Australian
Competition &
Consumer
Commission

Targeting scams

Report of the ACCC on scam activity 2011

Dr Michael Schaper
Chairman, Australasian Consumer Fraud Taskforce

Foreword

The Australian Competition and Consumer Commission's (ACCC) third annual report on scam activity and consumer fraud shows continued growth in the number of consumers and small businesses reporting scams. More than 83 000 scam reports and enquiries were received by the ACCC in 2011 with reported losses more than $85.6 million, a 35 per cent increase from 2010. While this continuing increase supports growing public awareness of the ACCC as an avenue to report scams, these figures also show that scams targeting Australians continue to evolve and increase. Scammers are going to great efforts to adjust their approach and deceive victims.

This report is designed to raise awareness of the problem and extent of scams. It explains key trends observed by the ACCC in 2011. We hope this report will promote discussion about how we can best address the challenges posed by scams to the Australian community.

In 2011 reports indicated a shift to 'high volume scams', which are delivered to a large number of recipients but cause smaller amounts of loss per victim. The ACCC observed a shift from internet and email to telephone as the preferred method of scam delivery, assisted in part by the abuse of cheap or freely available voice-over-internet services. Almost 52 per cent of consumers reporting scams to the ACCC in 2011 reported being approached in this manner. The Australasian Consumer Fraud Taskforce's (ACFT) 2012 Slam Scams! Fraud Week campaign will focus on raising public awareness of the delivery methods used by scammers.

In 2011 the ACCC remained active in the area of scams awareness, launching its SCAMwatch Twitter page in March which quickly gained thousands of followers. The SCAMwatch website received in excess of 20.5 million hits over the year, almost 400 per cent more than in 2010. Close to 5000 people subscribed to receive email alerts from SCAMwatch warning of emerging scam threats.

This report also highlights the extensive work conducted by the ACCC with other regulators and law enforcement agencies to disrupt scams and educate consumers and small businesses. International and domestic partnerships with consumer, government and private organisations are critical to tackling the increasingly personalised and sophisticated nature of scams. Through the ACFT and other partnerships, the ACCC will continue to work collaboratively to try to minimise the harm arising from consumer fraud.

Dr Michael Schaper

Deputy Chairman, ACCC
Chairman, Australasian Consumer Fraud Taskforce

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

© Commonwealth of Australia 2012

This work is copyright. Apart from any use permitted by the *Copyright Act 1968*, no part may be reproduced without prior written permission from the Commonwealth available through the Australian Competition and Consumer Commission. Requests and inquiries concerning reproduction and rights should be addressed to the Director Publishing, Australian Competition and Consumer Commission, GPO Box 3131, Canberra ACT 2601 or by email to publishing.unit@accc.gov.au.

ISBN 978 1 921964 80 0

ACCC 03/12_24005_450

www.accc.gov.au

Contents

Foreword i

1 Snapshot of 2011 1

2 Contacts and trends 2

2.1 Scam reports and inquiries received by the ACCC 2

2.2 Financial losses reported to the ACCC 4

2.3 Most reported scams 5

2.4 Understanding the victim experience—Australian Institute of Criminology research report 17

3 Awareness raising and education initiatives 19

3.1 SCAMwatch website—www.scamwatch.gov.au 19

3.2 SCAMwatch joins Twitter 21

3.3 Printed materials 21

3.4 Media and communications activity 22

3.5 National education and engagement activities 22

4 Action to disrupt scams and enforce the law 24

4.1 Scam disruption activities 24

4.2 Scam-related enforcement activities 25

5 Domestic and international collaboration 27

5.1 The Australasian Consumer Fraud Taskforce 27

5.2 The International Consumer Protection and Enforcement Network 29

5.3 International Mass Marketing Fraud Working Group 30

5.4 The Cyber White Paper 31

5.5 Investment Scams Task Force 31

5.6 Australian Transaction Reports and Analysis Centre partnership 31

5.7 Organisation for Economic Co-operation and Development Committee on Consumer Policy 32

6 Conclusions and challenges for 2012 33

Appendix 1: 2011 SCAMwatch radars 34

Appendix 2: ACCC scam-related resources for consumers and businesses 37

Appendix 3: Key ACCC media releases and communications initiatives 39

Appendix 4: Australasian Consumer Fraud Taskforce members and partners 40

1 Snapshot of 2011

Scams reports

- In 2011 the ACCC received 83 150 scam-related contacts from consumers and small businesses, almost double that of 2010 when 42 385 contacts were received, and more than four times that of 2009 (20 554 contacts).
- Scam losses reported to the ACCC totalled $85 607 748, a 35 per cent increase from 2010 ($63 436 348). Losses reported are 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 (nearly 88 per cent) who contacted the ACCC about scams in 2011 reported no financial loss. The most common category of loss was $100 to $499 compared to $1000 to $9999 in 2010. This indicates an increase in 'high volume scams', which are delivered to large numbers of recipients but cause smaller amounts of loss per victim.

Most reported scams

- For the third consecutive year, mass marketed advance fee fraud (MMAFF) recorded the highest number of scam reports, contributing to more than half (44 233) the total reported to the ACCC.
- Computer hacking was the second most reported scam type in 2011, contributing more than 23 per cent to the total scam reports to the ACCC, compared to almost 12 per cent in 2010. For the second consecutive year this was largely due to scam phone calls requesting remote access to the recipient's computer to 'fix' technical problems.
- The ACCC also continued to receive a high level of contact about online auction and shopping scams, banking and online account scams, false billing, job and employment scams, and computer prediction software scams.

Age

- In 2011 scams were most commonly reported in the 25 to 34, 35 to 44 and 45 to 54 year age groups.

Scam delivery method

- In 2011 the ACCC observed a shift in preferred mode of scam delivery from online methods (including internet and email) in 2010, to unsolicited telephone calls in 2011. Almost 52 per cent of scams reported to the ACCC in 2011 were delivered by phone, increasing from just over 33 per cent in 2010 and almost 10 per cent in 2009. The ACCC received 42 977 reports of scam telephone calls in 2011 with a total loss of $27 773 729.

The ACCC's awareness raising and education activities

- Community awareness and interest in scams continued to grow. In 2011 the SCAMwatch website received in excess of 20.5 million hits, approximately 15 million more than in 2010, or an almost 400 per cent increase. It also attracted 774 989 unique visitors in 2011, almost 275 000 more visitors than 2010.
- Since its launch in March 2011 the ACCC's SCAMwatch Twitter account gained 2636 followers.
- In 2011 the ACCC distributed more than 77 000 copies of its scam-related publications.

The ACCC's collaboration, scam disruption and enforcement activities

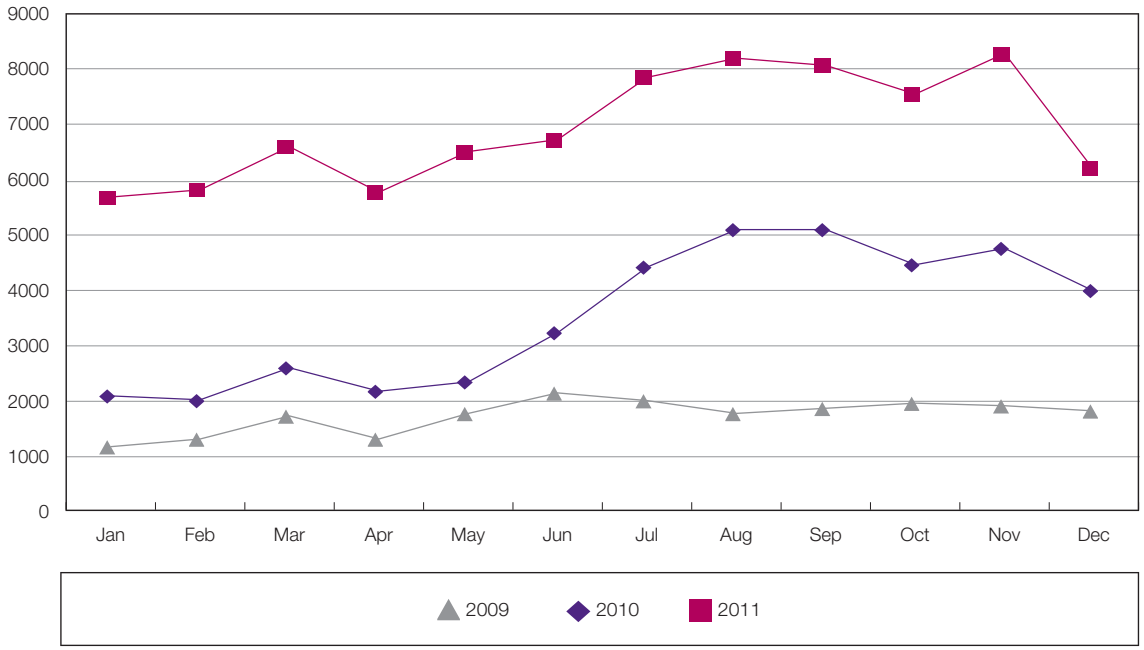
- In 2011 the ACCC worked extensively with a wide range of domestic and international agencies and private bodies to disrupt scams, enforce the law, and protect consumers and small business from scams.
- A key initiative was the ACCC's work with private operators of dating websites to address scams targeting their users. The ACCC also joined the Australian Crime Commission's multi-agency task force aiming to disrupt fraudulent, serious and organised investment scams. The ACCC continued to chair the Australasian Consumer Fraud Taskforce in 2011, hosting two events during the year.

2 Contacts and trends

2.1 Scam reports and inquiries received by the ACCC

From 1 January to 31 December 2011 the ACCC received 83 150 scam-related contacts (82 338 scam reports and 812 inquiries). This represents almost double that of 2010 (42 385 contacts—41 582 scam reports and 803 inquiries) and more than four times that of 2009 (20 554 contacts—19 886 scam reports and 668 inquiries). These shifts are illustrated in Figure 1.

Figure 1: Number of scam-related contacts made with the ACCC in 2011, 2010 and 2009



The continued increase may be attributed to a number of factors including:

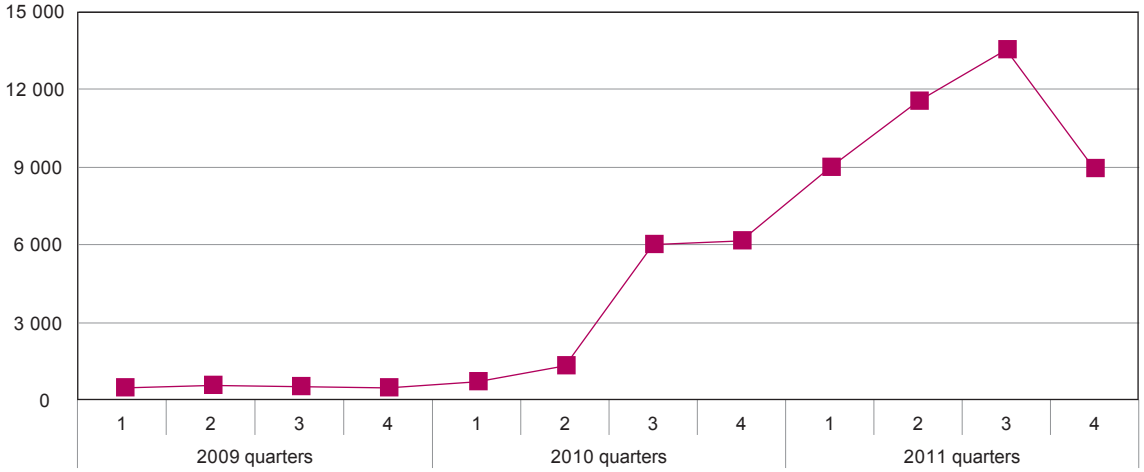
- heightened consumer awareness of scam approaches and the option to report to organisations such as the ACCC
- continued consumer education activities, such as the launch of the ACCC's SCAMwatch Twitter page in 2011, which gained more than 2636 followers in its first 10 months
- scammers' increased sophistication and use of low-cost technologies and services to target ever-growing audiences with convincing personalised approaches.

Scam reports increased across many scam types. Reports of scams delivered by unsolicited telephone calls also increased, assisted in part by the abuse of cheap or freely available voice-over-internet services (VoIP).

Method of delivery of scams

In 2011 the ACCC observed a shift in the preferred method of scam delivery from online (including internet and email) in 2010, to unsolicited telephone calls. Almost 52 per cent of scams reported to the ACCC in 2011 were delivered by telephone, increasing from just over 33 per cent reported in 2010. Figure 2 shows the significant increase since the third quarter of 2010 in consumers reporting that they were contacted with scam telephone calls. This scam delivery method was reported 42 977 times in 2011 and can be attributed to a total loss of $27 773 729.

Figure 2: Comparison between number of consumers who reported being contacted by telephone in 2011, 2010 and 2009



Online methods of scam delivery (including the internet and email) continued to be popular as the second most commonly reported, at slightly over 28 per cent. However this represented a significant decrease from the 45 per cent reported in 2010.

Table 1 compares scam delivery methods in 2011 and 2010. Other methods in 2011 included text message (almost 10 per cent), postal mail (almost 8 per cent), other, such as newspaper advertisements (just over 1 per cent), and in person and fax (each under 1 per cent).

Table 1: Scam delivery methods during 2011 and 2010

	2011		2010	
Scam delivery method	**Number**	**Percentage**	**Number**	**Percentage**
Phone	42 977	51.7	14 144	33.4
Email	15 080	18.1	8 213	19.4
Internet	8 698	10.5	10 861	25.6
Text	8 264	9.9	2 618	6.2
Mail	6 508	7.8	4 621	10.9
Other	884	1.1	584	1.4
In person	580	0.7	386	0.9
Fax	159	0.2	958	2.3

Similar to 2010, in 2011 the ACCC continued to receive consumer reports indicating that many telephone scams may be operating through overseas call centres. This could be due to the continued outsourcing by criminal networks of unsolicited telephone activities to cheaper overseas providers and to the growing availability of low or no-cost VoIP call services.

While VoIP call services are provided through the internet, reports indicate that the scam approach is usually directed at the home telephone and it is almost exclusively reported to the ACCC as a telephone scam. The ACCC categorises scams delivered through VoIP as a telephone delivery method.

The most prominent scams delivered by phone in 2011 included calls:

- claiming the recipient's computer was infected with a virus and requesting remote access and payment to fix it
- requesting payment to deliver fake parcels
- offering fake government rebates to install solar panels
- offering fake carbon compensation payments
- conducting fake surveys or scam surveys
- offering to reclaim fake overcharged bank fees or tax refunds.

Scam callers often pretended to be from government or large well-known companies including banks, computer companies and telecommunications service providers.

Age range

While the provision of age data to the ACCC is voluntary, of those who provided these details, almost 63 per cent were between 25 and 54 years of age. As shown in Table 2, the percentage of individuals contacting the ACCC between 55 and 64 and over 65 years of age increased. In contrast, the percentage of contacts from people under 18, and in the 18 to 24, 25 to 34 and 35 to 44 years of age categories decreased.

Table 2: Comparison of age ranges provided by consumers when they contacted the ACCC in 2011 and 2010

Age range	Number	Percentage	Variance from 2010
<18	164	0.7	–0.1
18–24	1958	8.1	–1.1
25–34	4915	20.4	–0.9
35–44	5064	21.1	–3.4
45–54	5110	21.2	–0.2
55–64	3871	16.1	+3.3
>65	2970	12.3	+2.4

2.2 Financial losses reported to the ACCC

In 2011 the ACCC received reports of losses arising from scam activity of $85 607 748, a 35 per cent increase on the amount reported in 2010 ($63 436 348). It is important to note that this amount is based on information provided to the ACCC by complainants. As such, it does not represent the actual total financial loss to Australians caused by scams in 2011. The ACCC considers that the figure represents only a proportion of total losses—many scams are unreported and the ACCC is only one of many agencies that receive scam complaints.

In 2011 almost 88 per cent of consumers contacting the ACCC about scams reported no financial loss. The remaining almost 13 per cent reported losses ranging from very small amounts for unsolicited credit card deductions up to $3.5 million for a business that was a victim of advance fee fraud.

Table 3 provides a breakdown and comparison of the financial losses reported by consumers in 2011 and 2010. The data shows an increase in 'high volume scams', which request small amounts of money but target a large number of recipients. Typically these scams cause smaller amounts of loss per victim. In 2010 the most commonly reported loss ranged from $1000 to $9999, but dropped significantly to $100 to $499 in 2011. The ACCC recognises that some reported losses may represent amounts that complainants believe they may have been entitled to if the offer were genuine.

Table 3: Comparison of scam-related monetary losses reported by consumers in 2011 and 2010

Monetary range ($)	Number of people reporting this loss amount in 2011	Variance from 2010
1–99	1335	+601
100–499	3486	+1508
500–999	1310	+505
1 000–9 999	2696	+492
10 000–49 999	865	+241
50 000–499 999	319	+115
500 000–999 999	14	–1
1 million–10 million	3	–1
10 million +	0	0

2.3 Most reported scams

Overview of scams reported to the ACCC in 2011

Table 4 provides an overview of all scam types reported to the ACCC in 2011, including the number of consumers reporting losses from each scam and the total sum of losses per scam type.

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 respond, then subsequently lose money. Some categories, such as dating and romance scams, have comparatively low numbers of reports but achieve very high conversion rates.

Table 4: Overview of scams types reported to the ACCC in 2011 in order of total reported losses

Scam type	Total reported loss	Number of reported scams	Number of people who reported a loss	Number reporting losses more than $10 000	Number reporting losses less than $10 000	Number reporting no loss	% of people who lost money (conversion rate)
Advance fee/up-front payment	$27 483 743	30 426	2759	330	2429	27 667	9.1
Dating and romance (including adult services)	$21 908 851	2 110	1013	348	665	1 097	48.0
Investment seminars and real estate	$10 143 200	552	252	132	120	300	45.7
Job and employment (including business opportunity)	$7 342 643	2 505	368	76	292	2 137	14.7
Computer prediction software (including betting)	$4 712 528	646	291	89	202	355	45.0
Online auction and shopping	$4 161 590	5 012	2177	69	2108	2 835	43.4
Lottery and sweepstakes	$4 015 544	7 863	277	62	215	7 586	3.5
Unexpected prizes	$1 968 942	3 834	171	24	147	3 663	4.5
Banking and online account (including phishing)	$1 299 869	5 430	253	21	232	5 177	4.7
Computer hacking	$625 464	19 473	1537	8	1529	17 936	7.9
False billing (advertising, directories, domain names, office supplies)	$615 071	2 754	412	13	399	2 342	15.0
Door-to-door and home maintenance	$312 744	276	43	4	39	233	15.6
Spam and ‘free’ offers on the internet	$219 074	530	92	1	91	438	17.4
Chain letter and pyramid scheme	$101 275	158	9	3	6	149	5.7
Health and medical (including weight-loss, miracle cures)	$56 368	274	124	1	123	150	45.3
Mobile phone (ringtones, competitions, missed calls)	$40 444	509	99	1	98	410	19.4
Psychic and clairvoyant	$13 987	72	29	0	29	43	40.3
Fax back	$1 300	24	3	0	3	21	12.5
Other	$585 113	702	119	19	100	583	17.0

For more information on the broad variety of scams affecting Australians visit the SCAMwatch website at: www.scamwatch.gov.au.

The top 10 scams reported to the ACCC in 2011

For the third consecutive year, mass marketed advance fee fraud (MMAFF) recorded the highest number of scam reports, contributing to more than half (44 233) the total scams reported to the ACCC in 2011. MMAFF consists of four of the scam types listed in Table 5—advance fee/up-front payment, lottery and sweepstakes, unexpected prizes, and dating and romance scams.

The ACCC also continued to receive considerable complaints about the other scams listed in Table 5, including computer hacking, banking and online account, false billing, job and employment, and computer prediction software scams.

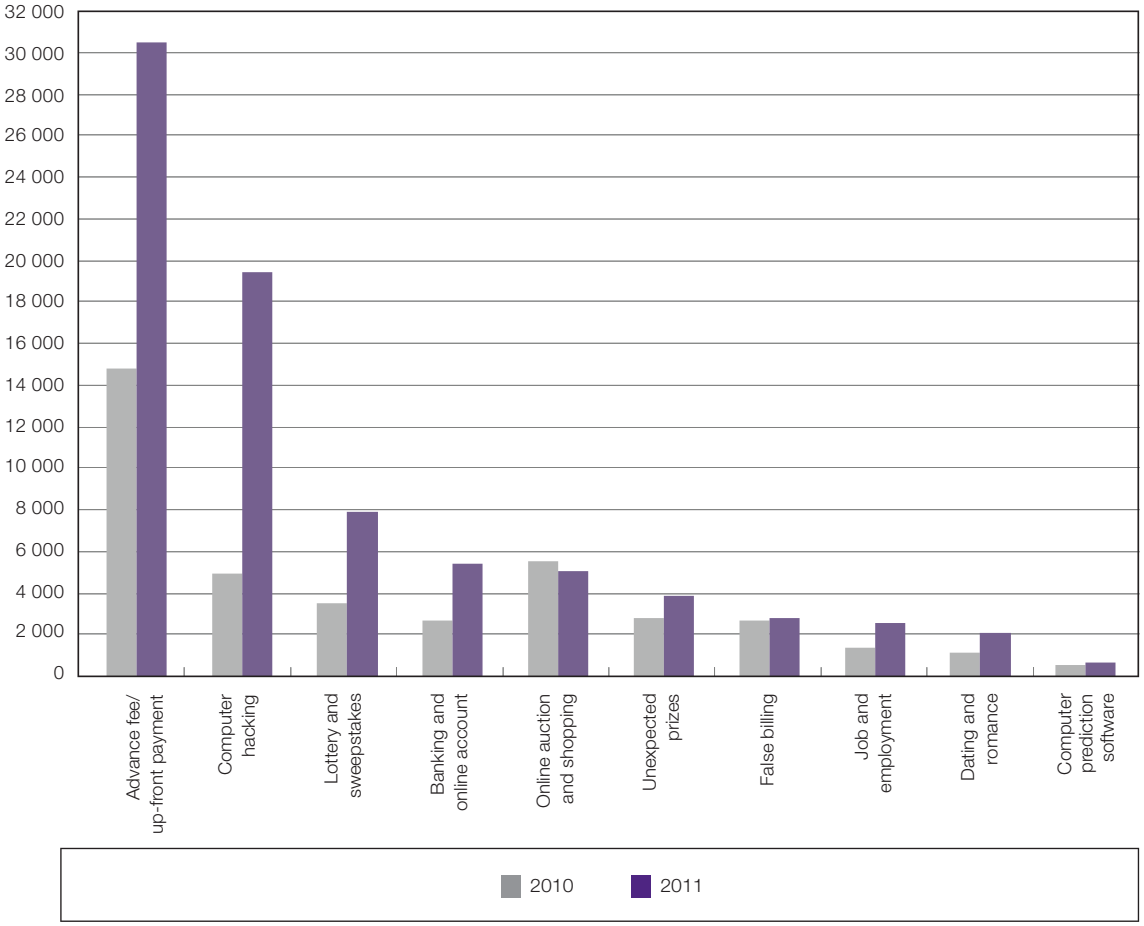
Of particular note in 2011 was a reduction in reports of online auction and shopping scams. In 2010 these were the second most reported scams but dropped to the fifth most reported in 2011, despite the growth in popularity of online shopping in Australia.

Table 5: Top 10 identified scam types complained about to the ACCC in 2011

Type	Total scams reported to ACCC in 2011	% of total reports
Advance fee/up-front payment	30 426	36.6
Computer hacking	19 473	23.4
Lottery and sweepstakes	7 863	9.5
Banking and online account (including phishing)	5 430	6.5
Online auction and shopping	5 012	6.0
Unexpected prizes	3 834	4.6
False billing	2 754	3.3
Job and employment (including business opportunity)	2 505	3.0
Dating and romance (including adult services)	2 110	2.5
Computer prediction software (including betting)	646	0.8

Figure 3 compares the number of reports of the top 10 scam types in 2011 and 2010. Growth was recorded across all scam categories except online auction and shopping which decreased slightly in 2011, false billing and computer prediction software which both remained the same.

Figure 3: Comparison of the number of reports of the top 10 scam types in 2010 and 2011



Mass marketed advance fee fraud

The ACCC defines MMAFF as any scam involving a scammer requesting fees up-front in return for goods, services or rewards that they never supply. MMAFF characteristically tricks consumers into sending money by using inventive and seemingly legitimate reasons for requesting payment, for example, paying fees or taxes to claim a prize, reward or other benefit.

Details on the four types of MMAFF scams are provided below.

Advance fee/up-front payment scams

Number of scam reports in 2011: 30 426

Per cent of total scams reported in 2011: 36.6

Number of consumers reporting losses: 2759

Total losses reported by consumers: $27 483 743

Scam conversion rate: 9.1 per cent

The proportion of reports of advance fee/up-front payment fraud during 2011 increased by almost two per cent from 2010 and for the third consecutive year it was the most commonly reported scam type to the ACCC.

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.

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

In 2011 the ACCC continued to see large numbers of advance fee/up-front payment scams initiated by telephone. 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 provide payments and personal details more readily.

In 2011 scammers pretended to be from the following government departments or services:

- the Australian Government
- the Office of Fair Trading
- the fictitious 'Australian Government Reclaim Department' or 'Australian Council'
- the Australian Taxation Office
- Centrelink
- Consumer Affairs Victoria
- various birth, death and marriage registries.

Scammers even masqueraded as the ACCC's SCAMwatch service.

Scammers also posed as representatives from private companies including:

- banks
- computer companies
- telecommunications services
- postal and logistics services
- solar panel installers.

Reports of advance fee/up-front payment scams delivered by fake online classifieds ads continued in 2011. While scam ads for pets, used cars, boats and bikes continued to be popular, 2011 saw an increase in scam offers for electronic items such as smartphones, tablet devices and laptops. This activity often became more prominent around the launch or upgrade of products, and commonly involved the promise of bonus products with bulk purchases, for example, 'buy three, get one free'.

Classifieds scam ads often show a product at a significantly lower price than it is available elsewhere or even on the same website. As with many advance fee scams, victims are asked to send funds by wire transfer, money order or international funds transfer. Scammers abuse these payment services as it is difficult to trace or recover money sent this way.

Victim story: Consumer loses more than $20 000 to bank fee reclaim scam

A consumer received a phone call from a scammer who said the consumer had been overcharged $3495 in bank fees. The scammer offered to retrieve these fees following a $1550 payment by way of wire transfer.

The scammer claimed to be from the Office of Fair Trading and provided a client reference number and a return phone number to make the scam appear convincing.

Following the initial payment, the victim was advised she had been overcharged $32 000 and that she could get this money back if she first paid four more instalments of $4500 and one donation of $4000. The scammer threatened that the victim could not get any money back unless she made this donation.

The victim never received any of the money promised and lost $23 550 dollars to this scam.

From the SCAMwatch radar: Your parcel could not be delivered

In 2011 scammers called consumers claiming that they had been posted a parcel that could not be delivered due to, for example, size or weight.

Scammers pretended to be staff from postal or logistics services and said they could redeliver the fake parcels for a fee. Some scammers also asked for personal details. Parcels were never delivered following payment.

This scam played on the fact that online shopping is popular in Australia with high numbers of parcels sent and received through postal and logistics services. To make the scam seem legitimate, scammers carried it out during the lead up to Christmas, when Australians normally send and receive millions of parcels.

In November 2011 Australia Post joined with SCAMwatch to advise Australians that it would never call consumers requesting payment for undelivered mail items.

Read more on the SCAMwatch radar: www.scamwatch.gov.au.

Lottery and sweepstakes scams

Number of scam reports in 2011: 7863

Per cent of total scams reported in 2011: 9.5

Number of consumers reporting losses: 277

Total losses reported by consumers: $4 015 544

Scam conversion rate: 3.5 per cent

Lottery and sweepstake scams were the third most commonly reported to the ACCC in 2011. In these scams, consumers are told they have won money in a lottery they never entered. The winnings are commonly offered in currencies other than Australian dollars, for example British pounds or American dollars. To claim winnings, victims are asked to provide an up-front payment and/or personal details. Victims are not able to use their 'winnings' to pay the required fees and no money is ever received.

These scams continued to be sent by post and email in 2011 but were increasingly popular using SMS. SMS lottery scams often abuse genuine company names and brands including computer, car and mobile phone manufacturers.

Victim story: Consumer loses almost $18 000 to fake lottery

A consumer had been using lottery websites for some time so was pleasantly surprised when he was contacted and told he had won US$10 million. What the victim did not realise was that he had been contacted by a scammer.

The scammer told the victim that he must pay various up-front fees by way of wire transfer to claim his winnings. The victim paid a total of $18 000 and never received the money promised.

The scammer kept making excuses for more up-front payments including asking for money to cover 'internal revenue' and charges to convert the money into Australian dollars. No money was ever received.

From the SCAMwatch radar: Lottery scammers seek credit card details

In late 2011 SCAMwatch received numerous reports of scammers sending letters to recipients claiming they had won $15 000 or $25 000 in a lottery they had never entered. The scammers claimed to be from a lottery company in the United States.

The scam letters looked official and were accompanied with forms the victims had to complete and return in a supplied prepaid envelope. Scammers commonly asked for an initial up-front payment of $25 to enable the victim to claim winnings. However following the initial payment, victims were asked for additional, larger amounts.

Unsuspecting victims were invited to pay the initial fee by providing their credit card details on the form, exposing themselves to credit card fraud or identity theft.

Read more on the SCAMwatch radar: www.scamwatch.gov.au.

Unexpected prizes scams

Number of scam reports in 2011: 3834

Per cent of total scams reported in 2011: 4.6

Number of consumers reporting losses: 171

Total losses reported by consumers: $1 968 942

Scam conversion rate: 4.5 per cent

With unexpected prizes scams, scammers offer consumers a prize, such as a cheap holiday, smartphone or laptop, to elicit payment or obtain personal or credit card details. Often the promised prize does not exist or is not what was promised. Unexpected prize scams operate in a similar way to lottery and sweepstakes scams, however the scammer offers a good or service rather than money.

Victim story: Free holiday offer leads to credit card fraud

A consumer received a call from a scammer who claimed to be in the United States. The scammer was offering a free 15-day holiday for up to five people.

The scammer told the victim that he had been nominated to receive the holiday by his credit card provider for being an 'excellent customer'. The scammer offered the victim the option of taking $15 000 in cash instead of the holiday.

The scammer asked the victim to provide his credit card details so the victim could be registered as a client. When the victim subsequently contacted his bank he found that the scammer had taken $1000 from his credit card account.

From the SCAMwatch radar: Won a new car in a promotion you did not enter?

In early 2011, SCAMwatch received reports of scammers masquerading as a well-known car manufacturer, sending text messages to victims claiming they had won a new car in a promotion or lottery they had never entered.

Some messages also claimed that the victim had won money in a non-existent lottery held by the car manufacturer.

The text messages requested a response that involved the victims providing personal details and a payment to claim their prize.

Read more on the SCAMwatch radar: www.scamwatch.gov.au.

Dating and romance scams

Number of scam reports in 2011: 2110

Per cent of total scams reported in 2011: 2.5

Number of consumers reporting losses: 1013

Total losses reported by consumers: $21 908 851

Scam conversion rate: 48 per cent

Dating and romance scam losses per victim continued to be high in comparison to most other scam categories. Almost five per cent of consumers who reported a loss to this type of scam in 2011 lost more than $100 000.

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. This scam type commonly sees the scammer trying to exploit their victim's emotions. Dating and romance scammers often approach their victims on legitimate dating websites, then quickly attempt to move the victim away from the security of the website, communicating through other methods such as email.

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

In 2011 the ACCC launched a project working with operators of dating websites to address scams targeting their users. More details are in Section 4.1.

Victim story: Consumer loses $100 000 in 'soldier' romance scam

As is often the case with dating and romance scams, the victim reported meeting a scammer through a scam profile on a legitimate dating website. The scammer was masquerading as a romantic interest and pretending to be an American soldier serving overseas. He declared his love for the victim quickly and was convincing.

After gaining his victim's trust the scammer started asking for large sums of money to be sent by way of international wire transfer.

The scammer claimed he needed the money due to a series of 'mishaps', including accidents and injuries. He promised he could buy a leave pass to visit the victim if she provided enough money.

The victim realised it was a scam when the requests for money did not stop. Each time the scammer was scheduled to come to Australia another excuse would arise that prevented him from travelling and required more money from the victim.

The victim stopped sending money but shortly after was approached by the same or another scammer, this time pretending to be from a law enforcement agency. This time the scammer promised they could secure and return the money the victim initially lost, but that more wire transfer payments were required for this service. Upon paying, the victim never received any money back. The two scams cost the victim $100 000, as well as leaving her feeling hurt and betrayed.

Computer hacking scams

Number of scam reports in 2011: 19 473

Per cent of total scams reported in 2011: 23.4

Number of consumers reporting losses: 1537

Total losses reported by consumers: $625 464

Scam conversion rate: 7.9 per cent

Computer hacking was the second most reported scam to the ACCC in 2011, contributing more than 23 per cent to the total number of scam reports compared to just under 12 per cent in 2010.

As in 2010, the majority of consumers who reported a scam under this category received a phone call from a scammer posing as a representative of a well-known computer or telecommunications company. The scammer led their victim to believe their computer was infected with a non-existent virus or experiencing other technical problems that could only be fixed by giving the scammer remote access to the computer.

Once access was granted, the computer was vulnerable to the scammer installing malware and spyware that could gather the victim's online passwords, as well as other personal and financial details. The scammer also encouraged their victim to visit a scam website during the call and enter their credit card details to buy fake antivirus software. This software was a ruse to gain access to the victim's financial information and install additional malware, spyware or viruses onto the victim's computer.

In these scams, the victim was present when the scam was committed and was directed by the scammer to compromise the security of their own computer and personal details. This is a departure from the anonymous internet-based hacking scams of previous years, in which the victim had no contact with the scammer. In these more recent scams, the scammer often takes advantage of their direct contact with the victim to make the victim fear the repercussions of not granting remote access or installing software.

Another prominent scam in this category in 2011 involved scammers hacking consumers' social networking and email accounts. After accessing the account, the scammer would commit identity theft, posing as the owner to gain money or personal details from friends, family, followers or contacts. Account hacking was often initiated by a phishing scam asking the victim to enter their account password on a fake copy of their social networking site or email login page.

Victim story: Social networking account hacked

In a common hacking scam, a victim's social networking account was compromised after they provided their password and account details in response to a phishing scam email. The victim lost control of their account as the scammer changed the password used to access the account. The scammer then began having conversations with many of the victim's online friends.

Having gathered email addresses off the friends, the scammer then contacted them posing as the victim, claiming he was in London being held at gun-point and had lost his money and passport. The scammer asked the victim's friends to send money by an international wire transfer service.

The victim's aunty, trying to help, unwittingly sent $1400 to the scammer and as such became a victim herself.

Online auction and shopping scams

Number of scam reports in 2011: 5012

Per cent of total scams reported in 2011: 6

Number of consumers reporting losses: 2177

Total losses reported by consumers: $4 161 590

Scam conversion rate: 43.4 per cent

After being the second most reported scam in both 2010 and 2009, online auction and shopping scams dropped to the fifth most reported in 2011, contributing six per cent to the ACCC's total scam contacts throughout the year. The conversion rate on this scam increased nine per cent from 2010.

In this scam category, scammers typically advertise products on popular online auction websites, however when the victim 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 scam category.

Victim story: Consumer loses $20 000 to boat sale scam

A consumer was interested in buying a boat and thought he had found the perfect one listed on an online auction website.

The price seemed too good to pass up so the consumer contacted the seller and was told he needed to pay the full price of $20 000 before he could inspect the boat. The consumer was told he would get his money back if he did not like the boat or changed his mind about buying it.

With that assurance, the consumer followed the seller's instructions and paid in advance by way of international wire transfer rather than through the auction website's secure payment facilities.

When it came time to inspect the boat the consumer could not contact the seller. He never received the boat and lost his $20 000 to the scammer.

Banking and online account scams (including phishing)

Number of scam reports in 2011: 5430

Per cent of total scams reported in 2011: 6.5

Number of consumers reporting losses: 253

Total losses reported by consumers: $1 299 869

Scam conversion rate: 4.7 per cent

Banking and online account or phishing scams trick victims into providing their personal and banking information so the scammers can steal their money or identity.

Scammers send emails that appear to be from legitimate businesses such as banks, financial institutions, online payment services or telecommunications service providers, asking victims to provide account details (including usernames, unique user numbers and passwords). In 2011 phishing scammers also sent emails pretending to be from social networking websites, postal and logistics services.

This type of scam continued to use visual tricks to convince victims that the request was genuine, such as copying bank logos and email signatures. Phishing emails also commonly provided links to fake websites displaying convincing copies of genuine account login pages.

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

From the SCAMwatch radar: New twist on bank account phishing scam

In late 2011, SCAMwatch received reports of a sophisticated twist to standard online bank account phishing scams.

Some internet banking systems send authentication messages to their account holder's mobile phone before they are able to make a transaction with a new party. In 2011 scammers developed techniques to tap into these authentication messages by sending a phishing email to gather the victim's mobile number, internet banking password and username.

The scammer used these details to both access the victim's online banking accounts and transfer their mobile number to a scam mobile phone. The scammer then used the scam phone to receive the victim's bank authentication messages and perpetrate fraudulent internet banking transactions.

Often the victim would not know they had been scammed until their mobile phone was unexpectedly disconnected by their provider.

Read more on the SCAMwatch radar: www.scamwatch.gov.au.

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

Number of scam reports in 2011: 2754

Per cent of total scams reported in 2011: 3.3

Number of consumers reporting losses: 412

Total losses reported by consumers: $615 071

Scam conversion rate: 15 per cent

The ACCC received a slight increase in the number of false billing scam reports in 2011, but a reduction in the total losses reported. In 2010 small businesses reported losses of almost $1 million compared to just over $600 000 in 2011.

This type of scam targets small businesses to trick them into paying for unwanted or unauthorised listings or advertisements in magazines, journals, business registers or directories. Common scam tactics are to send a business a subscription form disguised as an outstanding invoice to get the business to sign up for unwanted ongoing advertising services. Scammers also falsely claim that the directory or publication is well-known or has a high readership.

These scams were discussed during the Australasian Consumer Fraud Taskforce forum—*Small business and scams: sorting out the shams*—in September 2011. More details are in Section 5.1.

In 2011 the ACCC also finalised court action against traders targeting small business operators with scam-like conduct, such as to sign businesses up to directory services or to demand payment for unsolicited advertisements. More details are in Section 4.2.

Victim story: Small business pays for advertising they never authorised

In 2011 one small business lost almost $12 000 to a scammer for advertising they never authorised.

The scammer made repeated calls to the victim over several months, claiming that the victim had agreed to ongoing advertising and requesting payment for outstanding invoices.

The accounts staff of this small business paid the invoices each time thinking the agreement for the advertising was legitimate.

Job and employment scams (including business opportunity)

Number of scam reports in 2011: 2505

Per cent of total scams reported in 2011: 3

Number of consumers reporting losses: 368

Total losses reported by consumers: $7 342 643

Scam conversion rate: 14.7 per cent

Job and employment scams can involve offers to work from home or to set up and/or invest in a business.

Scammers promise a high salary or a high investment return following initial up-front payments. Payments can be for training courses, uniforms, security clearances, taxes or fees.

This type of scam is sometimes used to launder money, for example a victim is paid to receive money into their bank account and then transfer it to another location or account.

Victim story: Scammer gives a little back to encourage more payments

A consumer contacted SCAMwatch worried that his wife had fallen victim to a work-from-home scam. His wife had been in contact with a supposedly legitimate work-from-home employment scheme that charged her several payments totalling almost $22 000 to set up a website. They claimed that the website could be used to generate financial returns.

The scammer sent the victim a cheque for $29.18 and credited almost $2500 of the victim's own money back to her. However, the victim's husband believed this was a tactic to encourage his wife to continue participating in the scam. The husband reported that the scammer was constantly calling asking for more money so the couple decided to stop all contact and payments.

Computer prediction software scams (including betting)

Number of scam reports in 2011: 646

Per cent of total scams reported in 2011: 0.8

Number of consumers reporting losses: 291

Total losses reported by consumers: $4 712 528

Scam conversion rate: 45 per cent

In computer prediction software scams, scammers promote software packages or memberships for betting schemes with promised returns. Consumers are asked to pay large sums of money up-front to purchase the membership or software. They may also have to pay ongoing fees and bets.

Returns are promised over timeframes that can sometimes be up to 10 years. Victims may therefore continue to make payments for years before realising they are involved in a scam. As this is a gambling scam, victims may not initially be concerned by losses; however continual underperformance and failure to meet promised returns may alert them to the scam.

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

- sports-betting packages that claim to predict the outcome of races or games
- investment software that claims to predict stock market movements and promises big returns
- lottery prediction software that claims to guarantee winning lotto numbers.

Victim story: Computer betting software upgrade sham

A consumer received a cold call from a scammer and was offered betting software for a payment of $2000. She accepted the offer but lost the money and lost contact with the scam company. Some months later she was re-contacted and encouraged to invest in an upgraded, 'new and improved' betting package.

The victim invested another $27 500 but again did not receive the promised returns.

She was contacted a third time by the scammer, guaranteeing they could get all of her money back in return for a final payment of $5500. The victim paid this amount but did not receive anything from the scammer. The victim subsequently received a call claiming the original company had gone into receivership and that a new company had bought it out.

The new company offered the victim similar services to retrieve her previous losses. The victim did not take up the offer recognising that this was yet another scam.

Investment and real estate scams

Whilst the investment and real estate scams category was not in the top 10 scams reported to the ACCC in 2011, it recorded the third highest total losses due to the emergence of serious and organised investment fraud schemes. In these schemes the victim is promised hefty returns on investments, for example in international companies. These types of scams are sometimes initiated through seminars but more often through unsolicited telephone calls, emails and letters.

2.4 Understanding the victim experience—Australian Institute of Criminology research report

As detailed in Section 2.3, for the third consecutive year advance fee fraud[1] (AFF) was the most commonly reported scam to the ACCC. From 2009 to 2011 this type of scam contributed to more than 35 per cent of those reported. AFF scams can involve a broad range of tactics and approaches. The end goal is always to convince the victim to part with their money and/or personal details in advance, following a promise they will later receive substantial benefit or financial return.

In 2011 the Australian Institute of Criminology (AIC) released a research report[2] based on responses from a sample of AFF victims who had sent money to scammers in Nigeria. The research aimed to better understand how victim behaviours and personal circumstances might have contributed to their response to a scam invite and subsequent loss of money or personal details.

The AIC report exposed some mechanics of AFF scams including the interactions between victim and scammer over the life of the scam. These mechanics go beyond traditional research which commonly analyses victim demographics.

Research results—a profile of advance fee fraud from the victim's perspective

Initial contact with the scammer

Eighty-five per cent of victims in the sample said they were initially contacted by the AFF scammer over the internet, most commonly by email or through dating websites or social networking services.

Motivations for response

The research analysed victim motivation for sending money overseas to scammers. Victims responded that they wanted to make extra money, obtain something they were entitled to receive or take advantage of a unique offer. Victims of dating and charity scams identified wanting to help out someone seeking their assistance or support their relationship with the scammer.

Ongoing contact with the scammer

One third of victims said they had been in contact with their scammer more than 20 times. Three dating scam victims had been in contact with their scammer more than 200 times. Nearly 30 per cent of victims said they were still in contact with the scammer when responding to the survey.

Verifying the scammer's identity

Results showed that 30 per cent of victims had undertaken some research to verify who they were dealing with during the scam. Around 40 per cent had been provided with some verification of the scammer's identity, such as bank records or passports, although these documents—while initially convincing—ended up being counterfeit. More than 40 per cent of victims had attempted to meet the scammer with four travelling overseas to do so.

Introduction to new scammers

AFF scammers often introduce a new person to the victim in an attempt to authenticate their story. This new person is either the same scammer or another one posing, for example, as a bank manager, doctor or, in the case of dating scams, a relative such as a mother. This tactic was used on roughly 40 per cent of the research sample.

---

1 Advance fee fraud falls under the Mass Marketed Advance Fee Fraud scam category and is defined by the ACCC as any scam that involves a scammer requesting fees up-front in return for goods, services or rewards that they never supply.

2 S Ross & RG Smith, 'Trends and issues in crime and criminal justice, no. 420: Risk factors for advance fee fraud victimisation', Australian Institute of Criminology, August 2011.
Viewed at: *www.aic.gov.au/publications/current%20series/tandi/401-420/tandi420.aspx* (20 February 2012).

Financial losses

Approximately three quarters of victims had sent money to offenders more than once and more than 40 per cent had sent money five or more times. Losses ranged from $100 to $120 000. More than half the victims were in contact more than five times with the scammer before sending money. One in six had 20 or more contacts before sending money. For 80 per cent of victims the money sent came out of their personal savings, although some took out loans, borrowed from family or friends or mortgaged their property.

Non-financial losses

Many victims experienced trauma or hardship, primarily financial hardship (54 per cent), emotional trauma (43 per cent) or loss of confidence in other people (40 per cent) as a result of the scam. Others also expressed marital or relationship problems (12 per cent) as a result of their victimisation.

Lifestyle circumstances

Victims reported a number of negative life circumstances, including 40 per cent experiencing depression in the last five years (either related or un-related to the scam), 45 per cent suffering financial crisis and 22 per cent suffering a serious illness.

Reporting the scam

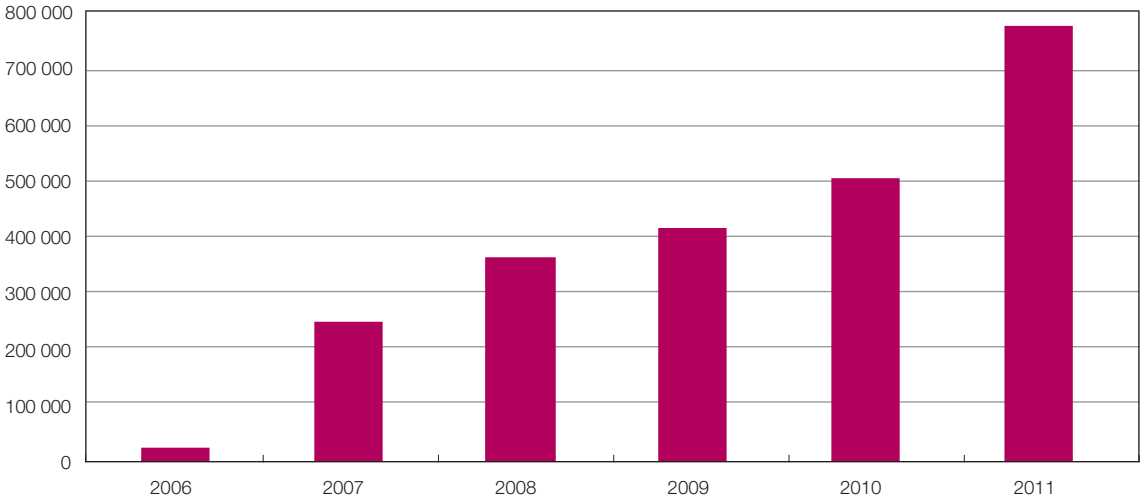
A common element of AFF is for the scammer to convince the victim to keep their arrangement secret, claiming that not doing so would jeopardise the promised benefit. The reality is that the scammer does not want concerned family members or friends interfering with the victim's willingness to continue to pay. Results showed that 75 per cent of victims did not discuss the matter with anyone before sending money to the scammer and 20 per cent had still not told anyone at the time of the survey. While 25 per cent of victims had reported the scam to their bank or financial institution, 75 per cent had not reported it to their state or territory police force, or the Australian Federal Police. Common reasons included embarrassment, the belief that authorities would not be able to find the scammer or the belief there was insufficient evidence to proceed against the scammer.

3 Awareness raising and education initiatives

3.1 SCAMwatch website—www.scamwatch.gov.au

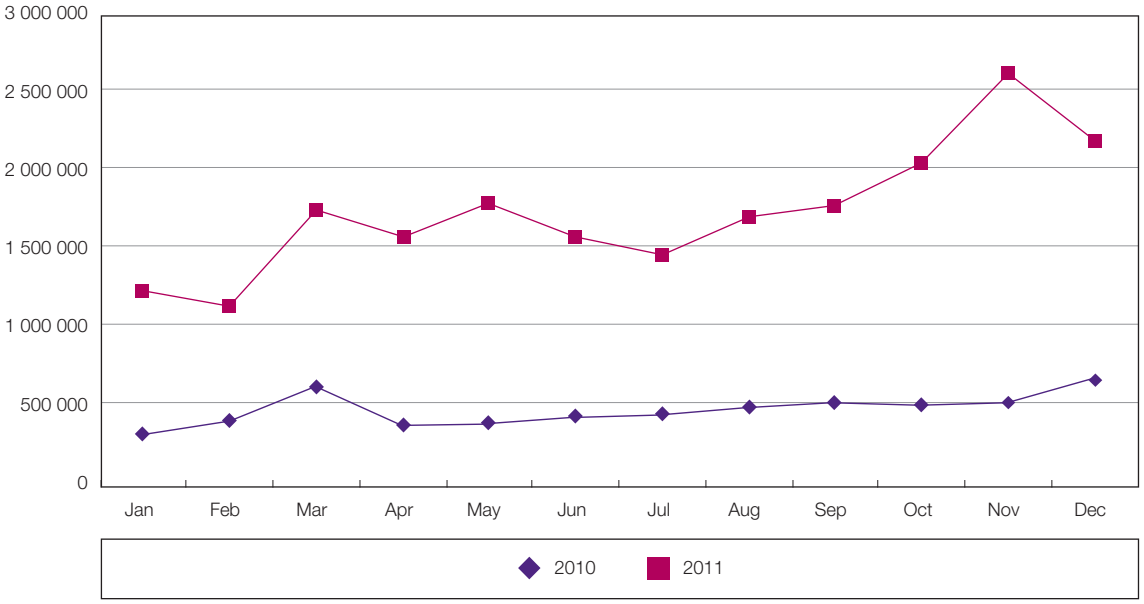
The ACCC's SCAMwatch website (www.scamwatch.gov.au) provides information to consumers and small businesses about how to recognise, avoid and report scams. In 2011 the website had more than 20.5 million hits, a substantial increase of roughly 15 million more hits than received in 2010 (an almost 400 per cent increase). On average in 2011 the site received almost two million hits a month compared to less than 450 000 a month in 2010. In 2011 the site also received 774 989 unique visitors, approximately 275 000 more than in 2010.

Figure 4: Unique visitors to the SCAMwatch website from 2006 to 2011



For the third year in a row, March saw a surge in the number of hits and visitors to SCAMwatch, largely attributed to increased public awareness generated by the annual Australasian Consumer Fraud Taskforce National Consumer Fraud Week. In 2011 hits and visitors to the site also surged between August and November, possibly due to the high activity and rapidly increasing number of followers and retweets on the SCAMwatch Twitter account, which links back to the SCAMwatch website. These trends are shown in Figure 5.

Figure 5: Comparison of hits to the SCAMwatch website in 2010 and 2011



As well as providing generic content about each commonly reported scam category, the SCAMwatch website also posts radar alerts about emerging scams and changes in common scam conduct. In 2011 SCAMwatch issued 28 alerts, warning consumers about the imminent risk of scams around current events such as the Queensland floods, the Japan earthquake disaster, the introduction of the carbon price, the lead up to the London 2012 Olympics and Paralympics, and holidays such as Christmas.

Radars show that scammers try to target victims in all facets of their life, whether booking flights or accommodation, buying birth, death or marriage certificates, organising delivery of parcels, disposing of old computers, using social networking websites, buying and installing solar panels or shopping online. A full list of 2011 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 private businesses wishing to warn customers of scammers masquerading using their brands and logos.

Each time a radar alert is published on the website, the ACCC also sends it to subscribers by email. In the five years since the SCAMwatch email alert service was established it has gained 18 666 subscribers, almost 5000 of those joining in 2011.

In addition to publishing information about scams and how to avoid them, SCAMwatch operates as a portal for the Australasian Consumer Fraud Taskforce (ACFT). It promotes ACFT initiatives, campaigns and the Taskforce's annual National Consumer Fraud Week campaign. More information about the ACFT is in Section 5.1.

In Australia, the Australian Government, state and territory government departments, police forces, the media, consumer groups and private companies continue to direct their website users to SCAMwatch. Internationally, SCAMwatch is considered a best practice resource. A number of agencies in countries such as Canada, New Zealand and the United Kingdom refer consumers to the website.

In 2011 users of social media services such as Twitter and Facebook also increasingly directed friends and followers to SCAMwatch when scams were mentioned in online conversations. This contributed to growing brand awareness and visits to the site.

3.2 SCAMwatch joins Twitter

Twitter is a website enabling users to post and read short messages called tweets which are listed on a user's profile page. Members of the public, businesses and government departments use Twitter to communicate and collaborate.

On 7 March 2011 the ACCC launched its SCAMwatch Twitter page (http://twitter.com/SCAMwatch_gov). The page proved extremely popular, gaining 2636 followers in less than 10 months. In 2011 it raised awareness about many emerging scams and @SCAMwatch_gov was involved in interesting scam-related conversations with followers. Detailed advice and links were provided in all @SCAMwatch_gov tweets and other twitter users retweeted these on their own Twitter pages.

During 2011 @SCAMwatch_gov posted 1341 tweets about scams targeting Australian consumers and business, including:

- alerts warning of new and emerging scams
- alerts about ongoing scams with high conversion rates and which cause significant loss
- warnings about the potential for scammers to strike following significant events
- information exposing the tactics scammers use to lure victims
- tips to outsmart scammers and protect identity, money, family and friends
- information on the best way to report a scam
- tips on what to do after being scammed
- occasional statistics on scam complaints received by the ACCC.

The SCAMwatch Twitter account also answers questions posed by other Twitter users about specific scam conduct and directs users to other government services when appropriate. In 2011 the account was also used to retweet and promote consumer protection initiatives by other government departments.

Twitter allows SCAMwatch to reach consumers, businesses and the media in real time, as scams emerge. It can be followed at: http://twitter.com/SCAMwatch_gov or @SCAMwatch_gov.

3.3 Printed materials

The ACCC has a suite of scams-related publications which complement the information provided on the SCAMwatch website. In 2011 the ACCC distributed more than 77 000 copies of these publications.

The most popular was *The Little Black Book of Scams*. In 2011 more than 70 000 copies of this free booklet were distributed to consumers and businesses.

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

The ACCC has five scam-specific fact sheets that cover lotteries, sweepstakes and competition scams, money transfer scams, phishing scams, sports investment scams and small business scams.

Appendix 2 gives a detailed list of the ACCC's scam-related resources for consumers and businesses.

3.4 Media and communications activity

The ACCC uses media platforms and communication opportunities to raise awareness of scams to the widest possible audience.

In addition to issuing regular media releases, the ACCC also uses the media to publicise enforcement outcomes. The ACCC actively seeks and accepts opportunities to give media interviews, community and business presentations and speeches to increase knowledge of scams and promote awareness of its role in scam prevention and education. Major and local newspapers, radio stations and television programs across the country also run articles and segments 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 alert consumers and small businesses to the presence of scams.

Appendix 3 highlights the ACCC's key scam-related media and communications activities in 2011.

3.5 National education and engagement activities

During 2011 the ACCC's Education and Engagement Managers, located in every state, participated in activities with business intermediaries and professional associations. Activities were conducted to raise awareness and spread ACCC scams messages widely to groups that may be vulnerable to scams, including small businesses, senior citizens and local communities.

Meetings were held and presentations given to key local government economic development units in New South Wales, to professional associations such as the Institute of Public Accountants and to the Victorian Commercial Teachers' Association.

The Education and Engagement Managers also raised awareness of scams by working with other government agencies during National Law Week expos held in Sydney, and presented to the National Seniors Association, the South West Seniors Expo and jointly with Consumer Affairs in South Australia for the Hawthorn Senior Citizens.

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

Small business

In recent years the ACCC has observed that small businesses are most commonly targeted with false billing scams including:

- Directory entry or unauthorised advertising scams involving the scammer sending unsolicited invoices for marketing that does not exist or is of dubious quality.
- Office supply scams involving businesses receiving and being charged for goods they did not order such as paper, printing supplies or maintenance supplies.
- Domain name renewal scams involving a business being sent an invoice for a domain name that is similar to the business' current domain name or a document that looks like an official renewal notice from their current provider.
- Trade mark invoice scams involving a business being sent a scam invoice for the renewal of a trade mark, whether they own the trade mark or not. Any business responding is expected to pay costly fees and may be registered in an online trade mark directory or unknowingly engage a broker.

Scammers may set up websites that falsely convince businesses that they can directly provide government services and registrations, such as Australian Business Name registrations or grant applications. These sites charge large amounts for services which are provided at a much lower cost or free by legitimate government agencies.

The ACCC regularly engages with small businesses to raise awareness of the types of scams that target them. A key event in 2011 was the Australasian Consumer Fraud Taskforce forum—*Small business and scams: sorting out the shams*—held on 12 September in Canberra. Leading experts, including academics and businesses, provided insight into small business scams including how and why they target this sector. More information on the forum is in Section 5.1.

The ACCC provides small businesses with information on relevant enforcement action and scam-like conduct through its Small Business Information Network (SBIN). The network comprises more than 1100 small businesses and small business stakeholders, including industry associations, local government and business enterprise centres.

Eleven SBIN emails containing information and alerts on scams were sent out in 2011. These warned businesses to beware of misleading workplace safety claims, online directory scams and end of financial year scams.

The ACCC also has publications to help small businesses protect themselves against scams. In 2011 the ACCC published updated specific publications for small business to reflect the newly introduced Australian Consumer Law. One such publication is *Misleading job and business opportunity adverts: how to handle them*.

The ACCC's 2011 enforcement activity in the area of scams also had a direct impact on scammers targeting small businesses. Chapter 4.2 has more details.

4 Action to disrupt scams and enforce the law

This chapter outlines action taken by the ACCC to enforce the law against scammers and 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 agencies and private entities to protect consumers and small businesses from scams, disrupting and limiting the harm they cause when enforcement action is inappropriate or unavailable. The ACCC carefully analyses offers to determine if they are legitimate or a possible scam. Wherever possible the ACCC communicates 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 prevent the harm they may otherwise cause, often without having identified or located the scammer.

In 2011 the ACCC continued to work with external government and non-government parties who provided information that on closer analysis confirmed various activities as scams. One such example was the ACCC's continued work with international email service providers to develop ways to better identify scam emails and reduce the harm they cause.

The case studies below highlight two of the ACCC's 2011 collaborative activities to disrupt scams.

Case study—Queensland and Victorian flood scams

In January 2011 the ACCC, in collaboration with state and territory consumer protection agencies and law enforcement bodies, carried out an extensive, pre-emptive public awareness raising campaign to protect Australians from scammers taking advantage of the Queensland and Victorian floods.

A set of national crisis fact sheets were developed to address consumer protection issues arising from the floods, including material specific to charity scams. Consumer warnings were released, as was a SCAMwatch radar alert warning consumers of scammers masquerading as legitimate charities in times of natural disaster.

This cooperative effort achieved media saturation and may have been a strong contributing factor to the low level of scam-related contacts which the ACCC received relating to the floods.

In January the ACCC also scrutinised a number of websites operating in the Australian domain name space. This was done to pre-empt significant financial loss resulting from online scam activity related to the Queensland floods. Through its liaison with auDomain Administration Ltd, the ACCC identified a number of domain names that warranted investigation.

While no serious scam activity was detected, the investigation highlighted that some website operators were collecting money unaware of the registration requirements for doing so as a charity. ACCC staff liaised with the appropriate state agencies to have this issue addressed.

Case study—Dating and romance scams project

In light of increasing reports to the ACCC of dating and romance scams in recent years, the ACCC began working with operators of dating websites to address scams targeting their users.

On 4 July 2011 the ACCC held a roundtable meeting with a number of dating website operators, including those with major dating websites based in Australia, to discuss measures to improve their response to online dating and romance scams.

Industry response was positive and website operators provided information on the measures they had already implemented to protect their users from scams. Following the meeting, a working group of nine dating websites and the ACCC was formed to develop best practice guidelines for dating websites. On 30 November 2011 the ACCC distributed the draft guidelines to the broader dating website industry for review and comment.

Finalised guidelines were released on 14 February 2012 to coincide with Valentine's Day. The guidelines are intended to bolster existing measures used by dating websites to counter scam activities and provide guidance to industry on how to better protect users from scams.

While the guidelines are voluntary, the ACCC considers that they represent best practice and encourages all dating websites used by Australian consumers to adopt them, both those based in Australia and overseas.

4.2 Scam-related enforcement activities

In 2011 the ACCC initiated proceedings or concluded action against a number of traders allegedly involved in misleading and deceptive or scam-like conduct. In particular two court actions were finalised against traders targeting small business operators with scam-like conduct to sign them up to directory services or to demand payment for unsolicited advertisements. While perpetrators of this type of conduct are often based overseas, the ACCC has instituted proceedings against a number of identified traders in recent years.

Two enforcement case studies from 2011 are listed below.

Case study—Yellow Page Marketing BV and Yellow Publishing Limited

Following ACCC court action, in April 2011 the Federal Court of Australia imposed penalties totalling $2.7 million against two overseas companies, Yellow Page Marketing BV and Yellow Publishing Limited, for sending thousands of Australian businesses misleading faxes and invoices.

Communications falsely led businesses to believe they were dealing with Sensis Pty Ltd Yellow Pages® and attempted to encourage them to subscribe and pay for listings in their online business directories.

The faxes and invoices contained prominent banners including the words 'Yellow Page' and an inverted walking fingers logo. Businesses that did not pay the invoices were threatened with late fees.

The court orders marked the Court's disapproval of the conduct (which involved no human contact) and declared such online directory contracts void, meaning businesses affected by the scam could ignore demands for payment and stop making payments to the companies. Justice Gordon remarked that the court orders would serve as a warning to the public to be wary about signing up to anything looking like a 'free offer'.

The ACCC was also able to return a number of cheques to businesses as they had been subpoenaed from the Commissioner of Police of Western Australia.

Case study—European City Guide trading as Industry and Commerce

In July 2011 the Federal Court of Australia found that the Spanish-based company, European City Guide S L, trading in Australia as Industry and Commerce, misled Australian small businesses into signing up with its online business directory.

The Court declared that between 2006 and 2009 Industry and Commerce wrote to Australian businesses asking them to update or check that the information on the Register of Business Information was 'positively and correctly presented'.

The forms sent by Industry and Commerce falsely represented that the Register of Business Information was a record of the Australian Government and, for some of that time, represented that the register would be free to update, when this was not the case.

Businesses that completed the forms were pursued by Industry and Commerce for fees of between $1200 and $1600 a year for a minimum of three years. Businesses that tried to cancel the service, which amounted to a listing on an Industry and Commerce website, were threatened with debt collection and legal action.

In his judgment, Justice Moore said: "A charitable person would describe [European City Guide]'s conduct as an opportunistic exploitation of consumers. A less charitable person would probably use more robust language".

5 Domestic and international collaboration

As scams commonly operate in a global environment, national and international cooperation is an essential part of effective prevention. Some partnerships and activities the ACCC participated in during 2011 are outlined in this chapter.

5.1 The Australasian Consumer Fraud Taskforce

About the Australasian Consumer Fraud Taskforce

The Australasian Consumer Fraud Taskforce, established in 2005, comprises 22 federal and state government regulatory agencies and departments (including New Zealand) that have a responsibility for consumer protection in relation to fraudulent and scams activity.

The Taskforce's primary functions are to:

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

The ACCC's Deputy Chair, Dr Michael Schaper, is the Chair of the Taskforce. The ACCC also assumes the secretariat role.

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

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

National Consumer Fraud Week

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

2011 campaign—Scams: It's Personal

The 2011 Fraud Week campaign, *Scams: It's Personal*, ran from 7 to 13 March and explored the personal side and impact of scams—not only on individuals, but businesses, community, government and society more broadly. The theme was chosen to highlight the high cost of consumer fraud both financially and non-financially, and the emerging trend of personalised scams.

Scams: It's Personal was supported by a busy program comprising initiatives by members and partners. Two important reports were launched: *Targeting scams—Report of the ACCC on scam activity 2010*, highlighting key trends in scams activity; and the Australian Institute of Criminology's *Consumer fraud in Australasia*, reporting on the results of the Taskforce's 2008 and 2009 surveys.

Several important events were held throughout the week, including:

- *Supporting Victims of Scams* forum—Australia's first ever event exploring this issue
- *You, Me and Scams* event—bringing together Taskforce members and partners to discuss scams
- *Consumer fraud campaigns: panacea or fig leaf?* seminar—exploring the effectiveness of campaigns.

International guest speaker Mike Haley of the United Kingdom's National Fraud Authority presented throughout Australia and provided invaluable insight into his country's response to scams.

The campaign received strong support from the Parliamentary Secretary to the Treasurer, David Bradbury MP, and the Minister for Home Affairs and Justice, the Hon. Brendan O'Connor, MP.

The campaign also generated significant media interest with all major metropolitan newspapers and radio stations, and several major television programs, running stories on scams. Overall, coverage was considerably higher than it was for previous campaigns.

A coordinated approach to using social media generated more than 200 tweets, reaching a combined Twitter community of 27 000 followers.

In 2011 the Partners Program added 30 new partners, expanding to a total of more than 100. The Taskforce's new 'Principal Partners' approach saw 17 companies and/or organisations join up and contribute to the campaign with some important initiatives including scams awareness videos, free advertising, permanent online material and media.

With a busy program, widespread media coverage, and strong support from the community, ministers and partners, *Scams: It's Personal* was a highly successful campaign.

Other key Australasian Consumer Fraud Taskforce activities 2011

Examples of key initiatives undertaken by ACFT members in 2011 are discussed below.

Australasian Consumer Fraud Taskforce 2011 online survey

Since 2006 the AIC, on behalf of the Taskforce, has conducted an annual online survey to assess the consumer fraud experiences of participants. This annual survey is hosted on the AIC's website (http://www.aic.gov.au/crime_community/surveys/acft.aspx) and consumers can self-select to participate in the survey when they visit the site.

Between 1 January and 31 March 2011, 1153 people responded to the survey, creating a useable sample of 1145 Australian and New Zealand responses. The number of respondents in 2011 was more than four times that of 2010.

The 2011 survey results showed that scam invitations are common throughout the community, with 1078 (94 per cent) of survey respondents indicating that they had received a scam invitation in the 12 months prior to the survey. However, because the sample of respondents was self-selected it is likely that those who have been victimised would be more likely to participate in the survey.

Some substantial scam losses were reported in 2011. Of the 289 respondents who advised they had responded to a scam, 125 sent money and 164 personal information. Survey results also demonstrated that consumers did not always require much contact from scammers before responding, with 79 respondents indicating they sent money or personal information after only one contact.

The survey highlighted the need for continued consumer education on scams and how to identify scam approaches. This is reflected in the changing nature of scams and the adaptability of scammers. Results demonstrated that scam techniques and delivery are adapting. For example there was an increase in the use of telephones, mobiles and text messaging as methods for scam delivery. The computer remote access scam delivered by telephone (explained in more detail in Section 2.3) led numerous survey respondents to become victims.

Australasian Consumer Fraud Taskforce 'Small business and scams' forum

On Monday 12 September 2011 more than 70 businesses, industry association and government representatives attended the joint Taskforce and Council of Small Businesses of Australia forum—*Small business and scams: sorting out the shams*.

Academics, compliance and enforcement experts, as well as small business specialists, shed light on their experiences with scams, the sophisticated techniques employed by scammers to target small business and how to disrupt the techniques.

The forum highlighted underreporting of small businesses affected by scams and the difficulties faced by law enforcement agencies in gauging the level of financial and non-financial impact on this sector. It proved to be an important event in bringing together public and private sectors to talk about scams, with presentations leading to lively discussion among participants.

National Cyber Security Awareness Week

From 30 May to 3 June 2011 the Department of Broadband, Communications and the Digital Economy held its annual National Cyber Security Awareness Week. This campaign aims to educate home and small business users on the simple steps they can take to protect their personal and financial information online.

In 2011 more than 500 industry, community and consumer organisations, and government agencies, partnered to deliver events and activities in metropolitan, regional and rural Australia. During the campaign, a new version of the Budd:e cybersecurity education package was launched. This interactive website helps primary and secondary school students adopt secure online practices and behaviours in a fun way.

The department conducted a second campaign in the lead up to Christmas 2011 promoting secure online shopping practices and warning of malware-infected Christmas e-cards.

2012 campaign—Slam Scams!

The ACFT's 2012 Fraud Week campaign will run from Monday 19 to Sunday 25 March and will focus on scam delivery methods. The *Slam Scams!* campaign will aim to raise awareness of scam delivery methods so Australians can identify a scam at the point of contact and avoid becoming victims. A phone call, SMS, mobile app, house visit, letter, email, fax, blog, online chat or dating service—scammers will use any of these means to target victims.

The primary message is simple: stop the contact at the point of delivery—if you do not engage with a scammer in the first place, you will avoid being scammed.

Appendix 4 includes a list of the 2011 and 2012 ACFT members and partners.

5.2 The International Consumer Protection and Enforcement Network

The ICPEN comprises consumer protection authorities from almost 40 countries. It is a network through which authorities can cooperatively share information and look at combating consumer problems arising with cross-border transactions in goods and services, such as e-commerce fraud and international scams.

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

The network's annual conference was held in The Netherlands in April 2011. Key focus areas included:

- affiliate marketing
- deceptive health claims
- misleading advertising in telecoms
- deceptive advertising in travel and tourism.

The ICPEN website (www.icpen.org) provides consumers with tips on where to look for help and how to lodge a complaint in cross-border disputes.

Key ICPEN activities 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 National Consumer Fraud Week campaign with the ACFT (more information is in Section 5.1).

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 complaints about online and related transactions with foreign companies. The site was developed in 2001 as a response to the challenges of multinational internet fraud. It is available in seven languages. The portal also provides consumers with tips on how they may be able to resolve issues and provides contacts for alternative dispute resolution services in ICPEN member jurisdictions, including Australia.

Annual International Internet Sweep Day

The ICPEN Annual International Internet Sweep Day is a global web-surfing exercise designed 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.

Annual International Internet Sweep Day—Australia

In 2011 Australia's Sweep Day was held on 6 September. The theme was *The Use (and misuse) of Third Party Authority*—targeting unauthorised online use of third party authorisations.

The ACCC focused on websites that falsely represented government endorsement or affiliation in the areas of government programs or services, carbon pricing and green claims, immigration, taxation, education, sport, nutrition and community services. Of particular concern were websites charging for services that can be obtained free or at a relatively low cost from genuine government websites.

As in previous years, the ACCC was joined by state and territory consumer protection agencies across the country as well as a number of Australian Government agencies.

Media coverage included reports broadcast on metropolitan and regional radio, national television news and articles in print and online media.

The ACCC 'swept' approximately 1300 websites and identified around 250 sites for final analysis. Problematic online conduct included:

- 'brokers' touting for services that are provided free or at low cost through government websites without making it clear they are not the official provider
- misrepresentations on eligibility for government grants—suppliers of directories suggesting that using the service will be an advantage as well as drawing attention away from free government directory websites
- misrepresentations on immigration services—inbound and outbound—suggesting that using the service will guarantee a positive result.

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

5.3 International Mass Marketing Fraud Working Group

Since February 2008 the ACCC has participated in the International Mass Marketing Fraud Working Group, which comprises domestic and international law enforcement agencies.[3] Participation assists the ACCC to combat cross-border mass-marketed fraud by:

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

3 Members of this group include the United States Federal Trade Commission, United States Department of Justice, United States Postal Inspection Service, United States Federal Bureau of Investigation, 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 The Cyber White Paper

The Australian Government has announced it will release a Cyber White Paper in the first half of 2012 to outline how government, industry and the community could work together to address the challenges and risks Australians will face from increased engagement in the digital economy. The ACCC is working with the Department of Prime Minister and Cabinet and other relevant parties in developing the paper.

5.5 Investment Scams Task Force

In 2011 the Australian Crime Commission Board established Task Force Galilee, a multi-agency task force focused on preventing and disrupting serious and organised fraudulent investment scams.

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

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

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

Led by the Australian Crime Commission, the task force comprises law enforcement, regulatory and service delivery agencies across federal, state and territory governments including the ACCC, all Australian Crime Commission Board agencies, the Department of Broadband, Communications and the Digital Economy, the Department of Immigration and Citizenship, the Department of Human Services and the Australian Transaction Reports and Analysis Centre.

5.6 Australian Transaction Reports and Analysis Centre partnership

Since 2006 the ACCC has been a partner agency of the Australian Transaction Reports and Analysis Centre (AUSTRAC) as authorised under the *Anti-Money Laundering and Counter-Terrorism Financing Act (Cwlth) 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 $10 000.

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

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

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

6 Conclusions and challenges for 2012

In 2011 the ACCC observed a number of significant changes in the scam landscape. Consumer reports to the ACCC revealed a resurgence in scammers approaching victims by telephone. Until recent years telephone was considered an old style of scam delivery, but scammers' abuse of recent advancements in VoIP technology contributed in part to this shift.

Losses increased for the third consecutive year. This was partially due to the prevalence of 'high volume scams' which saw large numbers of victims targeted concurrently, with requests for smaller sums of money, often below $500.

Despite these challenges, the ACCC continued its work to educate and protect consumers and small businesses from scams. New initiatives in 2011 included the launch of the highly successful SCAMwatch Twitter page, collaborative work with dating websites to address scams targeting their users, scam disruption activities surrounding the Queensland and Victorian floods, delivery of forums and engagement activities for particularly vulnerable consumer segments, and successful court outcomes against a number of overseas traders scamming Australian small businesses.

In 2012 the ACCC, consumer protection agencies and law enforcement will continue to face challenges that new scam approaches and technology pose.

The global nature of scams and the increasing connectivity between citizens from different countries—whether to communicate, shop, make new friends, find romance or invest, among other activities—opens channels and opportunities for unscrupulous people to reach new victims. This is a significant challenge for the ACCC and international consumer protection agencies, and will most likely continue in the foreseeable future.

To address these challenges, in 2012 the ACCC will develop new approaches to combating scam activity and will continue to work collaboratively with private and public entities to counter the prevalence of scams targeting Australians.

Appendix 1: 2011 SCAMwatch radars

Beware fake Australian Government climate change website

December 2011: SCAMwatch is warning Australian consumers to beware of a fake website pretending to be the official Australia Government Department of Climate Change website.

Scam birth, death and marriage certificate websites

November 2011: SCAMwatch is warning Australians to be wary of websites that appear official but fail to deliver on promises to provide birth, death, marriage or divorce certificates in return for a fee.

Classifieds scammers advertise smartphones and tablets online

November 2011: Beware of scam online classifieds ads for smartphones, tablet devices and other small electronic items which are never delivered following payment.

The 12 scams of Christmas

November 2011: SCAMwatch is advising consumers to watch out for this year's 12 scams of Christmas. Scams occur all year round but scammers prey on people's generosity and vulnerabilities at this time of year.

Erase your hard drive before disposing of old computers

November 2011: SCAMwatch is warning Australians to erase their hard drive before parting with old computers and laptops. Simply deleting individual files is not enough to remove personal details, documents and passwords stored on the machine.

Scam callers asking for payment to deliver parcels

November 2011: SCAMwatch and Australia Post are warning of scam callers pretending to be from Australia Post and requesting payment to redeliver an undelivered parcel.

Beware of scam gift voucher & product offers on social networking sites

November 2011: SCAMwatch is warning social networking users to beware of scam posts which offer fake gift vouchers or products for free. The vouchers are offered in exchange for personal details and passing on a scam link to friends.

Avoid 2012 London Olympics accommodation scams

November 2011: SCAMwatch is joining the UK Metropolitan Police Service in warning of online accommodation booking scams in the lead up to the London 2012 Olympics and Paralympics.

Protect your credit card details from lottery scammers

October 2011: SCAMwatch is advising Australians to ignore recent lottery scam letters requesting $25, credit card details, or payment by cheque in return for a false $15 000 windfall.

Phishing scam emails and SMS continue

October 2011: SCAMwatch is warning Australians to continue to be wary of phishing scams received by email or SMS following a twist which leads to fraudulent online banking transactions.

Continue to beware of scam solar offers

September 2011: SCAMwatch is warning Australians to continue to be wary of scammers who offer bogus government rebates for the installation of solar panels.

Beware of scam websites making fake claims of government affiliation

September 2011: SCAMwatch is warning small businesses and consumers to be on the look out for scam websites that either falsely claim to be affiliated with government or boast bogus government endorsements.

New round of scam scratchie cards in the mail

August 2011: SCAMwatch and Carnival Australia are warning Australians to beware of a new spate of scam scratchie cards and travel brochures sent in the mail. Every package contains a 'winning' card but when you try to claim the fake prize you will be asked to wire transfer thousands.

Computer remote access scammers now masquerading as Telstra—new twist

August 2011: SCAMwatch has received reports of a new twist on the computer remote access scam with callers now claiming to be from (or affiliated with) Telstra or BigPond.

Beware of scam calls offering carbon compensation payments

July 2011: SCAMwatch is warning Australians to be alert to scam calls offering to pay carbon price compensation into your bank account or asking survey questions about carbon.

Beware of scams targeting VIPtel Mobile customers

June 2011: SCAMwatch is warning current and former VIPtel Mobile customers to beware of scam phone calls offering a refund in exchange for payment of a fee. Scammers may claim to be from Centrelink and will ask for the fee to be paid by wire transfer.

Beware of scam phone surveys which lead to other scam calls

May 2011: SCAMwatch is warning Australians to be alert to scam telephone surveys which gather your personal and banking information and use it to make future scam phone calls you receive appear legitimate.

Fake FBI email scam claims you've visited "illegal websites"

May 2011: Beware of fake Federal Bureau of Investigation (FBI) emails which claim that you've visited illegal websites. These emails are a scam. If you receive one, delete it! Don't open any attachments and don't provide your personal details.

Scammers pose as government & banks offering to reclaim overcharged bank fees

May 2011: Beware of scam callers pretending to be from the Government or a bank and asking for an upfront fee to reclaim your overcharged bank fees.

Make mum's day, not a scammer's!

April 2011: If you're shopping online for a Mother's Day gift be alert! Scammers use online classifieds and auction sites to post scam ads, taking your money but leaving you without that perfect gift for mum!

New twist on computer error message/virus scams: joint warning

March 2011: SCAMwatch, Microsoft and the Australian Communications and Media Authority (ACMA) are warning Australians to continue to be wary of scam calls claiming that your computer is infected with a virus or is sending out error messages.

Avoid charity scams—Japan earthquake disaster

March 2011: SCAMwatch is warning consumers to thoroughly check the legitimacy of charities when donating to Japan disaster relief.

Valentines Day—Don't fall head-over-heels for a scammer

February 2011: If you meet someone special online, be careful: scammers use online dating websites too but they're not genuinely after your love, only your money!

Don't let scalpers spoil your sporting events and festivals

February 2011: SCAMwatch is warning consumers to be vigilant when buying 2011 Rugby World Cup tickets and festival tickets online.

Won a new car in promotion you didn't enter?

January 2011: Could you really be lucky enough to win a new car or money in a promotion or lottery you did not enter? SCAMwatch is warning you not to be fooled.

Donate wisely—Central Queensland flood crisis

January 2011: SCAMwatch is warning consumers to thoroughly check the legitimacy of charities when donating to help flood victims in central and south east Queensland.

Fake SCAMwatch and Consumer Affairs Victoria emails

January 2011: SCAMwatch, the ACCC and CAV are warning consumers to be on the look out for fake emails claiming to be from SCAMwatch and CAV representatives.

Secrets of your DNA revealed?

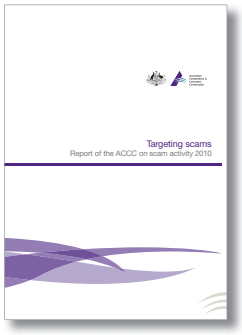
January 2011: A state-of-the art DNA test that will reveal the blueprint of your genetic code and hold all the answers to your health, wealth and personal prosperity? Not likely!

Appendix 2: ACCC scam-related resources for consumers and businesses

Scam reports

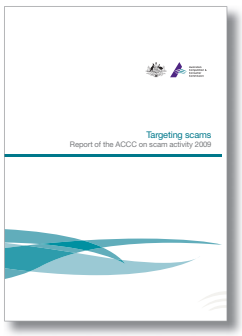
Targeting scams: Report of the ACCC on scam activity 2010

Date published: 6 March 2010



Targeting scams: Report of the ACCC on scam activity 2009

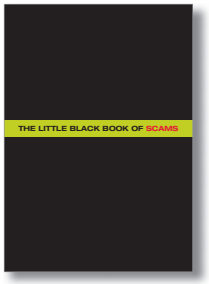
Date published: 1 March 2009



ACCC education resources

The little black book of scams[4]

Date published: 5 October 2011



Small business scams[4] (fact sheet)

Date published: 3 March 2010

Phishing scams[4] (fact sheet)

Date published: 23 October 2008

4 See the publications page at: www.accc.gov.au.

Money transfer scams[4] (fact sheet)

Date published: 23 October 2008

Lotteries, sweepstakes and competition scams[4] (fact sheet)

Date published: 23 October 2008

Sports investment scams[4] (fact sheet)

Date published: 25 June 2009

2011 ACFT National Consumer Fraud Week campaign resources

Postcard

Campaign web button

Campaign web banner

4 See the publications page at: www.accc.gov.au.

Appendix 3: Key ACCC media releases and communications initiatives

2011 ACCC scam media releases

ACCC calls for comment on draft guidelines for dating websites—2 December

ACCC takes court action against publishing companies—26 September

International Internet sweep targets websites with false sponsorships—6 September

Industry and Commerce business directory promotion declared misleading—29 July

Beware of end of financial year scams—30 June

$2.7 million penalty for fake 'Yellow Pages' directory scam—14 April

Beware of websites offering access to government grants—23 March

Scam reports double—National Consumer Fraud Week 7–-13 March Scams: it's personal—6 March

ACCC warns sports fans to be vigilant when buying tickets online—10 February

2011 press articles contributed by the ACCC

Deputy Chairman, Michael Schaper—Statistics show small businesses unaware of being scammed—30 September

2011 ACCC speeches containing scam messages

Executive General Manager, Marcus Bezzi—Australian Skeptics National Convention, Sydney—19 November

Chairman, Rod Sims—ACCC local business event, Darwin—8 November

Deputy Chairman, Michael Schaper—Small Business Open Forum, Richmond Vic—21 September

Deputy Chairman, Peter Kell—Small Business and scams (ACFT), Canberra—12 September

Deputy Chairman, Michael Schaper—Small Business and scams (ACFT), Canberra—12 September

Deputy Chairman, Michael Schaper—Family Business Australia, WA—3 September

Deputy Chairman, Michael Schaper—Small Business Open Forum, Kinglake Vic—23 August

Deputy Chairman, Michael Schaper—Parramatta Business Enterprise Centre—3 May

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

New Zealand Ministry of Consumer Affairs

State and territory governments

Australian Capital Territory Office of Fair Trading

Consumer Affairs Northern Territory

Consumer Affairs Victoria

Fair Trading New South Wales

Queensland Office of Fair Trading

South Australia Office of Consumer and Business Affairs

Tasmanian Office of Consumer Affairs and Fair Trading

Western Australia Department of Commerce

Representatives of the state and territory police

New South Wales Police Service

Queensland Police Service

State and territory Police Commissioners

2011 Taskforce partners

Principal partners

Australian Communications Consumer Action Network

BankWest

CarsGuide

Commonwealth Bank

Consumer Action Law Centre

Facebook

Fairfax Media

Gumtree

Holiday Coast Credit Union

Horseyard.com.au

Microsoft

PayPal

Telstra

The Westpac Group (including Westpac Bank, St.George Bank and BankSA)

Trading Post

Western Union

Yahoo

Partners

Consumer advocacy (general)

CHOICE

Public Interest Advocacy Centre

Legal centres

National Association of Community Legal Centres

Peninsula Community Legal Centres

Financial services

Abacus—Australian Mutuals

Adelaide Bank

ANZ Bank

Australian Bankers' Association

Australian National Audit Office

Bendigo Bank

ComSuper

Financial and Consumer Rights Council

Police Credit Union

Suncorp Metway

Visa

Gaming associations

Australian Casino Association

BetFair

Sportsalive.com

Tabcorp

Ombudsman services

Commonwealth Ombudsman

Energy and Water Ombudsman of NSW

Fair Work Ombudsman

Telecommunications Industry Ombudsman

Social/welfare/community bodies

Alexandra District Hospital

Australian Association of Social Workers

Australian Federation of Disability Organisations

Australian Financial Counselling and Credit Reform Association

Better Hearing Australia Vic Inc.

Brotherhood of St Laurence

Comcare

Country Women's Association of Australia

Cranbourne Information and Support Service

CRS Australia

Departmentof Human Services

Diamond Valley Community Support

Indigenous Consumer Assistance Network

Laverton Community Centre

Mental Health Council of Australia

Neighbourhood Watch

Sane Australia

Social Securities Appeal Tribunal

Western Australia Council of Social Services Inc.

Whittlesea Community Connections

Returned and Services League groups

RSL NSW

RSL SA

RSL TAS

RSL VIC

Aged care services

Australian Seniors Computer Club Association

Council on the Ageing—Australian Capital Territory

Council on the Ageing—Northern Territory

Council on the Ageing—Queensland

Council on the Ageing—South Australia

Council on the Ageing—Tasmania

Council on the Ageing—Western Australia

Seniors Information Victoria

Housing associations

Tenants Union of Victoria

Online and computer bodies

auDA

AusCERT

Australian Computer Society

Community Technology Centres Association

Internet Industry Association

Surete Group

Internet security

Symantec

Telecommunications

Australian Mobile Telco Association

Australian Telecommunications Users Group

Communications Alliance

Optus

Miscellaneous

Ailean

Australia Post

Australian Trade Commission

eBay

Cootamundra Police Station

Crime Stoppers

Migration Review Tribunal and Refugee Review

National Archives of Australia

National Measurement Institute

Office of the Australian Information Commissioner

Victoria Police Service

2012 Taskforce Partners

As at 31 January 2012 the following entities have confirmed their partnership with the Taskforce for 2012.

Principal partners

3H Group Pty Ltd–OasisActive.com

Australian Bankers' Association

Australia Post

Commonwealth Bank

Community Technology Centres Association

Crime Stoppers Australia

Cupid Media Pty Ltd

Department of Attorney General & Justice (NSW)

eBay

Facebook

Giga Pty Ltd–Adult Match Maker

Gumtree

Jet Place Pty Ltd–Redhotpie.com.au

Lucky Tanuki Pty

Microsoft

PayPal

Rural Heartlands Pty Ltd

Slinky Dating Australia Ltd

Telstra

The Westpac Group (including Westpac, St.George, BankSA, Bank of Melbourne, BT)

Trading Post

Partners

Consumer advocacy (general)

CHOICE

Indigenous Consumer Assistance Network

Public Interest Advocacy Centre

Business associations

Chamber of Commerce Northern Territory

Liquor Retailers Australia

Master Builders Australia

Master Grocers Australia

Tasmanian Small Business Council

Legal centres

National Association of Community Legal Centres

Peninsula Community Legal Centres

Financial services

Abacus—Australian Mutuals

Adelaide Bank

ANZ Bank

Australian National Audit Office

Bendigo Bank

ComSuper

Financial and Consumer Rights Council

Financial Counselling Australia

Holiday Coast Credit Union

Police Credit Union

Suncorp Metway

Visa

Western Union

Gaming associations

Australian Casino Association

BetFair

Tabcorp

Government and Ombudsman services

Australian Trade Commission

Commonwealth Ombudsman

Cootamundra Police Station

Energy & Water Ombudsman of NSW

Fair Work Ombudsman

Migration Review Tribunal and Refugee Review

National Measurement Institute

National Archives of Australia

Office of the Australian Information Commissioner

Telecommunications Industry Ombudsman

Victoria Police

Social/welfare/community bodies

Alexandra District Hospital

Australian Association of Social Workers

Australian Federation of Disability Organisations

Better Hearing Australia Vic Inc.

Brotherhood of St Laurence

Comcare

Country Women's Association of Australia

Cranbourne Information & Support Service

CRS Australia

Department of Human Services

Diamond Valley Community Support

Laverton Community Centre

Mental Health Council of Australia

Neighbourhood Watch

Sane Australia

Social Securities Appeal Tribunal

Western Australia Council of Social Services Inc.

Whittlesea Community Connections

Returned and Services League groups

RSL NSW

RSL SA

RSL Tas

RSL Vic

Aged care services

Australian Seniors Computer Club Association

Council on the Ageing—Australian Capital Territory

Council on the Ageing—Northern Territory

Council on the Ageing—Queensland

Council on the Ageing—South Australia

Council on the Ageing—Tasmania

Council on the Ageing—Western Australia

Seniors Information Victoria

Housing associations

Tenants Union of Victoria

Online classifieds, auction and shopping service providers

Eljo

Fairfax Media

Horseyard.com.au

Online service providers and associations

Ailean

auDA

AusCERT

Australian Computer Society

Internet Industry Association

Surete Group

Symantec

Telecommunications

Australian Communications Consumer Action Network

Australian Mobile Telecommunications Association

Communications Alliance

Optus

Academic institutions

Curtin University of Technology