams

Number of scam reports in 2010: 2740

Number of consumers reporting losses: 357

Total losses reported by consumers: $966 844

Scam conversion rate: 13 per cent

As in previous years, the ACCC received numerous complaints about false billing in 2010 (comprising 6.5 per cent of the total reported).

Scammers continued to target small businesses to trick them into paying for a listing or advertisement in a magazine, journal, business register or directory. A common example was where a small business was sent a subscription form disguised as an outstanding invoice to get the recipient to sign up for unwanted advertising services. Often the scammers made false claims that the directory or publication is commonly known and/or has a high readership.

Observation: False billing scams were a common small businesses scam in 2010. Scammers frequently used copies of legitimate company logos on fake invoices to trick small businesses into thinking they would be advertising or listed in a well-known publication and/or directory with high readership.

Victim story: small business pays for non-existent advertising

Over the course of several months, a small business received a series of invoices for half-page advertisements totalling more than $20 000. The advertising was to be featured in a related industry journal but upon further investigation, the journal did not exist. The small business was left without the funds or the advertising.

Banking and online account scams (including phishing)

Number of scam reports in 2010: 2692

Number of consumers reporting losses: 175

Total losses reported by consumers: $1 606 450

Scam conversion rate: 6.5 per cent

Banking and online account or phishing scams aim to trick people into providing their personal and banking information so that scammers can steal their money or identity.

Scammers will send emails that appear to be from legitimate businesses—such as banks, financial institutions or telecommunications companies—requesting that recipients provide personal bank account details. Phishing scammers also posed as government agencies such as the Australian Taxation Office, Medicare Australia and Centrelink in 2010.

This type of scam saw scammers commonly using sophisticated techniques to convince recipients that their request is genuine. Often they will copy an institution's logo or email format and provide links to fake websites which are convincing copies of genuine company sites.

Observation: Banking and online account scammers typically do not request money from their victims. Rather they focus on obtaining personal information and passwords to gain access to bank accounts or to commit identity theft.

Outsmarting scammers: email phishing for personal details

A consumer received an email asking them to click on a link and confirm their user name and password to a payment system. The email had what appeared to be the correct company logo and the email address contained the title of the company. The consumer realised the email came from a free email provider instead of from an official email addresses and did not click on the link. They deleted the email and avoided falling victim to the scam.

From the SCAMwatch radar: scam emails target Telstra BigPond customers

In 2010 various companies were falsely represented in online account scam emails. This included Telstra.

In September, Telstra had to advise customers of scam emails misrepresenting BigPond. These emails directed recipients to follow an email link to a scam website where they were asked to provide personal details.

Often with banking and online account scams, perpetrators will gather victims' personal details so they can commit identity theft.

www.scamwatch.gov.au

Job and employment (including business opportunity) scams

Number of scam reports in 2010: 1322

Number of consumers reporting losses: 265

Total losses reported by consumers: $3 567 619

Scam conversion rate: 20 per cent

Job and employment scams contributed just over 3 per cent of the scams reported to the ACCC in 2010.

These 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 where a victim is paid to receive money into their bank account and then transfer it to another location or account.

Observation: In 2010 scammers targeted the mining and seasonal employment industries with offers to work at the February 2010 Winter Olympic Games in Canada.

Victim story: payment for work-from-home

A consumer answered a newspaper job vacancy advertisement for secret shoppers and began working for an overseas-based company. The consumer received travellers cheques of $500 in payment for their work, in which they had to cash the cheque, deduct $200 for their wage and send the remaining balance overseas to their employer by way of a wire transfer. The cheques were later identified as being fraudulent and the victim was left out of pocket and unpaid for their work.

Computer prediction software (including betting)

Number of scam reports in 2010: 604

Number of consumers reporting losses: 278

Total loss: $3 426 288

Scam conversion rate: 46 per cent

With computer prediction software scams, scammers promote software packages or memberships to betting schemes with promised returns. Consumers are asked to pay large sums of money up-front to purchase the membership or software. In some reports from 2010 these fees were as high as $15 000. Victims may then also have to pay ongoing fees and bets.

Consumers are often promised returns but rarely see any of their money back and problems may arise years after the original purchase.

This category includes different scams, which are often quite sophisticated, such as:

- sports-betting packages that claim to predict the outcome of races or how to always make money on bets
- investment software that claims to predict stock market movements and promises big returns
- lottery prediction software which guarantees winning lotto numbers.

Observation: In this scam, high returns are promised over a specific timeframe which can sometimes be up to 10 years. Victims may therefore continue to make payments for years before realising they are involved in a scam and that the returns promised have not eventuated. As this is a gambling scam, victims may not initially be concerned by losses as it is the nature of betting, however continual losses may alert them to the scam.

Victim story: horse-racing betting system not returning promised results

A consumer was cold-called and offered a horse racing investment system with promised returns. The scammer convinced the consumer to buy the system for $8000 and to make an additional $10 000 investment. The consumer did not receive the promised returns on his $10 000 investment and tried to contact the company for a refund. The phone number he was provided with was disconnected and the webpage no longer existed. The consumer lost $18 000 to the scam.

2.4 Cyber criminals and scammers

Who are the scam operators?

Scam operators can range from opportunistic individuals undertaking relatively small actions through to major international criminal networks. While individual scammers can generate significant detriment for some consumers, the latter category has grown in recent times and is generating greater risks for consumers both within Australia and overseas by exploiting new technologies and global opportunities. Organised cyber crime groups are drawn to scams because of the vast profit potential, low risk of detection and relatively minor penalties compared with other crime types. While some operators are domestically-based or have Australian links, most major networks exist outside of Australia.

In mid 2010 the International Mass Marketing Fraud Working Group (IMMFWG), a coalition of global law enforcement agencies including the ACCC, United States Federal Bureau of Investigation (FBI) and others, issued a study of contemporary cyber crime and scam operations (section 5.3 has more details). The study noted that law enforcement intelligence reports increasingly reveal that organised criminal groups conduct, facilitate and profit from international cyber crime activity. These range from highly structured enterprises to loosely knit groups as Nigerian organisations. Many have international reach, operating from numerous countries and continents. The nature and degree of organised cyber crime groups' involvement in advanced fee fraud vary substantially. Some exercise control over all aspects of a fraud operation and others outsource or provide specialised support services, including mailing documents, hosting fraudulent websites and laundering illicit proceeds.

Cyber criminals are highly adaptive and opportunistic. They often share successful cyber crime techniques with and provide assistance to other groups, a practice that may lead to the commission of nearly identical scams by multiple groups acting independently of one another. Some intelligence suggests that proceeds from cyber crime may fund other criminal activity.

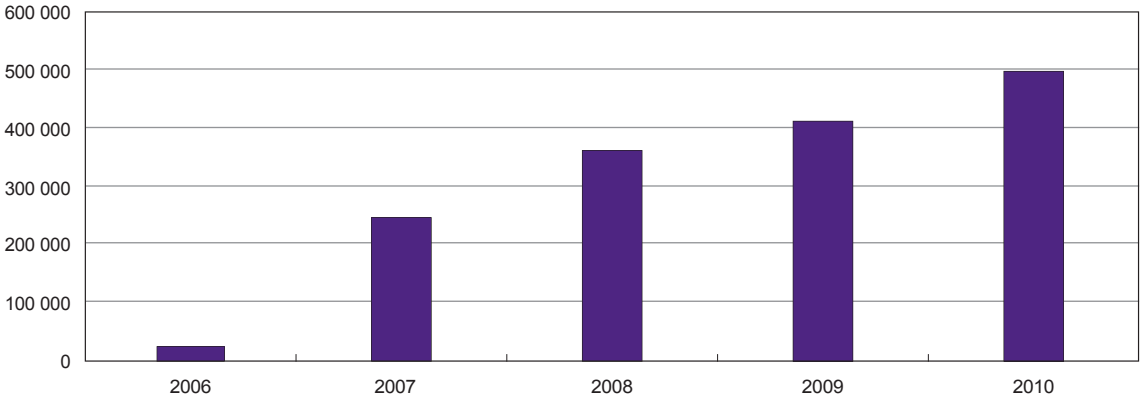
The ACCC will continue to work with global counterpart agencies to better detect and deter the organised cyber crime groups targeting Australian consumers and businesses.

3 Awareness raising and education initiatives

SCAMwatch website—www.scamwatch.gov.au

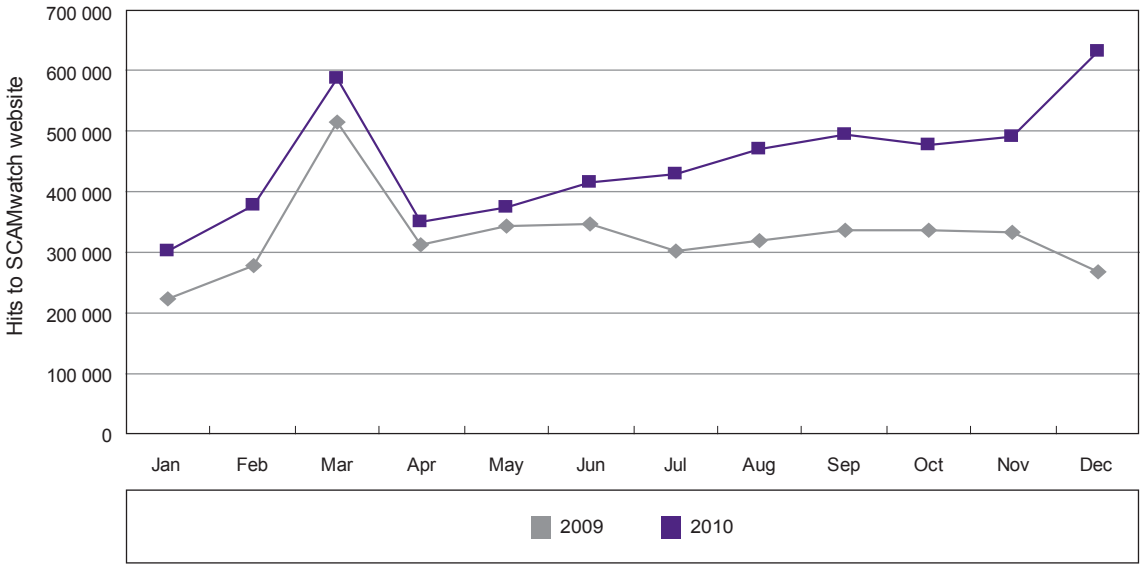
In 2010 the ACCC's SCAMwatch website (www.scamwatch.gov.au) received 500 284 visitors. The website is supported by consumer protection agencies in the ACFT from around Australia and New Zealand. There were in excess of 5.3 million hits to the site over the 12 months (measured as the total number of individual clicks across all SCAMwatch pages). This is an average of more than 448 000 hits per month. In 2009 the site received 413 155 visitors and 3.8 million hits.

Figure 5: Unique visitors to the SCAMwatch website from 2006 to 2010



March 2010 saw a surge in both the number of hits and unique visitors to SCAMwatch, largely attributed to increased public awareness generated by the annual ACFT National Consumer Fraud Week. This is a continuing upward trend from 2009, as shown in figure 6.

Figure 6: Comparison of hits to the SCAMwatch website in 2009 and 2010



Since its launch in 2006 the number of subscribers to SCAMwatch email alerts has grown substantially to almost 14 000.

The SCAMwatch website provides information to consumers and small businesses about how to recognise, avoid and report scams. It explains how scams operate and offers guidance on what to look for and how to minimise the chances of being scammed.

SCAMwatch also posts radar alerts about emerging scams. In 2010 SCAMwatch issued 38 such alerts, warning consumers about the imminent risk of scams around current events such as Australia's digital television switchover, the Haiti earthquake, the Canadian Winter Olympics, Iceland's volcanic eruption and the FIFA World Cup. Radars show that scammers try to target victims in all facets of their life whether they are trying to book flights, rent a property, buy a car, protect their computer from viruses, buy environmentally green products, sell an item online, make holiday plans, find true love or even adopt a pet. A full list of 2010 SCAMwatch radar alerts is at appendix 1.

SCAMwatch radar alerts are often issued in partnership with other government agencies, consumer protection and advocacy bodies and, more recently, with private businesses wanting to warn customers of scammers masquerading using their brands, products and services as a lure.

Besides publishing information about scams and how to avoid them, SCAMwatch operates as the portal for the ACFT. It promotes ACFT initiatives and campaigns and the taskforce's annual fraud week campaign. More information about the ACFT is in section 5.1.

The SCAMwatch website is a popular and valuable resource. Increasingly over 2010 the media, Australian Government and state and territory government departments, as well as police forces, consumer groups and private companies directed their website users to SCAMwatch. This contributed to growing brand awareness of the site.

Internationally, SCAMwatch is considered a unique resource. A number of agencies in countries such as the United Kingdom, South Africa and New Zealand refer consumers to the website.

Twitter coming in 2011

Besides providing general scams awareness messaging, the ACCC is also continuing to explore new communications options to quickly and effectively alert Australians to scams that may target them.

In 2011, for example, the ACCC will launch a SCAMwatch Twitter page, as a new way of engaging with existing and new audiences. Twitter will allow the ACCC to inform consumers of scams as they emerge, in real time. Consumers and partner organisations will be able to disseminate scams messages by re-tweeting ACCC scam tweets on their own Twitter pages.

Printed materials

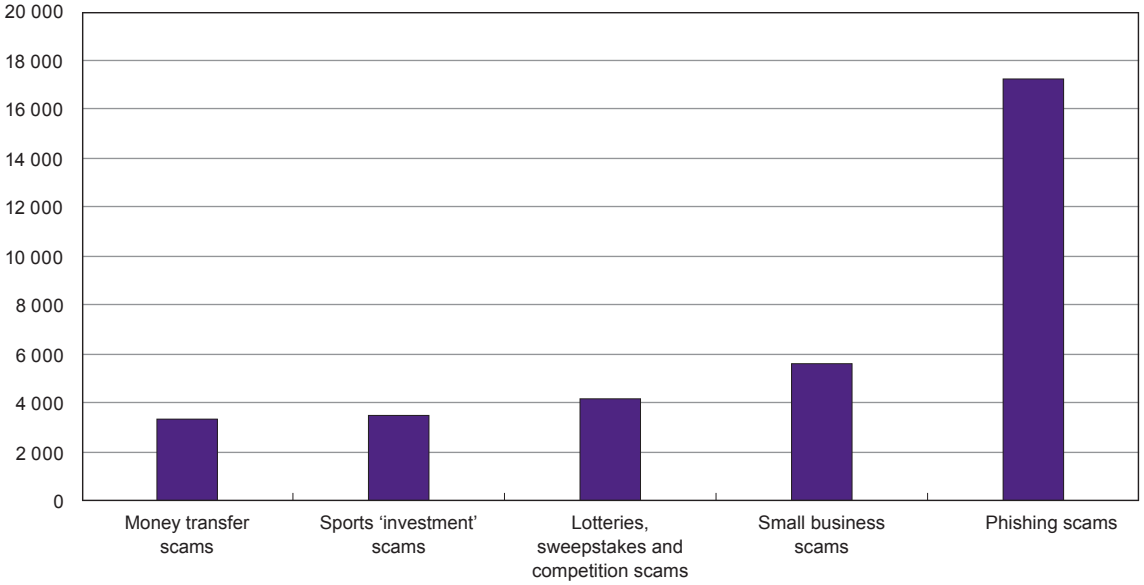
The ACCC has a suite of scams-related publications which complement the SCAMwatch website. In 2010 the ACCC distributed more than 102 000 copies of these publications.

The most popular is the *Little black book of scams*. In 2010 almost 68 000 copies of this free booklet were distributed to consumers and businesses.

The *Little black book of scams* highlights various 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 opportunities. It offers consumers tips on how to protect themselves from scams, what they can do to minimise damage if they get scammed and how they can report a scam.

Also among this suite of scams publications is five scam-specific fact sheets. In 2010 the ACCC distributed 34 615 copies of these fact sheets. They cover lotteries, sweepstakes and competition scams, money transfer scams, phishing scams, sports investment scams and—new in March 2010—*Small business scams*. In its first year of publication the *Small business scams* fact sheet became the second most popular of the suite, with 5574 copies distributed. The fact sheet for phishing scams was by far the most popular in 2010 as shown in figure 7.

Figure 7: Number of scams fact sheets distributed in 2010



Appendix 2 has a full list of ACCC scam-related publications.

Media and communications activity

The ACCC uses various media platforms and communication opportunities to promote its scams-awareness message to the widest possible audience.

Besides issuing regular media releases to promote both general and specific scams-awareness messages, the ACCC also uses media releases to publicise its enforcement action. ACCC Commissioners and outreach officers actively seek and accept opportunities to give media interviews, community and business presentations and speeches to increase knowledge of new scams and promote awareness of the ACCC's roles in scam prevention and education. Major and local newspapers across the country also publish articles by the ACCC on topical scam issues.

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

Appendix 3 highlights the ACCC's key media and communications initiatives in 2010.

Regional outreach

The topic of scams is frequently addressed in presentations, meetings and other communications undertaken by the ACCC's Regional Outreach Managers. These managers are based in each ACCC state and territory office and work with a business and community organisations to educate members how to recognise and avoid falling victim to scams.

During 2010 Regional Outreach Managers were involved in activities organised to provide information to a number of groups that may be vulnerable to scams, such as small business, senior citizens, the hearing impaired and young consumers.

The managers attended a number of expos and meetings with seniors groups, making presentations, for example, to the Senior Deaf Society (Queensland), the National Seniors Association and the Australian Computer Conference for Seniors. Young consumers were also a focus for the ACCC's scam education through work with other Australian Government departments and agencies during National Youth Week in May, to promote awareness of the particular types of scams that target young consumers.

Small business

The ACCC regularly engages with small business on the topic of scams. In 2010 the ACCC gave presentations on small business scams at a number of local events around Australia including some hosted by the Australian Institute of Company Directors, the Small Business Development Corporation and regional development boards. The ACCC also discussed small business scams at the 2010 Small Business Expo.

The ACCC regularly updates Australia's Small Business Information Network on relevant enforcement action and scam-like conduct. The network comprises more than 700 small businesses and small business stakeholders, including industry associations, local government and business enterprise centres.

The ACCC also has resources to help educate small businesses about the steps they can take to protect themselves against scams, including the *Small business scams fact sheet*.

Consumer scams survey

In May 2010 the ACCC commissioned a telephone survey of consumers who had previously contacted the ACCC Infocentre to report a scam. Results provided a deeper understanding of consumer awareness of, and reaction to, scams and confirmed the appropriateness and effectiveness of the ACCC's current education approach.

Results highlighted the continued necessity to break through the embarrassment barrier which is the main cause of inaction for scam victims. This result supported the need for the ACCC to continue to illustrate how widespread scams are and how any consumer can be scammed, regardless of age, gender, education or income level.

4 Action to disrupt scams and enforce the law

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

4.1 Scam disruption activities

The ACCC and other agencies recognise 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 increased sophistication in the use of technology to perpetrate scams. To combat this, the ACCC cooperates with a number of agencies and private entities to protect consumers and small businesses from scams, disrupting and limiting the harm they cause when enforcement action is unavailable. The ACCC carefully analyses offers to determine if they are legitimate or a possible scam. Wherever possible the ACCC seeks to communicate with the operator to stop the conduct if there are doubts about its legitimacy.

Disruption activities may allow the ACCC to restrict or even discontinue the activities of a scammer, and the harm they may cause, often without having even identified or located the scammer.

One challenge in disrupting scams is correctly identifying those that have been executed so meticulously that even experts can be fooled. In 2010 the ACCC worked broadly with external parties, from both government and non-government, who provided information that on closer analysis, confirmed various activities as scams. This collaborative approach helps the ACCC protect consumers and small businesses from harm.

The case studies in this section show some results achieved through the ACCC's collaborative work with external parties.

Case study—WesternField Holdings Inc. investment

Following an ACCC investigation, WesternField Holdings Inc was identified as a fraudulent business. They engaged overseas telemarketers to tout a scam carbon credit investment opportunity which may have fleeced consumers of more than $3.5 million, many of whom were small business operators, self-funded retirees and individuals hoping to find an ethical investment opportunity.

The telemarketers made unsolicited calls to Australian consumers and businesses asking for their views on current environmental concerns and if they would consider investing in environmental projects. Anyone who expressed an interest was contacted by someone claiming to work for the bogus Japanese-based business, WesternField Holdings, and offered an opportunity to invest in projects generating carbon credits.

WesternField Holdings went to great lengths to convince investors that its offer was a legitimate investment opportunity and referred them to a genuine-looking website. Investors reported to the ACCC, however, that they could not obtain investment certificates and that requests to sell their investments and/or obtain a refund were ignored. Some investors reported they were given false promises that if they made additional investments their money would be returned.

Investigating staff organised a mail-out to 84 identified investors warning them to stop sending money to the scammers. As at March 2010 the ACCC identified that the 84 investors had lost more than $3.5 million to the scam. The ACCC media warning and the letters to investors resulted in the scammers stopping the scam.

Case study—scratch card travel scams

A prevalent unexpected prize scam from 2010 was a scratch card travel scam in which the Aviats Travelling group (among others) posted colourful travel brochures and scratch cards from Malaysia to Australian consumers.

When consumers scratched a winning card (which ACCC investigators found was included in every envelope) they were directed to call the scammers to claim their prize of more than $100 000. Consumers were then asked to pay up-front fees and charges. They were also asked to provide important personal details such as copies of drivers licences.

To date the main promotions have targeted specific Australian states or territories at different times as can be seen from the following list:

- EverMas Tourism Group targeted Western Australia
- Aviats Travelling Group targeted South Australia and Northern Territory
- Holiday Symphony Travelling Group targeted Queensland
- Euphoria Travelling Group targeted the eastern states and territories
- Malaysia Starize Travelling Group targeted Western Australia.

Mail-outs were also supported by professional looking websites—this combination of different media is an increasing feature of scams.

The ACCC carried out various disruption activities including naming each of the above scams in a media release and on the SCAMwatch website. The ACCC also participated in a radio interview where the scam scratch card promotions were discussed.

4.2 Scam-related enforcement activities

In 2010 the ACCC initiated proceedings or concluded actions against a number of traders allegedly involved in misleading and deceptive or scam-like conduct.

Small business operators continued to be the target for unsolicited offers for directory and internet-based listings as well as for the practice of 'blowing', in which payment is demanded for advertisements which a business never authorised. The conduct ranges from opportunistic to blatant scams. While perpetrators are often based overseas, the ACCC has instituted proceedings against a number of identified traders in recent years.

In 2010 the ACCC was involved in Federal Court proceedings alleging that traders had engaged in misleading conduct to sign up unwary small business owners to their directory services or to demand payment for unsolicited advertisements.

Two enforcement case studies from 2010 are listed below.

Case study—distribution scheme business opportunity

In 2010 the ACCC issued its first public warning notice concerning the activities of Halkalia Pty Ltd, Heartlink Enterprises Pty Ltd and National Semi Retired Group Pty Ltd, following complaints from individuals who had paid between $10 000 and $30 000 for a part-time delivery business and who were promised a certain level of income. The majority had earned no income, however, and none had reached the projected figure.

The ACCC suspected that the companies selling the business opportunities had breached the *Trade Practices Act (1974)* by making misleading claims about the potential income from the business opportunity. The business opportunity was advertised in rural, regional and metropolitan newspapers and promised earnings of between $900 and $2000 per week for between three to four days of work, delivering Heartlink-branded household products to independent supermarkets.

Case study—Powerball bogus scam

Constantine 'Con' Barris and his company, Powerballwin.com.au Pty Ltd, were found to have engaged in false or misleading conduct following ACCC action in the Federal Court.

The scheme asked consumers to pay a $59 subscription fee to receive a series of predicted numbers to help win all divisions of Powerball. The predicted numbers failed to produce a dividend for subscribers.

The trader had set up a website and distributed 163 000 leaflets to households around Australia claiming '... an amazing discovery that disputes the theory of random probability and has totally shocked the experts.'

Justice Tracey labelled Powerballwin a bogus scheme and found there:

'… could be no "100 per cent guarantee" that a number provided by the company would be the Powerball number in any given draw. Nor could any other information, supplied by the company, assist anybody to choose the five remaining numbers. They [the subscribers] would have been in no better position than if they had relied on their own intuition.'[3]

3 Legal reference: Australian Competition & Consumer Commission versus Powerballwin.com.au PTY LTD [2010], FCA 378, para 26.

5 Domestic and international collaboration

5.1 The Australasian Consumer Fraud Taskforce

About the Australasian Consumer Fraud Taskforce

The ACFT, established in 2005, comprises 21 Australian Government and state and territory government regulatory agencies and departments (including New Zealand) that have responsibility for consumer protection relating to fraudulent and scams activity.

The taskforce's primary functions are to:

- enhance Australian and New Zealand government 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, Peter Kell, is the taskforce chair. The ACCC also assumes the taskforce's secretariat role.

The work of the taskforce is assisted by a growing number of government, business and community 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 initiative of the taskforce 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 Month.

2010 campaign—Online Offensive

The 2010 Fraud Week campaign, *Online Offensive—Fighting Fraud Online,* ran from 1 to 7 March and focused on the traps consumers and small businesses can encounter when transacting online and tips for dealing with the issue. The campaign had a particular focus on young consumers, older consumers and small business.

In recognition that the internet is now an integral part of daily life, the campaign helped consumers and businesses learn how to stay safe online. Educational messages were promoted and distributed nationally, and supported in government and partner activities such as a forum on the enforcement and disruption of online scams. The ACCC also released its inaugural scams report, *Targeting Scams, report of the ACCC on scam activity 2009*, which highlighted the breadth and scale of scams activity in Australia.

2011 campaign—Scams: It's Personal

The 2011 Fraud Week campaign, *Scams: It's Personal*, will run from 7 to 13 March focusing on the personal side and impact of scams.

Fraudulent activity increasingly involves personal and social facets ranging from the use of personal information, brands and organisations that people recognise and trust, through to social networking and communications platforms.

Scams can also have a devastating impact on victims including psychological, financial, familial and social harm.

Scams: It's Personal is relevant to both consumers and businesses, capturing how scams can affect individuals, loved ones, small and big business, as well as trusted brands, organisations and government.

The campaign will involve the taskforce and partners engaging in awareness initiatives to highlight the need for consumers to be aware of, and vigilant against, scammers who will not stop at anything to find a victim—including adopting a personal touch.

Appendix 4 includes a list of the 2011 taskforce members and partners.

Other key ACFT activities 2010

Examples of key initiatives undertaken by taskforce members in 2010 are discussed below.

ACFT 2010 online survey

Each year the Australian Institute of Criminology conducts an online survey to assess the consumer fraud experiences of participants. Between 1 January and 31 March 2010, 249 people responded to the self-selected survey hosted on the institute's website (*www.aic.gov.au*).

Survey results showed that consumers had sent more than $250 000 in response to scam invitations in the preceding year. Survey results revealed that people over 55 years of age were more likely to receive scam invitations than other age groups which confirms prior research in this area. The survey also revealed that young people were at higher risk of consumer fraud because of their use of the internet and mobile phones/SMS messaging. The study recommended raising public awareness through targeted age-specific campaigns as a potential means of reducing the risk of consumer fraud.

National Cyber Security Awareness Week

From 6 to 11 June 2010 the Department of Broadband, Communications and the Digital Economy (DBCDE) held its annual National Cyber Security Awareness Week. This campaign aimed to help consumers and small business understand cyber security risks and the steps they could take to protect their personal and financial information online.

During Cyber Security Awareness Week, around 150 state and territory government agencies, industry, community and consumer organisations partnered to deliver events and activities in metropolitan, regional and rural Australia.

The DBCDE conducted a second campaign during Christmas to promote secure and safe online practices.

5.2 The International Consumer Protection and Enforcement Network

ICPEN is a network of consumer protection law enforcement authorities from more than 40 economies. It is a forum through which authorities can cooperatively share information and look at combating consumer problems that arise with cross-border transactions in goods and services, such as e-commerce fraud and international scams.

ICPEN shares information about cross-border commercial activities and encourages international cooperation among law enforcement agencies.

The ACCC held the role of ICPEN President from August 2009 for a one-year term. Two ICPEN conferences and best practice workshops were held under the presidency, one in Sydney in November 2009 and another in Washington in May 2010. A key achievement of the Australian presidency was the facilitation and endorsement of the network's strategic plan providing ICPEN with direction for its future activities.

In March 2010 ICPEN launched its website, *www.icpen.org*, helping members deliver better consumer protection. The website provides consumers with tips on where to look for help and how to lodge a complaint in cross-border disputes.

Key activities of ICPEN are outlined below.

Fraud Prevention Month

Running throughout March each year, Fraud Prevention Month is an education campaign informing consumers about fraud and raising awareness of scams through events and activities. The ACCC participates as part of its Fraud Week campaign with the ACFT (see section 5.1 for more information).

E-consumer.gov

E-consumer.gov (www.econsumer.gov) is a website portal featuring a global online complaint mechanism which consumers can use to report suspect online transactions with foreign businesses. The mechanism is available in seven languages. The portal also provides consumers with tips on how they may be able to resolve issues and contacts for alternative dispute resolution services in ICPEN member jurisdictions, including Australia.

Annual International Internet Sweep Day

The ICPEN Annual International Internet Sweep Day is a global web-surfing exercise introduced to improve consumer confidence in e-commerce by demonstrating a law enforcement presence online. Throughout this day-long event, participating enforcement agencies search for websites that may potentially be deceiving and/or defrauding consumers. The ACCC is the international coordinator of the exercise.

In 2010 the sweep day was held on 21 September. The theme was *The Online Generation*—targeting online marketing and advertising to youth. 2010 saw an expansion to begin sweeping new technology platforms including social networking sites, blogs and mobile smart platforms.

As in previous years, the ACCC was joined by state and territory consumer protection agencies across Australia to sweep for misleading or deceptive conduct targeting young people who shop, conduct financial transactions and socialise online.

Attendance at the sweep headquarters in Canberra, Australian Capital Territory, exceeded expectations and resulted in national television news coverage, with the ACCC Deputy Chair, Peter Kell, giving numerous interviews. Overall, more than 300 media items were broadcast or published in the week of the event. Coverage occurred in both mainstream and youth media.

The ACCC continues to make contact with foreign enforcement agencies where suspect conduct is found to have originated overseas.

ACCC findings on International Internet Sweep Day

The ACCC swept close to 1400 websites, with 316 flagged for follow-up action.

Common problematic online conduct identified during the sweep included:

- internet pop-ups featuring a chance to win electronic gadgets or other prizes
- online classified ads for non-existent pets
- side bar ads on social networking sites offering free trials, weight loss products or unexpected prizes
- fine-print concerns relating to warranties, refunds and terms and conditions
- unrealistic claims about products and in some cases prices.

Some conduct was specifically identified as targeting the youth market including:

- offers for body image products such as those for skin and weight loss
- celebrity-related offers and advertisements
- brand name or gimmicky products
- pop-ups featuring prizes such as iPods and iPads.

5.3 International Mass Marketing Fraud Working Group

Since February 2008 the ACCC has participated in the IMMFWG, which consists of a number of domestic and international law enforcement agencies.[4] This multinational initiative focuses on mass-marketed fraud, to:

- improve intelligence
- increase disruption of scam/fraud operations
- expand public awareness and prevention measures
- enhance cooperation and coordination in enforcement actions against mass marketed fraud activity.

On 1 June 2010 the ACCC launched the Global Day of Action—Think Fraud! Think Fraud! was part of the world-wide effort by the IMMFWG to combat mass-marketed advance fee fraud. The ACCC and Australian state and territory police participated in the Global Day of Action to raise awareness of the issue. This initiative generated widespread media coverage. The day's activities increased awareness of these types of scams, and educated consumers on how to recognise and take action to protect themselves.

The IMMFWG also released the *Mass-marketing Fraud: A Threat Assessment* report to provide governments and the public with a current assessment of the nature and scope of mass-marketing fraud around the world. The report showed that recent law enforcement investigations have exposed large-scale criminal mass-marketing fraud operations in multiple countries in most regions of the world. It identified the increase in organised criminal enterprises conducting, facilitating and profiting from international mass-marketing fraud schemes as well as a trend in the foreign outsourcing of vital business functions to legitimate businesses and criminal enterprises globally.

The report also identified an increasing trend across large mass-marketing fraud operations to use specific resources to operate their scams which may include:

- legitimate or semi-legitimate businesses to perform critical functions such as the printing of lottery mailings
- customised lead lists which can be purchased and contain names and contact information for potential victims
- payment processors to facilitate the collection of victim funds through non-cash processes such as bank debits and credit card charges
- communications tools and networks
- fraudulent identification documents such as counterfeit passports, which enable perpetrators to open bank accounts under assumed names
- counterfeit financial instruments including cheques and money orders.

The report will assist agencies world-wide to develop enhanced counter measures to detect, deter and disrupt mass-marketed fraudulent activity.

4 Members of this group include the United States Federal Trade Commission, United States Department of Justice, United States Postal Inspection Service, United States FBI, United Kingdom Office of Fair Trading, United Kingdom National Fraud Agency, United Kingdom Serious Organised Crime Agency, Canadian Competition Bureau, Canadian Royal Mounted Police, Europol, Nigerian Economic Financial Crimes Commission, London Metropolitan Police, Netherlands Police and Amsterdam Police.

5.4 House of Representatives cyber crime inquiry

The House of Representatives Standing Committee on Communications started a 12-month inquiry into cyber crime and its impact on Australian consumers in May 2009.

Informed by submissions and contributions from consumers, businesses and experts in the field, as well as the Australian Government and state and territory governments, the Committee in June 2010 released its report, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*.[5]

The Australian Government released its response to the report in November 2010 acknowledging that governments, industry and individuals all have a role to play in taking action to mitigate online risks. This includes continuing to work towards a secure, resilient and trusted cyber environment through the Cyber Security Strategy and continuing to support domestic and international cooperation on investigating, prosecuting and preventing cyber crimes.

The ACCC has already taken significant steps to support domestic and international cooperation and it will continue to work closely with its government, non-government, business and consumer stakeholders to promote an integrated and coordinated effort to address cyber crime. The ACCC's work with ACFT, ICPEN and IMMFWG are such examples and are discussed further in sections 5.1, 5.2 and 5.3 respectively.

5.5 Other partnerships and cooperative activities

As scams commonly operate in a global environment, national and international cooperation is becoming an essential part of effective prevention. Some other partnerships and activities that the ACCC participates in are outlined below.

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.*

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 A$10 000.

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

Sports investment scams multi-agency taskforce

Sports investment scams have caused considerable detriment to consumers across Australia. Significant losses often stem from scammers using high-pressure sales tactics with reports to the ACCC in 2010 of consumers paying as much as $15 000 up-front followed by ongoing payments.

In 2009 and 2010 the ACCC joined with the Queensland Office of Fair Trading, Queensland Police, the Australian Securities and Investment Commission and the Australian Taxation Office to form a taskforce to target sports arbitrage and sports investment scams.

In May and September 2009 this taskforce instigated Operation Marble, which targeted a number of Gold Coast firms.

5 Paper available on the Parliament of Australia House of Representatives website—*www.aph.gov.au/house/index.htm*

The intelligence gathered through this operation continues to help the taskforce explore future complementary compliance and enforcement actions.

Email service provider partnership

In 2010 the ACCC started working with international email service providers to develop ways to better identify scam emails and reduce the harm they cause.

London Action Plan

The London Action Plan is a global collaboration of anti-spam regulatory authorities and industry representatives who work with the European Union's equivalent association, the Contact Network of Spam Authorities.

In October 2010 the ACCC attended the sixth Joint London Action Plan—Contact Network of Spam Authorities Workshop, a three-day conference hosted by the Australian Communications and Media Authority.

The event brought together experts, regulators and law enforcement agencies from Australia and more than 13 other countries to share experiences and develop strategies in the global fight against spam.

Throughout the conference, the need for streamlining global collaboration was repeatedly emphasised, while the need to engage with other jurisdictions was a clear outcome. Discussion also included the challenges faced by law enforcers, especially the difficulty in identifying and locating perpetrators and obtaining forensically sound evidence. The mobile wireless space was identified as a future area of concern.

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. Cross-border fraud and e-commerce are two current areas of focus with relevance to enforcement work on scams. The ACCC participates as a member of the Australian delegation.

6 Conclusions and challenges for 2011

In 2011 the increasingly sophisticated nature of scams and the growth in personalised scams will continue to pose challenges for the ACCC. Scammers will continue to masquerade as well-known government agencies or large global corporate entities to cheat consumers out of personal information and money. Higher contact levels show that consumers are becoming more alert to scam approaches and are more than ever willing to report them to the ACCC. However, many consumers still contact the ACCC reporting substantial losses.

The significant growth in visitors to the ACCC's SCAMwatch website and subscribers to its radar alert service shows a continued demand from the community for scam education resources and materials.

Along with international consumer protection and law enforcement agencies, the ACCC will continue to educate consumers to recognise and avoid scams and identify the steps they can take to prevent their personal information from falling into the hands of scammers. This is a growing challenge as consumers are increasingly encouraged to post their personal details online through social networking sites.

Ongoing challenges include the evolving nature of scams. As seen in 2010 technological advances can open up new avenues for scam approaches as well as the resurgence of approaches which were, until recently, considered old-style. The ways new technologies can be abused by scammers can be difficult to predict and this will continue to pose significant challenges for regulators. The ACCC will focus on unsolicited telephone scams in 2011 given the major growth in this activity in the second half of 2010.

The ACCC will continue to expand its collaboration with overseas regulators to confront the challenges of taking enforcement action against scammers who are often hard to trace or located in overseas jurisdictions. To meet these challenges the ACCC will continue to work in a collaborative manner with private and public entities to counter the prevalence of scam activity targeting Australians.

Appendix 1: 2010 SCAMwatch radars

Santa says stay scam savvy this holiday season

December 2010: SCAMwatch is advising consumers to be particularly cautious this festive season. Scams occur all year round but scammers prey heavily on people's generosity and vulnerabilities at Christmas.

End of year travel? Don't let scammers take you for a ride

December 2010: SCAMwatch is warning travellers to be cautious if they are approached on holidays by strangers offering travel club memberships which seem too good to be true.

Looking for rental properties online? Watch out for scams!

November 2010: SCAMwatch is warning consumers to be on the lookout for scam online classified ads for residential and holiday rental properties.

Don't be grounded by flight booking scams

November 2010: SCAMwatch is advising travellers to check the authenticity of flight booking websites before making any reservations for domestic and international travel.

Plan to get rich this racing season? Don't bet on it!

October 2010: SCAMwatch is warning punters this racing season to be cautious of investing in expensive betting schemes and software packages which make false claims of guaranteed winnings.

Scammers offer guaranteed Australian visas

October 2010: SCAMwatch and the Department of Immigration and Citizenship are warning people who wish to visit or migrate to Australia to be cautious of people offering guaranteed Australian visas.

Mystery shopper jobs

September 2010: SCAMwatch and South Australian Police are warning Australian job hunters to be wary of a mystery shopper job scam.

Hitman email scam

Updated September 2010: SCAMwatch and Victoria Police are warning Australians to beware of email death threats from scammers claiming to be hitmen hired to kill the email recipient unless they send cash.

Fake grants from a fake government department

September 2010: SCAMwatch and the Department of Infrastructure, Transport, Regional Development and Local Government are warning Australians of scammers who call offering fake government grants.

Beware of scam scratchie cards in your letterbox

Updated September 2010: If you unexpectedly receive colourful travel brochures in the mail, be very suspicious if the package also contains scratchie card tickets.

Do not pay for the Do Not Call Register

September 2010: Don't let someone trick you into paying to have your number listed on the Australian Government's free Do Not Call Register.

Aussie veterans targeted by scam

September 2010: SCAMwatch is warning veterans to be cautious of potential scammers posing as representatives from the Australian Government Department of Veterans' Affairs.

Pedigree pups at prices too good to be true

September 2010: SCAMwatch is again warning consumers to be cautious of classified ads for pedigree pups at prices that are too good to be true.

Telstra warns of email scam targeting BigPond customers

September 2010: Don't let scam emails fool you into providing your personal details.

Beware of green scheme scammers!

August 2010: Consumers are urged to beware of scammers who call offering rebates on energy efficient initiatives.

Scratchie card scams continue

July 2010: SCAMwatch continues to receive reports about scams involving scratchie cards received in the mail.

Spam SMS: report it!

July 2010: Are you an avid mobile phone texter, using SMS to keep in contact with friends and family? Watch out—scammers love texting too.

Refund scams: Australian Taxation Office taxes and bank fees

July 2010: If you receive a call or email claiming you're entitled to reclaim overpaid tax or bank fees, ignore it—these scams are doing the rounds.

Telemarketing scam: your computer has a virus!

July 2010: Don't let a scammer scare you into believing your computer is infected with a virus.

End of financial year: directory and fax back scams targetting small businesses

June 2010: With the end of the financial year upon us, small businesses across Australia are busy tidying up their financial affairs. However, this time is not only busy for business, but for scammers as well.

Beware of scams

June 2010: Scammers continue to target everyone, regardless of age, gender, education or income level.

Looking for 2010 FIFA World Cup tickets?

June 2010: FIFA has warned fans that genuine 2010 World Cup tickets can only be purchased from legitimate sources.

Scammers pretending to represent Medicare and Centrelink

May 2010: Recently, Medicare and Centrelink have received reports of scammers posing as employees asking recipients for their personal information.

TVI Express money-making venture

May 2010: The ACCC has quickly acted to stop the individuals behind TVI Express from enticing consumers to join its so called money-making venture.

Beware of scammers—offering compensation for disrupted travel plans

May 2010: The recent volcanic eruption in Iceland resulted in thousands of flights cancelled and travel plans disrupted.

Scammers infecting smartphones with viruses

May 2010: SCAMwatch reminds consumers to be careful when downloading and/or installing any electronic material on their computers and phones—including material from the internet (attachments and links) and phone applications.

Powerball bogus scam

April 2010: SCAMwatch alerts consumers to a company, Powerballwin.com.au Pty Ltd, that claimed it had a secret method to predict future Powerball draws.

Enjoy the Easter holiday—but watch out for Easter scams!

March 2010: Easter scams have become part of the ritual of using holidays and global and/or domestic events to trick Australians.

WesternField Holdings Inc. carbon credit investment scams

March 2010: SCAMwatch warns Australians to be wary of carbon credit investment opportunities from WesternField Holdings Inc.

Climate change grants and other government grants

February 2010: SCAMwatch has joined with the Australian Government Department of Climate Change and the Commonwealth Grants Commission to warn consumers about anyone who approaches them with the offer of grants for climate change or other government grants.

Be my Valentine

February 2010: SCAMwatch is warning those looking for love online to be wary of dating and romance scams.

Put the freeze on Winter Olympics holiday job scams

February 2010: SCAMwatch warns consumers to be wary of advance fee fraud disguised as bogus job offers.

Australian Taxation Office tax refund online!

February 2010: SCAMwatch is warning Australians to be on the lookout for an email purporting to be from the Australian Taxation Office trying to trick consumers into providing their private details.

Happy win or just a scam?

January 2010: SCAMwatch warns consumers to be wary of an advance fee fraud scam disguised as winnings from the Euphoria Travelling Group.

Haiti crisis scams

January 2010: Australians eager to help the nation of Haiti recover from the earthquake that struck on 12 January 2010 are being warned to be alert and ensure that they are not taken in by scammers.

The National Breast Cancer Foundation pink logo

January 2010: Australia's National Breast Cancer Foundation has raised concerns over unauthorised use of the trusted pink ribbon logo in relation to marketing of health-related products online.

Switch over to digital television is ripe for scams

January 2010: The Australian Government warns consumers to be very wary of door-to-door salespeople offering to sell you digital television products in your home.

Selling goods through the internet or classifieds?

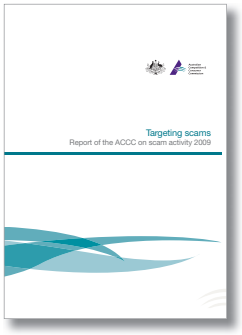
January 2010: If you are selling something over the internet or through the classifieds, you may be targeted by scammers posing as legitimate buyers!

Appendix 2: ACCC scam resources for consumers and businesses

Scam reports

Targeting scams: Report of the ACCC on scam activity 2009

Date published: 1 March 2010

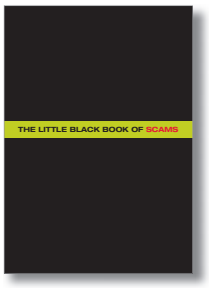


ACCC education resources

SCAMwatch website (www.scamwatch.gov.au)

The little black book of scams[6]

Date published: 24 February 2008



6 See the publications page at accc.gov.au.

Small business scams[7] (fact sheet)

Date published: 3 March 2010

Phishing scams[7] (fact sheet)

Date published: 23 October 2008

Money transfer scams[7] (fact sheet)

Date published: 23 October 2008

Lotteries, sweepstakes and competition scams[7] (fact sheet)

Date published: 23 October 2008

Fact sheet: *Sports investment scams*[7]

Date published: 25 June 2009

2010 ACFT campaign resources[8]

7 See the publications page at accc.gov.au.

8 See *www.scamwatch.gov.au*

Appendix 3: Key ACCC media releases and communications initiatives

2010 ACCC scam media releases

Beware the 10 Scams of Christmas, 8 December 2010

ACCC takes court action against 'Yellow Page' directories, 9 November 2010

Slam phone scammers: ACCC and ACMA (joint release), 12 October 2010

ACCC institutes proceedings for alleged blowing by Adepto Publications Pty Ltd, 11 October 2010

Beware of scratching your way into a scam, 7 October 2010

Internet sweep day focuses on the online generation, 21 September 2010

Working globally to combat mass marketing fraud, 1 June 2010

ACCC brings Powerball bogus scam to a halt, 23 April 2010

Consumers warned against Westernfield Holdings Inc investment, 16 March 2010

New ICPEN website—more information for consumers and consumer experts, 15 March 2010

False billing scams hit small business: Fraud Week warning, 3 March 2010

New scam protection advice for Darwin small businesses, 3 March 2010

Scams advice for online shoppers and small business: Fraud Week 2010, 3 March 2010

$70 million lost: ACCC scam activity report, 1 March 2010

Online offensive–fighting fraud online—Fraud Week 2010, 26 February 2010

Scammers breaking hearts online, 12 February 2010

2010 press articles contributed by the ACCC

'Due diligence or the possible nasty surprise', *Franchising Magazine,* December 2010.

'Help foil those sly scammers', *The Senior* (New South Wales and Victoria), January 2011 edition (published December 2010).

'Time to get smart … not scammed', *NT News*, 20 October 2010

'ACCC: Don't get sucked in by a scam', *My Business e-News*, 26 August 2010

'It pays to look out for false advertising bills', *Sydney Morning Herald*, 6 March 2010

'False billing major growth area for scammers', *The Age*, 3 March 2010

'Scams cost us many millions', *The Canberra Times,* 12 January 2010

2010 ACCC speeches containing scam messages

Bruce Cooper, Telstra Forensic Analysts Forum, 'Combating Scams—The ACCC's role in disrupting fraudulent activity', 7 December 2010.

David Snowden, International Mass Marketing Fraud Working Group meeting (Bruges), 'The use of Financial Intelligence Unit information in Australia to detect and disrupt scam activity', 4 November 2010.

Therese Dupe, Public Lecture National Seniors Week, 'Scam Awareness', 8 July 2010.

Brenton Philp, 11th Annual Fraud Summit 2010, 'Educating Consumers to be Safer Online', 28 June 2010.

Therese Dupe, Public Lecture, 'Fighting the Scammers—the ACCC tackles scams', 15 February 2010.

Appendix 4: Australasian Consumer Fraud Taskforce members and partners

Taskforce members

Australian Government

Attorney-General's Department

Australian Bureau of Statistics

Australian Communications and Media Authority

Australian Competition and Consumer Commission (Chair)

Australian Federal Police

Australian Institute of Criminology

Australian Securities and Investments Commission

Australian Taxation Office

Department of Broadband, Communications and the Digital Economy

New Zealand Government

New Zealand Commerce Commission

Scamwatch New Zealand (New Zealand Ministry of Consumer Affairs)

State and territory governments

Consumer Affairs Northern Territory

Consumer Affairs Victoria

Department of Commerce Western Australia

Fair Trading New South Wales

Office of Consumer Affairs and Fair Trading Tasmania

Office of Consumer and Business Affairs South Australia

Office of Fair Trading Queensland

Office of Regulatory Services Australian Capita Territory

Representatives of the state and territory police

New South Wales Police Fraud Squad

State and territory Police Commissioners

2010 Taskforce partners

Government partners

Australian Agency for International Development

Australian Commonwealth Scientific and Industrial Research Organisation

Australian Customs

Australian Department of Foreign Affairs and Trade

Australian Trade Commission (Austrade)

Child Support Agency

Comcare

Commonwealth Ombudsman

ComSuper

CRS Australia

Department of Finance and Deregulation

Department of Human Services

Department of Immigration and Citizenship

Department of Innovation, Industry, Science and Research

Department of Parliamentary Services, Parliament of Australia

Energy and Water Ombudsman of New South Wales

Energy and Water Ombudsman of Victoria

Fair Work Ombudsman

Federal Magistrates Court of Australia

Financial Ombudsman Service

Geoscience Australia

Insurance Ombudsman Service

Intellectual Property Australia

Medicare

Migration Review Tribunal and Refugee Review Tribunal

National Archives of Australia

National Audit Office

National Library of Australia

National Native Title Tribunal

Office of the Inspector-General of Intelligence and Security

Office of the Official Secretary to the Governor-General

Office of the Privacy Commissioner
Social Securities Appeal Tribunal
Telecommunications Industry Ombudsman
Workplace Ombudsman

Private partners

AAPT
Abacus—Australian Mutuals
Adelaide Bank
Age Concern
Ailean
ANZ
Australia Post
Australian Bankers' Association
Australian Computer Emergency Reponse Team
Australian Computer Society Victoria
Australian Domain Name Administrator
Australian Hotels Association
Australian Mobile Telecommunications Association
Australian Super
Australian Telecommunications User Group
Bankwest
Beinteractive
Bendigo Bank
Betfair
CHOICE
Commonwealth Bank
Communications Alliance
CPA Australia
eBay Australia
Internet Industry Association
Internet Society of Australia
MasterCard
Microsoft
Motor Trades Association of Australia
Motor Trades Association of Australia Super
MySpace
National Australia Bank
Optus
PayPal Australia
PhoneChoice
Publishers Advertising Advisory Bureau
Sensis
Suncorp–Metway
Symantec
Telstra
Trading Post
Visa International Australia
Westpac

Community partners

Alexandra District Hospital
Australia Council of Social Services
Australian Council on the Ageing—South Australia
Australian Council on the Ageing—Victoria
Australian Federation of Disability Organisations
Australian Financial Counselling and Credit Reform Association
Australian Seniors Computer Clubs Association
Banyule Community Health
Better Hearing Australia Vic Inc
Brotherhood of St Laurence
Child and Family Services
Community Connections Victoria
Community Information Diamond Valley
Community Technology Centres Association
Consumer Action Law Centre
Consumers Federation of Australia
Consumers' Telecommunications Network
Country Women's Association of Australia
Cranbourne Information and Support Service
Federation of Ethnic Communties Council of Australia
Financial and Consumer Rights Council Victoria
Indigenous Consumer Assistance Network
JobWatch
Kidsafe Victoria
Laverton Community Centre
National Association of Community Legal Centres
National Children's and Youth Law Centre
Neighbourhood Watch
Otway Health and Community Services
Public Interest Advocacy Centre
Reach Out for Kids Foundation
RSL Headquarters
*RSL New South W*ales
*RSL South A*ustralia
*RSL West A*ustralia
Seniors Information Victoria
The Benevolent Society

The Salvation Army

Western Australia Council of Social Services Inc.

Whittlesea Community Connections

2011 Taskforce Partners

As at 31 January 2011, the following partners have confirmed their involvement with the Taskforce for 2011.

Principal Partners

Australian Communications Consumer Action Network

BankWest

Gumtree

Holiday Coast Credit Union

Horseyard.com.au

Telstra

Yahoo

Partners

Consumer advocacy (general)

CHOICE

Public Interest Advocacy Centre

Legal centres/associations

Consumer Action Law Centre

National Association of Community Legal Centres

Peninsula Community Legal Centre Inc.

Financial services

Abacus—Australian Mutuals

ANZ Bank

Australian Bankers' Association

Australian Financial & Consumer Rights Council Australia

Australian National Audit Office

Commonwealth Bank

ComSuper

Holiday Coast Credit Union

Police Credit Union

Western Union

Westpac Bank

Gaming associations

Australian Casino Association

BetFair

sportsalive.com

Tabcorp

Ombudsman services

Energy & Water Ombudsman of NSW

Fair Work Ombudsman

Social/welfare/community bodies

Australian Financial Counselling & Credit Reform Association

Better Hearing Australia Vic Inc

Brotherhood of St Laurence

Country Women's Association of Australia

Cranbourne Information & Support Service

CRS Australia

Dept of Human Services

Diamond Valley Community Support

Laverton Community Centre

Neighbourhood Watch

Social Securities Appeal Tribunal

The Australian Federation of Disability Organisations

Western Australia Council of Social Services Inc.

Whittlesea Community Connections

RSL groups

RSL NSW

RSL SA

RSL TAS

Aged care services

Australian Council on the Ageing—QLD

Australian Council on the Ageing—TAS

Australian Council on the Ageing—WA

Australian Seniors Computer Club Association

Seniors Information Victoria

Housing associations

Tenants Union of Victoria

Online and computer bodies

Australian Computer Emergency Response Team

Australian Computer Society

Community Technology Centres Association

eBay

Internet Industry Association

Surete Group

Internet security

Symantec

Telecommunications

Australian Mobile Telecommunications Association

Australian Telecommunications User Group

Communications Alliance

Miscellaneous

Ailean

Australia Post

Cootamundra Police Station

Migration Review Tribunal (MRT) & Refugee Review Tribunal (RRT)

National Archives of Australia

Victoria Police