Australian Competition & Consumer Commission

ACCC Report

Targeting scams

Report of the ACCC on scams activity 2015

May 2016

www.accc.gov.au

Foreword

Delia Rickard

The Australian Competition and Consumer Commission's (ACCC) seventh annual report on scams activity in Australia highlights the significant financial loss and emotional harm incurred by the Australian community as a result of scams.

In 2015 the ACCC received over 105 000 scam reports, 14 000 more than in 2014. Reported monetary losses also grew by 4 per cent, to almost $85 million. For this year's report the ACCC has also reviewed data from other jurisdictions that receive reports or detect scams to gain a clearer picture of the significance of losses caused by scam activity in Australia. Reports to the Australian Cybercrime Online Reporting Network (ACORN) revealed losses of over $127 million[1]. Additionally, various scam disruption programs, operated by the ACCC and other agencies, also detect Australians sending funds to high risk jurisdictions. A combined estimate of losses to this unreported scam activity is $17.1 million. Combining Scamwatch and ACORN data with losses detected through scam disruption work, total scam losses exceed $229 million.

This report seeks to explore the nature of scam losses and identify some emerging trends. It focuses on data reported to Scamwatch and statistics provided in the report are in respect of that data unless specifically stated otherwise.

By far the most concerning trend in the ACCC's Scamwatch data related to investment scams, which overtook dating and romance scams as the category with the largest financial losses reported by Australians in the last year. Losses to investment scams almost doubled, from $12.5 million to $24.4 million with six people reporting individual losses of $1 million or more. Additionally, ACORN data shows reported losses to investment scams of almost $17 million. This brings total reported losses to more than $41 million and this still does not include those that do not report or may have reported to another organisation.

It is not hard to see why many Australians are losing large sums of money in these scams given how difficult they are to identify. These more sophisticated scams often involve scammers who use accurate technical jargon in carefully crafted cold calling scripts and accompany this with glossy brochures backed up by professional-looking websites. Even astute investors have been known to fall victim to these more calculated scams.

Losses reported to Scamwatch from dating and romance scams have reduced by more than $5 million (18.5 per cent) to $22.7 million, and are the second highest category in 2015. Together with investment scams, they account for 56 per cent of scam losses reported to Scamwatch in the past year. A further $14.8 million was reported to ACORN. When you add in the $17.1 million identified through disruption initiatives, this brings the total for relationships scams to over $54 million.

While investment and dating scams caused the most losses in 2015, the most commonly reported scams to the ACCC have been phishing scams, reclaim scams and upfront payment/advanced fee scams. Over 15 000 reports of phishing scams have been received, resulting in a total reported loss of $363 270.

While the number of reports we received are spread across all age groups, it is middle aged and older Australians who are reporting the highest losses. The ACCC has taken a closer look at the risk that scam activity poses to older Australians in this report.

The ACCC is increasingly concerned that scammers will be setting their sights on older Australians to access their superannuation funds via investment scams or to prey on their victims' emotions for financial gain through romance scams. Reports

[1] ACCC analysis of ACORN data specifically excludes those reports where they identify as having reported to Scamwatch and those that did not identify whether or not they had reported elsewhere.

of large individual losses in the older age groups are alarming and often occur in the context of investment or dating scams. Both investment and dating scams reveal a significantly higher number of individual losses greater than $100 000.

To minimise the harm caused by scams, the ACCC has continued its ongoing education and disruption work, and this year released its revised Best Practice Guidelines to bolster the online dating industry's capacity to identify scam profiles and create a safer experience for users.

The ACCC's scam disruption project, which uses financial intelligence to identify people transferring money offshore to high risk jurisdictions and warn them about scams, started with a focus on New South Wales and Australian Capital Territory residents and was expanded in 2015 to also include Victoria, the Northern Territory and Tasmania. Results of this work to date have been encouraging with 75 per cent of those warned by the ACCC ceasing to send money within six weeks of receiving a letter and have not been detected sending since. Of the people who contacted the ACCC and confirmed they had been targeted by a scam, 80 per cent were involved in an online dating scam.

While phone scams remained the most common, 38 per cent of scam approaches occurred through email, over the internet or through a social network platform and accounted for 44 per cent of losses. These forms of communication give scammers the advantage because they provide anonymity, global reach and a cheaper means of engaging in their deceptive practices.

One of the more common cold calling scams in 2015 involved scammers claiming to be from the Australian Taxation Office. Victims were told they had unpaid taxes and were threatened with fines or arrest unless they made an immediate payment. The scam emerged early in 2015 and the ACCC issued numerous warnings throughout the year to alert Australians.

Education and community awareness remains a key tool available to the ACCC for combating scams. In 2015, the ACCC overhauled and updated its Scamwatch website making it more accessible and improving the material available, including frequently updated statistics on scams. As a result, visits to the website increased significantly and improved the recognition of Scamwatch as an avenue for reporting scams and getting helpful and up-to-date advice.

Reducing the impact of scams through education and disruption remains a priority in 2016 for the ACCC and the Australasian Consumer Fraud Taskforce. This year, we will use Fraud Week to remind everyone to 'Wise up to scams' with a particular focus on those scams targeting Australians over 55.

Scams continue to be a complex issue affecting the Australian public and we hope that this report will be an informative source on the evolving trends in scams and the challenges of combating them. In 2016, the ACCC will continue to help all Australians identify and avoid scams and stem the flow of money to those engaged in fraudulent activity.

Delia Rickard

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

Contents

ISBN 978 1 922145 79 6

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

Important notice

The information in this publication is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of the law in any jurisdiction. Because it is intended only as a general guide, it may contain generalisations. You should obtain professional advice if you have any specific concern.

The ACCC has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

Parties who wish to re-publish or otherwise use the information in this publication must check this information for currency and accuracy prior to publication. This should be done prior to each publication edition, as ACCC guidance and relevant transitional legislation frequently change. Any queries parties have should be addressed to the Director, Corporate Communications ACCC, GPO Box 3131, Canberra ACT 2601, or publishing.unit@accc.gov.au.

ACCC 05/16_1085

www.accc.gov.au

1. Snapshot of 2015[2]

Overall contact levels and financial losses

- In 2015, the ACCC continued to observe a high level of scams activity in Australia, with 105 201 scam-related contacts received from consumers and businesses, compared with 91 637 in 2014.
- Scam losses reported to the ACCC totalled $84 941 766, representing an increase of just over $3 million from 2014 ($81 832 793). However, actual losses are likely to be considerably higher as many scams go unreported and the ACCC is only one of several agencies that receive scam reports.
- The Australian Cybercrime Online Reporting Network (ACORN) also receives scam reports and ACCC analysis of data reported to ACORN reveals reported losses of over $127 million.[3]
- Various scam disruption programs, operated by the ACCC, South Australian Police and Western Australian Police in collaboration with the WA Department of Commerce, use financial intelligence to proactively detect Australians sending funds to high risk jurisdictions. A combined estimate of losses to this unreported scam activity is $17.1 million.
- Combining Scamwatch and ACORN data with losses detected through scam disruption work, total scam losses exceed $229 million.

Most significant scams and losses

- In 2015, losses reported to the ACCC for investment scams almost doubled to over $24 million with six people reporting individual losses of over $1 million. Additionally, computer prediction software and sports investment schemes, which are often marketed as investment opportunities, cost Australians another $5.5 million.
- Losses reported to the ACCC for dating and romance scams reduced by 18.5 per cent in 2015 to almost $23 million—a decrease of just over $5 million in losses from that reported in 2014. These scams are the second most harmful in terms of financial loss. The percentage of those reporting losses for dating and romance scams reduced from 41 per cent to 33 per cent suggesting that disruption initiatives and sustained messaging around the dangers of sending money to people that have only been met online has made some impact.
- Advance fee fraud including inheritance scams, reclaim scams and Nigerian scams resulted in reported losses of over $14 million.
- While losses relating to attempts to gain personal information only account for around 3 per cent of total reported losses, the deliberate misuse of personal information underpins several of the scam categories where significant financial losses are reported. In terms of volume, phishing scams accounted for over 15 000 reports and other attempts to gain personal information through hacking or identity theft, brings the total number of reports to almost 27 890. This accounts for approximately a quarter of all scam reports and is 9.3 per cent more than the 25 504 reports in 2014.

Demographics

- While scam reports continue to be fairly consistent across the different age categories, there was a greater increase in reports in the 65 and over category—up 38 per cent from 7436 in 2014 to 10 260 in 2015. More middle-aged and older (aged 45 and over) Australians report scams than younger age groups (aged 44 and under).
- Total losses for the older age categories were more than double the loss reported by Australians aged under 44.
- On gender, 41 per cent of reports to the ACCC were from females, 34 per cent from males and 25 per cent were not specified. While females reported more, the total loss reported by males was greater. This is consistent with figures recorded in 2014. Contact levels and associated losses were largely consistent with the percentage and distribution of the Australian population by state and territory. The greatest number of scam reports came from New South Wales, Victoria and Queensland.

[2] Unless otherwise indicated, all statistics relate to scams reported to the ACCC and do not include ACORN data or scams disruption statistics.

[3] ACCC analysis of ACORN data specifically excludes those reports where they identify as having reported to Scamwatch and those that did not identify whether or not they had reported elsewhere.

Scam delivery method

- In 2015, the proportion of scams delivered via phone and text message reduced from the 53 per cent recorded in 2014 to 45 per cent of reports where the contact method was identified. These contact methods remain a popular mode of communication for scammers with reported losses increasing from $23 470 222 in 2014 to $26 927 316 in 2015.
- Scams delivered online, including email, internet and social networking platforms, account for $37 554 429 or 44 per cent of losses for reports identifying the scammer contact method.
- The ACCC's Scam Disruption Project identified that a third of all confirmed victims were targeted by scammers through social media sites.

Indigenous scam reports

- In 2015, the ACCC received 801 reports from people identifying as having an indigenous background. Losses in this group totalled $1 221 290. This represents 0.7 per cent of the reports and 1.4 per cent of the total losses for 2015. While the sample size is small, the data suggests that indigenous people have been victims of dating and romance and inheritance scams in particular.

Small business contacts

- In 2015, reports by those who identify as a small business totalled 3585 with $2 883 809 reported lost. While a report may be made by a small business, the scammer may not have specifically targeted the small business. Scams known to target small businesses include false billing scams, buying and selling scams for office supplies, overpayment scams and computer hacking to obtain personal information or install malware.

The ACCC's scam disruption activities

The ACCC undertakes a range of disruption activities to combat scams, including:

- targeted advice to individuals sending money to high risk jurisdictions
- awareness raising through education campaigns such as Fraud Week
- educating the public on how to identify and protect themselves from scams by maintaining the Scamwatch website and through the use of social media
- enforcement of consumer protection legislation when this is considered to be an effective tool to stop the conduct and deter others from perpetrating similar scams
- working with intermediaries who play a role in connecting scammers with their victims or facilitating funds transfers from victims to scammers.

ACCC's Scam Disruption Project

- The ACCC's Scam Disruption Project involves the use of financial intelligence to identify Australians sending funds to high risk jurisdictions. The ACCC warns potential victims that they may be the target of a scam. The project was initially trialled in New South Wales and the Australian Capital Territory and expanded in July 2015 to include Victoria, Tasmania and the Northern Territory—other jurisdictions have had similar disruption programs[4]. Over 3700 letters were sent by the ACCC in 2015 encouraging recipients to contact the ACCC to discuss their situation on a confidential basis.
- Of those who received the ACCC's warning letter, 75 per cent stopped sending money to those jurisdictions within six weeks and have not been detected sending since. Additionally, rates of detection of those identified as sending money to high risk jurisdictions reduced significantly following commencement of the project and after the program expanded. Initial rates of detection were well in excess of 250 people sending money to high risk jurisdictions each fortnight but this reduced to around 70 per fortnight after commencement and again following expansion of the program. This suggests that the program is reducing the financial losses suffered by victims of these scams but it could also be that scammers are relocating and having money sent to other countries. Scam Disruption will remain an ACCC compliance and enforcement priority in 2016.

[4] Further information regarding different state disruption programs is discussed under the heading *Case study: West Australian and South Australian authorities help scam victims' at page 20*

The ACCC's education and awareness raising activities

- In 2015, the ACCC relaunched its Scamwatch website with clearer presentation, updated information and a new tool that gives access to up-to-date statistics on the scam data reported to the ACCC. In 2015, the Scamwatch website received 1 556 384 unique visitors, which is a 16 per cent increase from 2014.
- The ACCC also continued to publish Scamwatch radar alerts to its subscription base, which increased by 5.7 per cent to 38 241 subscribers in 2015. A total of 15 Scamwatch alerts were published warning subscribers about emerging and significant scams last year.
- The ACCC's Scamwatch_gov Twitter profile also continued to communicate with its 9921 followers with 374 tweets posted during the year alerting Australians to scams currently circulating online or in the community.
- The ACCC's Little Black Book of Scams increased in popularity with 235 057 copies distributed in 2015. This is over twice the number of copies distributed in 2014.

Collaboration

- In 2015, the ACCC continued to chair the Australasian Consumer Fraud Taskforce, and coordinated with members and partners on the 2015 Fraud Week Campaign 'Get smarter with your data'. The campaign focused on personal data security and received significant media coverage to raise awareness of scams.
- A major review of the Online Dating Industry Best Practice Guidelines was conducted in collaboration with industry. The revised version of the guidelines aims to address the evolving nature of online dating scams and provide the latest advice on how sites can take steps to create a safer online environment for their customers. Copies of the guidelines can be downloaded from the ACCC website.
- In 2015, the ACCC assisted the Australian Institute of Criminology with its 2015 Scam Survey by inviting select victims to participate in interviews about their scam experience. The results of the survey and a report will be released in 2016. The survey involved a number of interviews with fraud victims with the aim of:
  - documenting the various impacts and harms that victims of online fraud experience
  - examining the reasons why some individuals choose to report online fraud to authorities, while others fail to make reports
  - determining how the support needs of victims might best be met.

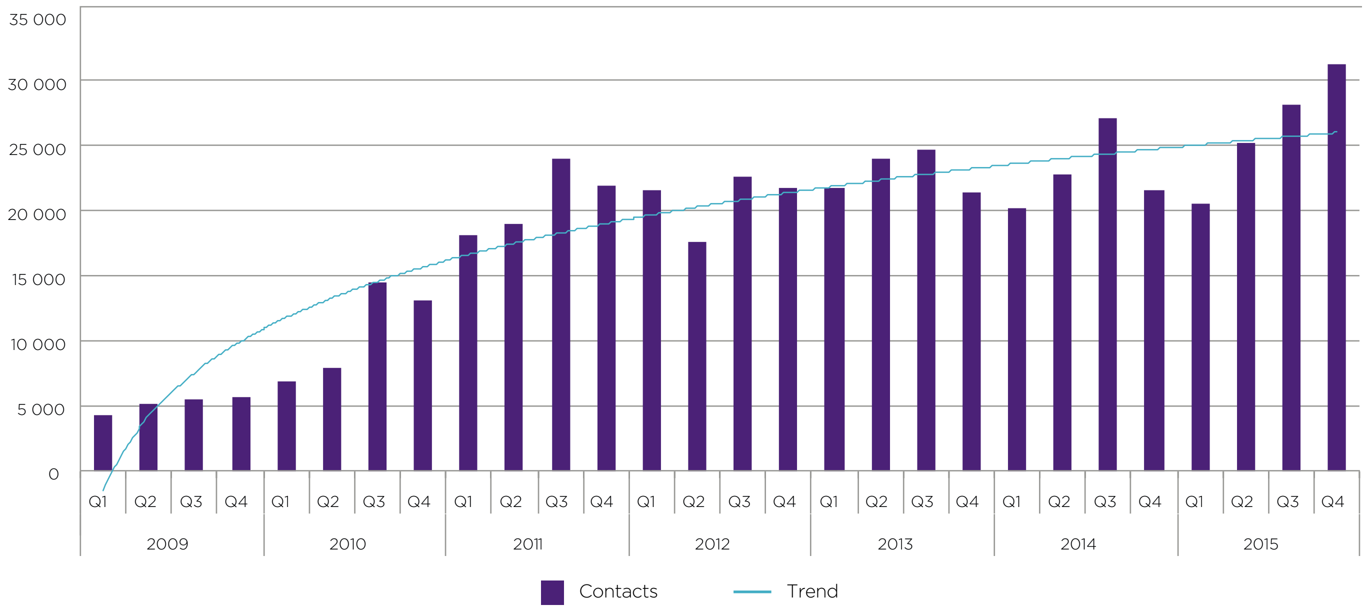
2. Scam contacts and trends[5]

2.1 Scam contact levels

In 2015, the ACCC received 105 201 scam-related contacts which is a 15 per cent increase over the 91 637 contacts reported in 2014.

Figure 1 provides a comparison of scam-related contacts to the ACCC over the past seven years. It shows an early upward trend with a slower level of increase in contact levels over the last three years.

Figure 1: Number of scam-related contacts to the ACCC 2009 to 2015



2.2 Financial losses to scams

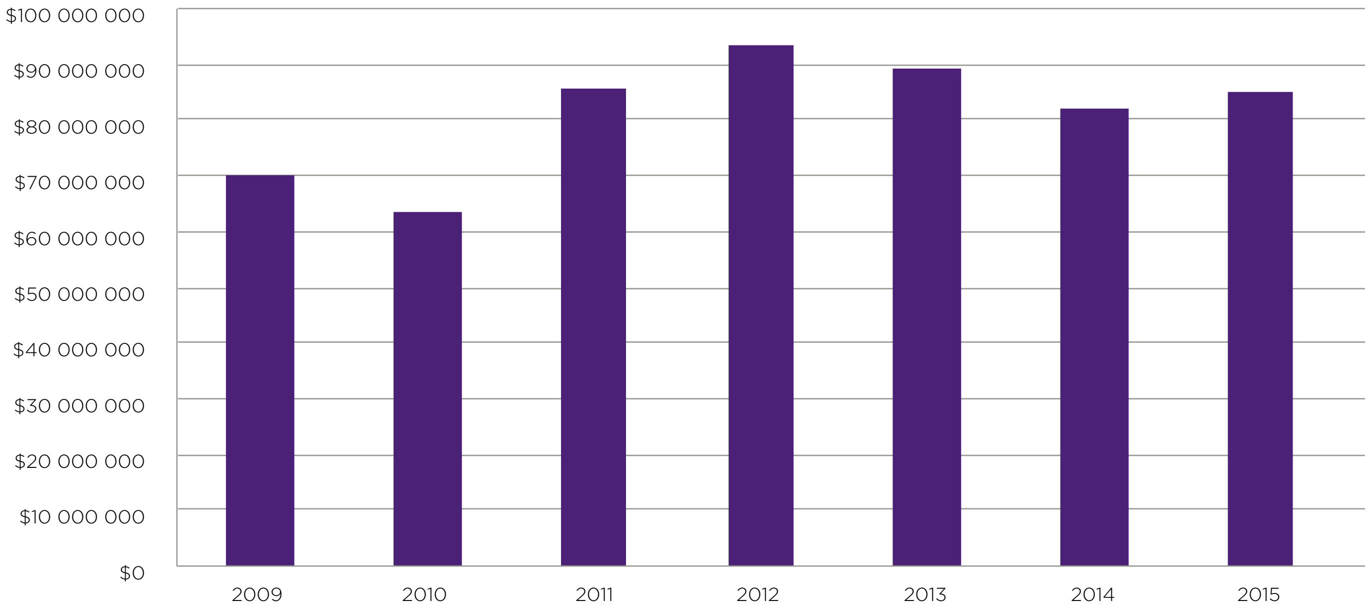
In 2015, the public reported losses of $84 941 766 to the ACCC which represents a 4 per cent increase over the $81 832 793 reported lost in 2014. While losses against some scams have decreased, others have dramatically increased. In 2015, losses reported to Scamwatch from dating and romance scams have decreased by 18.5 per cent from over $27 million to just below $23 million. Conversely losses attributed to investment scams have doubled from $12 million to $24 million.

- No financial loss was reported by 90 per cent of those reporting scam related activity to the ACCC in 2015. This represents an increase from the almost 88 per cent of those reporting no loss in 2014. This suggests many Australians can identify a scam when they encounter one and are aware of how to report it. The fact that many people report scams even though they have not themselves suffered a loss, demonstrates their desire to do what they can to alert others. This is pleasing and greatly assists Scamwatch in keeping abreast of the latest scams and alerting the community.
- A number of high loss scams were reported in 2015. 12.4 per cent of those who lost money reported losing over $10 000 and 319 people reported losing $50 000 or more. There were 8 reports with losses of $1 million or more.
- Over 50 per cent of people who lost money reported losing less than $500, which indicates most scams work as 'high volume low value scams'—that is, scams that are delivered to large numbers of recipients but cause smaller amounts of loss per victim.

Figure 2 provides a comparison of scam-related financial losses reported to the ACCC over the past seven years, with a slight decrease observed in 2013 and 2014 and an increase in 2015.

[5] Unless otherwise indicated, all statistics relate to scams reported to the ACCC and do not include ACORN data or scams disruption statistics.

Figure 2: Reported financial losses to the ACCC from 2009 to 2014



Losses to scams will be significantly higher than what is reported to Scamwatch, particularly given that many victims do not report their loss or may report it to a different agency.

The Australian Cybercrime Online Reporting Network (ACORN) also receives a large number of reports and ACCC analysis of data reported to ACORN reveals reported losses of more than $127 million[6] over and above losses reported to Scamwatch.

Various scam disruption programs, operated by the ACCC, South Australian Police and Western Australian Police in collaboration with the WA Department of Commerce, use financial intelligence to proactively detect Australians sending funds to high risk jurisdictions. A combined estimate of losses to this unreported scam activity is $17.1 million.

Adding the reported losses to Scamwatch and ACORN with unreported losses detected through scams disruption programs shows approximate overall losses in excess of $229 million.

Table 1 provides an overview of financial losses reported to Scamwatch against each scam category and sub-category. The top three scam sub-categories in terms of money lost were investment fraud, dating and romance and computer prediction software scams (often dressed up as investment opportunities). These three scams account for 62 per cent of reported financial losses.

A list of scam categories by state and territory is provided at appendix 2.

[6] ACCC analysis of ACORN data specifically excludes those reports where they identify as having reported to Scamwatch and those that did not identify whether or not they had reported elsewhere.

Table 1: Overview of scam types reported to the ACCC in 2015 by Scam Category Level 1

Scam category level 1	Scam category level 2	Amount reported lost	Contacts	Contacts reporting loss	Contacts reporting no loss	Less than $10K lost	More than $10k lost	Conversion rate
Attempts to gain your personal information (fake bank or telco, computer hacking, ID theft)	Hacking	$710 797	3 132	228	2 904	211	17	7.3%
	ID theft involving spam or phishing	$1 816 361	9 328	318	9 010	285	33	3.4%
	Phishing	$363 270	15 430	181	15 249	172	9	1.2%
	Sub total	**$2 890 428**	**27 890**	**727**	**27 163**	**668**	**59**	**2.6%**
Buying, selling or donating (classifieds, business listings, auction, health, fake business etc)	Classified scams	$856 442	2 851	442	2 409	419	23	15.5%
	Fake charity scams	$67 544	995	112	883	112	0	11.3%
	Fake trader websites	$1 458 858	2 735	1 587	1 148	1 567	20	58.0%
	False billing	$616 239	4 103	382	3 721	369	13	9.3%
	Health & medical products	$196 271	410	156	254	152	4	38.0%
	Mobile premium services	$19 821	826	327	499	327	0	39.6%
	Other buying & selling scams	$3 959 363	7 767	2 064	5 703	1 968	96	26.6%
	Overpayment scams	$179 112	1 506	125	1 381	121	4	8.3%
	Psychic & clairvoyant	$256 166	59	29	30	26	3	49.2%
	Remote access scams	$729 165	5 855	379	5 476	368	11	6.5%
	Sub total	**$8 338 981**	**27 107**	**5 603**	**21 504**	**5 429**	**174**	**20.7%**
Dating and Romance (Including Adult Services)	Dating & romance	$22 737 257	2 620	861	1 759	529	332	32.9%
	Sub total	**$22 737 257**	**2 620**	**861**	**1 759**	**529**	**332**	**32.9%**
Jobs & investment (sports betting, high return, pyramid scheme, employment)	Computer prediction software & sports investment schemes	$5 534 878	426	270	156	95	175	63.4%
	Investment schemes	$24 447 716	1 262	376	886	170	206	29.8%
	Job & employment	$952 742	2 456	246	2 210	214	32	10.0%
	Other business, employment & investment scams	$2 261 762	3 366	324	3 042	269	55	9.6%
	Pyramid Schemes	$951 721	259	32	227	28	4	12.4%
	Sub total	**$34 148 819**	**7 769**	**1 248**	**6 521**	**776**	**472**	**16.1%**
Threats & extortion (malware, ransomware and hitman scams)	Hitman scams	$456 396	816	28	788	21	7	3.4%
	Ransomware & malware	$388 167	4 439	154	4 285	144	10	3.5%
	Sub total	**$844 563**	**5 255**	**182**	**5 073**	**165**	**17**	**3.5%**
Unexpected money (inheritance, helping a foreigner, fake government or bank, loan opportunity)	Inheritance scams	$4 391 630	3 775	78	3 697	35	43	2.1%
	Nigerian scams	$4 549 807	980	141	839	104	37	14.4%
	Other upfront payment & advanced fee frauds	$3 899 312	11 502	893	10 609	808	85	7.8%
	Reclaim scams	$1 331 063	12 589	187	12 402	163	24	1.5%
	Sub total	**$14 171 812**	**28 846**	**1 299**	**27 547**	**1 110**	**189**	**4.5%**
Unexpected Prizes (lottery, travel, scratchie)	Scratchie scams	$284 324	565	19	546	11	8	3.4%
	Travel prize scams	$163 141	725	69	656	67	2	9.5%
	Unexpected prize & lottery scams	$1 337 296	3 683	258	3 425	235	23	7.0%
	Sub total	**$1 784 761**	**4 973**	**346**	**4 627**	**313**	**33**	**7.0%**
Not Supplied	Insufficient detail provided to classify scam	$25 145	741	6	735	5	1	0.8%
Grand total		**$84 941 766**	**105 201**	**10 272**	**94 929**	**8 995**	**1 277**	**9.8%**

Beyond the individual cost of scams

Victims of scams can experience loss ranging from a few dollars to one's life savings and even the family home. Many victims never recover financially and may become dependent upon welfare. While the impact of scams on Australian society and the economy is substantial, financial loss is just one part of the picture.

Non-financial losses

Scams can also result in unquantifiable loss such as emotional damage to the victims and their families. Individuals may suffer adverse effects on their mental health, work capacity, relationships and family.

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

In reality, everyone is vulnerable to scams at some stage in life (see page 21 for more information).

Economic and societal losses

The cost of scams to Australian business and consumers more broadly should not be underestimated.

Scams can cause significant harm to businesses. This may be experienced directly through loss of revenue when a business is a victim of a scam or indirectly as a result of reputational damage caused when scammers impersonate a business. There are also costs associated with ongoing monitoring and security upgrades.

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

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

Table 2 provides a comparison of financial losses reported to the ACCC in 2015 and 2014 by loss range. As with previous years, scammers continued to favour 'high volume scams', which involve targeting a large number of victims with requests for small amounts of money.

Unfortunately, in comparison to 2014 in which there were no reports of losses of $1 million or more, in 2015 there were eight such reports where victims lost money to more complex scams.

Table 2: Comparison of scam-related monetary losses reported to the ACCC in 2015 and 2014

Loss categories $	2015	Percentage 2015	2014	Percentage 2014	Variance
1-99	1 982	19.3%	1 834	16.5%	1.2
100-499	3 387	33.0%	3 957	35.7%	0.9
500-999	1 192	11.6%	1 469	13.3%	0.9
1000-9999	2 434	23.7%	2 576	23.2%	1.0
10000-49999	958	9.3%	884	8.0%	1.2
50000-499999	296	2.9%	352	3.2%	0.9
500000-999999	15	0.1%	14	0.1%	1.5
1 million–10 million	8	0.1%	0	0.0%	
Grand total	**10 272**	**100%**	**11 086**	**100%**	

2.3 Scam delivery methods

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

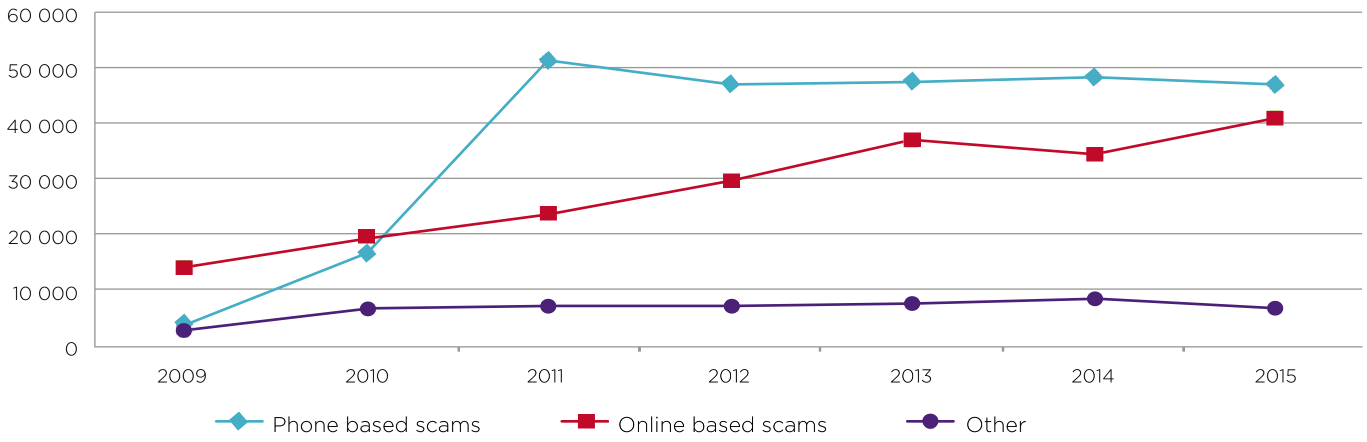
Table 3 provides a comparison of all scam delivery methods reported to the ACCC in 2015 and 2014. Scams delivered by phone (telephone calls and text messages) continued to be the most common method of targeting the public. Online delivery methods also continued to be popular with scammers in 2015.

Table 3: Scam delivery methods during 2015 and 2014 based on reports to the ACCC

Scammer contact mode	2015	Percentage 2015	2014	Percentage 2014
Phone	43 070	40.9%	44 411	48.5%
Email	29 151	27.7%	22 858	24.9%
Internet	8 394	8.0%	9 108	9.9%
Mail	5 059	4.8%	6 357	6.9%
Text message	3 985	3.8%	3 907	4.3%
Social networking/Online forums	2 653	2.5%	2 367	2.6%
In person	1 609	1.5%	1 431	1.6%
Mobile apps	599	0.6%	233	0.3%
Fax	151	0.1%	530	0.6%
N/A	10 530	10.0%	435	0.5%
Grand total	**105 201**	**100%**	**91 637**	**100%**

Figure 3 provides an overview of scam delivery methods over the past seven years.

Figure 3: Scam delivery methods 2009 to 2015 based on reports to the ACCC



Scams delivered by phone (landline and mobile)

In 2015, phones (landline and mobile) remained the most common scams delivery method with 43 070 reports. However, as a proportion of overall reported contact methods, it decreased from 53 per cent in 2014 to 45 per cent in 2015. Phone based scams resulted in losses totalling $25 794 447.

Of all the scams delivered via phone, reclaim scams were the most prevalent in 2015 with 8599 reports. Reclaim scams are those where scammers pretend to be offering a refund or payment of some kind in exchange for a small upfront fee. Often the scammer will claim to be a government representative. Attempts at phishing and identity theft via phone totalled 11 977. Together, these two scams account for 48 per cent of phone based scams reported to the ACCC in 2015.

In terms of losses, cold calling investment schemes resulted in losses to Australians of more than $11 million from just 636 reports. Computer prediction software and sports investment schemes were next in terms of losses for phone based scams, netting $3 424 610 from only 238 reports.

Scams delivered online (internet and email)

Online scams have increased by 18 per cent (6231) to 40 797 reports in 2015. This is mostly due to a substantial increase in email scams. Reports of scams delivered by email totalled 29 151 with a large number of these being phishing scams. While online scams are fewer in reports than phone based scams, they have resulted in greater losses ($38 473 213). The largest scam category for online losses was dating and romance scams. These scams with losses of $16 806 170 have been traditionally channelled through dating sites but are now occurring more frequently on social media platforms. Past experience shows that while these scams might originate from dating sites or through social networking sites, scammers move quickly to get their victims to correspond via phone or email, away from any scrutiny that online sites might conduct.

Online communication channels such as email and social networking forums allow scammers to communicate anonymously from anywhere in the world. The internet provides scammers with a level of anonymity, which gives scammers the ability to mask their physical location.

The increasing availability of wireless internet connectivity and use of mobile devices means that the public needs to be constantly alert to new scam approaches. Scammers will take advantage of the internet to transmit scams to any personal device that is connected to the web.

2.4 Demographics

Demographics are a useful tool for authorities in preventing scams. Demographic data such as age, gender and location provides an increased ability to identify those individuals most at risk of experiencing harm from scams. This data is necessary to inform potential targeted prevention strategies.

Age range

Table 4 shows the number of reports in each age category, reported and average losses, and a comparison of scam conversion rates by age range. The conversion rate is the percentage of scam contacts that report a loss. A low conversion rate could indicate a high probability that the scam is recognisable while a high conversion rate suggests that a scam is more likely to result in the loss of money.

Table 4: Age ranges provided by consumers reporting scams to the ACCC in 2015*

Age range	Number	% of total	Reporting loss	Reporting no loss	Conversion rate	Total loss	Average reported loss
Under 18	499	1%	157	342	31%	$131 684	$456
18-24	3 543	7%	923	2 620	26%	$2 017 702	$906
25-34	7 968	16%	1 641	6 327	21%	$5 829 047	$1 208
35-44	8 252	17%	1 402	6 850	17%	$7 372 195	$1 583
45-54	9 594	19%	1 357	8 237	14%	$13 320 853	$2 601
55-64	9 357	19%	1 083	8 274	12%	$11 004 587	$2 345
65 and Over	10 260	21%	861	9 399	8%	$10 215 426	$2 111
Grand total	**49 473**	**100%**	**7 424**	**42 049**	**15%**	**$49 891 494**	**$1 872**

* Provision of age data is not a mandatory reporting requirement. Consequently, totals will not match those provided for all scam reports.

In 2015, 47 per cent (49 473) of scam reports included the age of the victim, 2 per cent more than reports with age data in 2014. As a percentage of the total, each age category remained largely the same as 2014, with slight increases in the number of reports in the 55-64 and over 65 age categories. Combined, these groups represent 43 per cent of the total losses ($21 220 013) where age is recorded.

The total amount and average reported losses increased significantly for the over 45 age groups. While there are fewer people across these age groups reporting loss, when they do report loss it is often a lot higher. This suggests that older demographics are being targeted by low volume high value scams where scammers invest time in grooming their targets, e.g. online dating scams and investment scams. This indicates that education about these types of relationship scams might be usefully directed to older demographics to minimise the significant harm they cause.

Is age a factor?

That's where the money is

Purportedly, American bank robber Willie Sutton once said 'I rob banks because that's where the money is'. This self-evident truth doesn't seem too far from the thinking of the modern day scammer looking to make a fast buck.

In 2015, those reporting scams in the top three age groups lost more in total and on average than the remaining demographics, and accounted for almost 70 per cent of total losses. In terms of wealth, those over the age of 45 are more likely to be settled with significant assets and greater disposable income than younger people with a mortgage and balancing the weekly budget. It therefore makes sense, from a scammer's perspective, to target those with money.

Increasing internet use and victimisation

We know that scammers use any means available to them to target their victims and are increasingly using the anonymity that the internet and digital communications afford. It is not surprising then that as more Australians adopt these technologies, the risk of exposure to scams increases.

According to the Australian Bureau of Statistics (ABS), the proportion of those 55 and over accessing the internet frequently has grown from 53 per cent in 2010-11 to 65 per cent in 2014-15.[7] The rate of growth in this age group indicates later adoption and consequently less experience in the use of this technology. This increased exposure to digital communication technologies and lack of experience might help explain the increase in reported losses by older age groups.

Settling and unsettling

Australians aged 55 and over are often in periods of transition or undergoing considerations that leave them potentially vulnerable to investment or dating and romance scams. These two scam types accounted for $12 million or 56 per cent of the losses reported by this age group across all scams in 2015.

Australians approaching retirement or recently retired will naturally be looking for opportunities to invest or increase their investments. This mix of available funds through superannuation payouts and a desire to maximise wealth for retirement, leaves the over 55's open to exploitation by investment scammers who offer false promises of high returns and phoney assurances of low risks.

As online dating becomes more popular, it is likely that increasing numbers of mature-aged Australians will be looking for romance online. This mirrors trends in the United States where the share of 55 to 64 year olds who engage in online dating doubled from 6 per cent in 2013 to 12 per cent in 2015.[8] However, with it comes the risk of scams and past Scamwatch data consistently shows significant losses reported by this group.

A thesis from Swinburne University[9] suggests that senior singles commonly search for committed and deep relationships without necessarily desiring co-habitation. As such, seniors, and particularly those over 60, are potentially more open to the serious but distant relationships offered in common romance scam scripts and are more likely to encounter them as they seek romance online.

[7] Australian Bureau of Statistics' Australian Demographic Statistics Jun 2014, released Dec. 2014

[8] Pew Research Centre: http://www.pewinternet.org/2016/02/11/15-percent-of-american-adults-have-used-online-dating-sites-or-mobile-dating-apps/

[9] See: Sue Malta, http//researchbank.edu.au/vital/access/manager/Repository/swin:35671

Gender

Table 5 shows the breakdown of reports by gender.

Table 5: Gender breakdown of scam reports

Gender	Amount lost	Contacts	Percent of contacts	Contacts reporting loss
Male	$44 511 377	35 741	34%	15 919
Female	$26 543 191	42 768	41%	18 377
Not Specified	$13 887 198	26 692	25%	1232
Grand total	**$84 941 766**	**105 201**	**100%**	**35 528**

While 25 per cent of reports did not specify gender, 34 per cent of reports were from females and 41 per cent were from males. Females lost significantly less money, accounting for only 31 per cent of all reported losses.

Geographic location

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

Figure 4 shows a comparison of scam contacts received by the ACCC in 2015 from within Australia. New South Wales again received the greatest number of scam reports followed by Queensland and Victoria. Western Australia represents 10.6 per cent of the scam contacts this year, with the remaining states and territories recording below 10 per cent.

In addition to the above figures, the ACCC received 1251 scam contacts from people based overseas.

Figure 4: Scam contacts' location by state and territory 2015

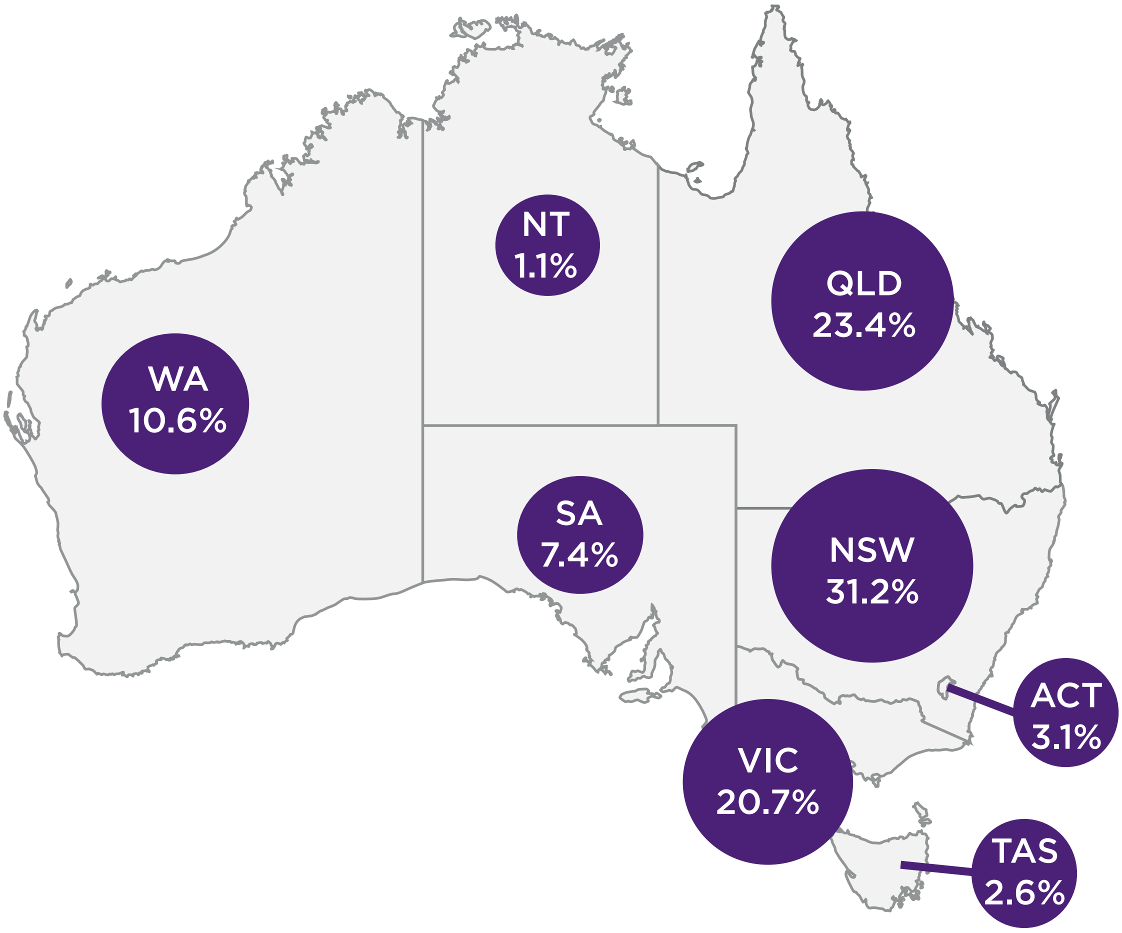


Table 6 provides a comparison of scam contact levels and financial losses against the distribution of the Australian population as a whole. Contact levels and associated losses reported to the ACCC were largely consistent with the percentage of the Australian population by state and territory. The Australian Capital Territory and Northern Territory reported double what might have been expected but their smaller population sizes means figures are more easily skewed and smaller increases in scam reports are more likely to affect overall percentages.

A breakdown of scam categories by state and territory is provided at appendix 2.

Table 6: Scam contacts' location by state and territory 2015

State	Percentage of total contacts that were based in Australia	Percentage of reported loss where contacts were based in Australia	Percentage of Australian population
NSW	31.2%	30.3%	32.0%
QLD	23.4%	21.7%	20.1%
VIC	20.7%	22.2%	25.0%
WA	10.6%	10.4%	10.9%
SA	7.4%	7.2%	7.1%
ACT	3.1%	3.6%	1.6%
TAS	2.6%	2.2%	2.2%
NT	1.1%	2.2%	1.0%
Grand total	**100%**	**100%**	**100%**

Indigenous Scam Reports

In 2015, the ACCC received 801 reports from people identifying as having an indigenous background. Losses in this group totalled $1 221 290. This represents 0.7 per cent of the reports and 1.4 per cent of the total losses for 2015. With such a small set of data it is difficult to draw clear conclusions about how or if indigenous Australians are uniquely affected by scams.

Overall, the data broadly reflects the trends seen in all 2015 scam reports. Dating and romance scams caused the greatest losses among indigenous people, followed by inheritance scams and computer prediction software & sports investment schemes. These scam types also feature in the top five scam types for all scam reports in 2015. The biggest difference related to investment scams, which were not as commonly reported by those with an indigenous background.

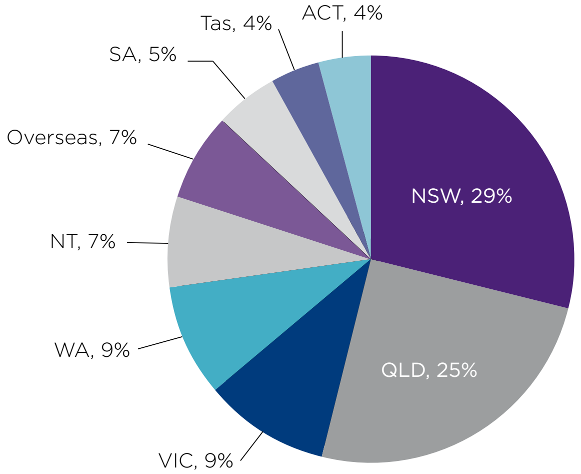
Table 7: Indigenous scam reports by category and reported loss

Scam category	Amount lost	Number of reports	Contacts reporting loss	Conversion rate
Dating & romance	$613 630	54	15	27.8%
Inheritance scams	$134 200	38	4	10.5%
Computer prediction software & sports investment schemes	$72 240	6	4	66.7%
Travel prize scams	$51 631	8	2	25.0%
Job & employment	$51 182	36	5	13.9%
Ransomware & malware	$45 010	26	5	19.2%
Nigerian scams	$41 300	21	5	23.8%
Reclaim scams	$37 375	38	2	5.3%
Other upfront payment & advanced fee frauds	$34 491	61	16	26.2%
Investment schemes	$33 479	11	7	63.6%
ID theft involving spam or phishing	$29 280	80	7	8.8%
Other buying & selling scams	$28 628	86	35	40.7%
Unexpected prize & lottery scams	$13 875	52	8	15.4%
Classified scams	$11 929	25	9	36.0%

Other business, employment & investment scams	$9 751	43	7	16.3%
Fake trader websites	$4 015	34	19	55.9%
Hacking	$2 016	33	4	12.1%
Hitman scams	$1 790	9	1	11.1%
False billing	$1 716	30	4	13.3%
Phishing	$1 200	54	1	1.9%
Overpayment scams	$1 135	15	2	13.3%
Fake charity scams	$530	13	2	15.4%
Psychic & clairvoyant	$450	2	2	100.0%
Pyramid Schemes	$260	9	1	11.1%
Health & medical products	$135	1	1	100.0%
Mobile premium services	$42.00	7	3	42.9%
Remote access scams		5		0.0%
Insufficent detail provided		4		0.0%
Grand total	**$1 221 290**	**801**	**171**	**21%**

A breakdown of indigenous reports by state also mirrors the national statistics.

Figure 5: Indigenous scam reports by location



The gender breakdown for indigenous reports follows a similar trend to the national figures where females report a greater number of scams but males suffer the greater share of the monetary losses.

Table 8: Indigenous scam reports by gender

Gender	Amount lost	Contacts	Percent of contacts	Contacts reporting loss	Percent of losses
Male	$714 723	319	39.8%	87	58.5%
Female	$501 409	446	55.7%	81	41.1%
Not Specified	$5 158	36	11.3%	3	0.4%
Grand total	**$1 221 290**	**801**	**100%**	**171**	**100%**

2.5 Conversion rates

The value of measuring the impact of a scam

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

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

Conversely, the lower the conversion rate, the greater the likelihood that more people can recognise a scam and avoid victimisation. Some scam categories achieve very high conversion rates and may highlight a particular susceptibility of victims to these types of scams.

While conversion rates for individual scam types fluctuate from year to year, the overall scam conversion rate has been falling for the last three years. In 2013, the rate was 14 per cent, falling to 12 per cent in 2014 and just 10 per cent in 2015.

This is a positive trend which suggests that Australians are increasingly able to identify scams when they encounter them. It also suggests that the vast majority of people who report scams to the ACCC do so for altruistic reasons and not purely because they have suffered a financial loss. This may also reflect the success of the ACCC and many other agencies to raise awareness of scams.

In 2015, there was a significant change in the conversion rate for dating and romance scams which reduced from 41 per cent to 33 per cent. The dating and romance scam category also saw a reduction of over $5 million in reported losses. These results may be an early reflection of recent scam disruption projects run by the ACCC and others and past efforts by the online dating industry following implementation of best practice guidelines on how to combat scams.

Table 9 compares conversion rates by scam categories in 2014 and 2015.

Table 9: Conversion rates by scam category 2014 and 2015

Scam category level 1	Scam category level 2	Conversion rate 2015	Conversion rate 2014
Attempts to gain your personal information (fake bank or telco, computer hacking, ID theft)	Hacking	7.3%	7.4%
	ID theft involving spam or phishing	3.4%	5.2%
	Phishing	1.2%	2.2%
	Sub total	**2.6%**	**4.1%**
Buying, selling or donating (classifieds, business listings, auction, health, fake business etc)	Classified scams	15.5%	24.3%
	Fake charity scams	11.3%	15.8%
	Fake trader websites	58.0%	65.4%
	False billing	9.3%	11.7%
	Health & medical products	38.0%	47.4%
	Mobile premium services	39.6%	38.1%
	Other buying & selling scams	26.6%	35.0%
	Overpayment scams	8.3%	14.5%
	Psychic & clairvoyant	49.2%	39.1%
	Remote access scams	6.5%	8.6%
	Sub total	**20.6%**	**23.7%**
Dating and Romance (Including Adult Services)	Dating & romance	32.9%	41.3%
	Sub total	**32.9%**	**41.3%**

Jobs & investment (sport, high return, pyramid scheme, employment)	Computer prediction software & sports investment schemes	63.4%	52.6%
	Investment schemes	29.8%	33.7%
	Job & employment	10.0%	13.6%
	Other business, employment & investment scams	9.6%	21.1%
	Pyramid Schemes	12.4%	15.7%
	Sub total	**16.1%**	**23.7%**
Threats & extortion (malware, ransomware and hitman scams)	Hitman scams	3.4%	12.1%
	Ransomware & malware	3.5%	6.3%
	Sub total	**3.5%**	**6.8%**
Unexpected money (inheritance, helping a foreigner, fake government or bank, loan opportunity)	Inheritance scams	2.1%	2.0%
	Nigerian scams	14.4%	8.2%
	Other upfront payment & advanced fee frauds	7.8%	15.7%
	Reclaim scams	1.5%	1.8%
	Sub total	**4.5%**	**4.6%**
Unexpected Prizes (lottery, travel, scratchie)	Scratchie scams	3.4%	5.4%
	Travel prize scams	9.5%	4.8%
	Unexpected prize & lottery scams	7.0%	8.2%
	Sub total	**7.0%**	**6.9%**
Not Supplied	Insufficient detail provided to classify scam	0.8%	3.5%
	Total	**9.8%**	**12.1%**

Spotlight on investment scams

Investment scams come in many guises including business ventures, superannuation schemes, managed funds and the sale or purchase of shares or property. Often the promised returns are higher than would normally be achievable, the scammers cleverly offer attractive, but not too unreasonable, returns.

In 2015, investment scams overtook dating and romance scams to take out the number one position for losses reported to the ACCC. As noted earlier in the report, investment scams reported to Scamwatch totalled $24.4 million. Additionally, ACORN data shows reported losses to investment scams of almost $17 million. This brings total reported losses to more than $41 million and this still does not include those that do not report or may have reported to another organisation. There were a number of significant individual losses reported to Scamwatch in this category with six reports of $1 million or more and an overall average loss per successful scam attempt of over $65 000.

The scammers often produce fake financial reports, forged share certificates, glossy initial public offerings and slick websites. In this context, it can be hard for potential victims to identify the scam and there is an increased likelihood of financial loss (which is also reflected in comparatively higher conversion rates for this scam category). Even experienced investors have been duped. The more popular contact methods for these scams are cold calling or unsolicited emails. Any investment offer out of the blue should be a clear warning sign that it is likely to be a scam.

Typically scam reports disproportionately come from older age groups as they seek to invest their savings and retirement funds. Should these age groups lose a significant portion of their savings, they may need to work longer than expected and experience a lower quality of life without their retirement funds.

Psychology

Investment decision making occurs through a process of assessment based on risk versus reward. Investment scams target this process and assure the victim of higher rewards while down-playing the relative risk of the venture or offer.

There are a number of common tactics used by investment scammers as explained by the United States Financial Industry Regulatory Authority who examined actual scripts of investment scammers. These tactics include:[10]

- **Phantom riches—**this is the most basic and obvious tactic, using the prospect of wealth to lure a victim in to sending money. This tactic generally offers greater than average returns on the investment.
- **Source credibility—**source credibility is the tactic of claiming superior credentials, experience or reputation to develop a level of trust.
- **Social consensus—**a tactic of claiming that others have invested to great success and the victim would be missing out if they did not.
- **Reciprocity—**offering a favour such as reduced commission or better service. Usually a time based tactic to attempt to convince the victim to take the offer without considering it fully.
- **Scarcity—**the tactic of suggesting the offer is for a limited time or supply creating a sense of urgency in the victim. Often used in fake initial purchase offers for shares.

[10] See http://money.usnews.com/mpney/personal-finance/invesing/articles/2009/03/05/the-psychology-of-investing-scams

Common types of investment scams

Share offers: These scams come in two varieties, either a purchase offer or a sale offer. Purchase offers often occur over the phone or email and target share owners. Scammers offer to purchase shares at a price lower than market value and rely on their victims not researching this price. They often attempt to pressure the sale.

Offers to sell shares occur in a similar manner, offering the sale of shares at a lower than market price, often using time limits to pressure the sale. Once money is sent, the victim will receive nothing from the scammers. Scammers will often use current events, such as creating fake initial public offer reports for reputable companies who are publicised as going public in the near future.

Managed funds: A managed fund is an investment account managed by an agent on behalf of the investor. Scams offering managed fund investments often sell their scams by offering high profit margins. These scams will usually be accompanied by websites with fake historical data demonstrating the supporting profitability of the firm.

Investment opportunities: Investment opportunities are very similar to managed funds, where the scammer is looking for direct transfer of funds that they will claim to manage thereafter. Often it will be associated with some form of business opportunity such as a new business, a mining opportunity or invention. The offer will usually be for a stake in the business or a set return on the investment. The scammer will provide glossy brochures or reports describing the business venture but these will be nothing more than works of fiction.

Protect yourself

The best strategy to avoid investment scams is to do your research. Investigate what you have been told and independently check the bona fides of those you are dealing with. Do not respond to emails and phone calls from strangers offering predictions on shares, investment tips, or investment advice. Always do your own research before you invest any money and check the company or scheme is licensed on ASIC's MoneySmart website. If there is any doubt at all, you should seek professional financial advice from an advisor registered with the Australian Securities and Investments Commission. Moneysmart.gov.au is a must visit for those contemplating investments.

3. Disruption activities

Disruption is the key focus of the ACCC's strategy to address scams. While enforcement action is appropriate in some cases, many scams operate from foreign jurisdictions which present considerable difficulties in identifying and prosecuting the perpetrators, and it is not always the most cost effective way of dealing with scams. Preventative measures are generally a more efficient way of reducing the potential harm caused by scams rather than prosecuting those that have committed fraud after the damage is done.

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

This chapter outlines efforts undertaken by the ACCC and others to deter, discourage and disable scammers targeting Australians.

3.1 Scam disruption activities

The ACCC recognises that disruption activity is one of the primary tools to effectively respond to scams given that many scams operate from a foreign jurisdiction, which makes traditional law enforcement complex and costly. Disruption activities provide cost effective alternatives for law enforcement agencies to restrict or even prevent scammers from operating, and to minimise the harm they may otherwise cause. Such disruption activities do not require scammers to be specifically identified or located. Instead, the focus is on collaborative efforts by government agencies and industry to identify intervention opportunities that might:

- prevent scammers from communicating with their targets
- provide timely warnings to better educate consumers that utilise legitimate services
- interrupt the sending of funds.

In 2015, the ACCC's key disruption activities focused on relationship scams and in particular, dating and romance scams. Working with the online dating industry, the ACCC revised the best practice guidelines in response to the evolving nature of scams and developments in technology. The ACCC also continued its targeted intervention strategy to warn Australians sending funds offshore that they might be the victim of a scam and commenced work with other intermediaries to make it harder for scammers to connect with their victims or for money to be transferred to them.

Relationship scams and the ACCC's Scam Disruption Project

In 2015, the ACCC continued and expanded its Scam Disruption Project, which commenced in August 2014. The project is a joint initiative working closely with state and territory police and consumer affairs agencies. It involves the use of financial intelligence to identify Australians sending funds to high risk jurisdictions and advising them that they may be the target of a scam. The objective of the project is to alert individuals to the fact that they may be victims of fraud and prevent them from losing more money. If people continue to send after six weeks of receiving the first letter, a second letter is sent urging them to stop sending and inviting them to contact the ACCC to discuss their situation.

Initially focusing on New South Wales and the Australian Capital Territory, the project expanded to Victoria, the Northern Territory and Tasmania in July 2015. Similar scam disruption projects have operated in Western Australia, South Australia and Queensland.

The ACCC has sent more than 6500 letters since the project began in August 2014 with over 3700 of these sent to potential scam victims in 2015. 75 per cent of those that received a letter stopped sending money within six weeks. Additionally, rates of detection for those sending money to high risk jurisdictions have significantly reduced. Early detection rates fell from 400 people per fortnight to just over 100 sending money to high risk jurisdictions. Similar reductions in the rate of detection were noted in the period just after the program expanded.

Dating and romance scams were the most common scam type reported by letter recipients who contacted the ACCC and accounted for 80 per cent of cases.

Where gender was identified, 67 per cent of letter recipients were male and 33 per cent were female.

In terms of losses, the Scam Disruption Project detected $8.7 million dollars of funds being sent to high risk jurisdictions in 2015. Since the commencement of the project amounts detected have totalled $18 million. However, many scam victims will have been involved in scams for lengthy periods of time and sent money to scammers in countries other than the high risk jurisdictions being monitored. Additional analysis of financial data on known scam victims, and those that continued to send money despite the initial warning, identified sending patterns that strongly suggested a scam was being perpetrated. Taking this data into account, the estimated losses for scam victims identified in 2015 are almost $35 million and approximately $65 million for the entirety of the project.[11]

As the project continues, fewer long-term scam victims are being detected. Experience tells us that detecting and warning potential victims before they have invested heavily in a scam, increases the likelihood that they will cease sending money.

[11] Estimated losses are calculated following further interrogation of financial intelligence related to confirmed victims and those that continue to send money beyond six weeks. An assessment is made as to what is likely to be related to the scam that has or is being perpetrated in order to gauge how much has been sent offshore to scammers. Factors taken into account are the timeframe in which the scam is likely to have been running, the destination of funds and the recipient of funds. Where these factors are consistent with known scam patterns, the amount is included in the total of estimated losses. The result is that significantly more money is detected as being lost to scams because this process detects money that may have been sent over several months, or even years, and often to numerous overseas jurisdictions that do not form part of the initial scam detection process. The losses identified here are in addition to losses noted elsewhere in this report.

Case study: West Australian and South Australian authorities help scam victims

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

South Australian scams disruption

In May 2013, a dedicated operation named 'Disrepair' was launched to help reduce the flow of cash from SA scam victims. As part of this operation, police officers follow the money trail of transfers to West Africa and identify South Australians who may be sending money without good cause. Police then send a letter to those identified alerting them to the fact they may be sending money to scammers and in some cases follow up with a home visit or phone call.

Figures provided by SA Police for 2015 show that fund transfers to known high-risk jurisdictions were down by 26 per cent on the previous year and there was an 18 per cent reduction in the number of people sending to West African countries. There has also been a 15 per cent reduction in the amount sent — from over $1.8 million dollars in 2014 to just under $1.6 million in 2015.

In December 2015, Operation Disrepair was the winner of a National Meritorious Police Award for the 2015 Australian Crime & Violence Prevention Awards.

West Australian scams disruption

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

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

Almost 6000 letters have been sent out since 2013 and more are sent every month . The first letter addressed to the householder leads to about 70 per cent of victims ceasing to send money. Those who continue sending receive a second personalised letter after which about 50 per cent stop sending funds.

During 2015, Project Sunbird identified over 1400 potential victims who sent almost $6.8 million to West Africa.

Consumer Protection also provides education and advice on all types of scams through its ScamNet service. In 2015, 391 Western Australian victims of scams reported losing a total of $7 399 388. While this represented a decrease in losses of 39 per cent from 2014, the average loss only decreased by 10 per cent. There is believed to be many more victims who have not contacted ScamNet for assistance so this is not necessarily indicative of an overall decrease in scam incidents.

WA Police and the Department of Commerce also help scam victims access support services to overcome their experience. Further information about Project Sunbird and ScamNet can be found at: www.scamnet.wa.gov.au.

Revised Best Practice Guidelines for the Dating Industry

In 2011–12, the ACCC released Best Practice Guidelines for the online dating industry following collaboration with dating website operators. The objective was to identify strategies to improve responses to these scams by assisting dating site operators in three key areas:

- the inclusion of appropriate scam warnings and information on websites
- establishing vetting and checking systems to detect and deal with scammers
- making available to consumers a scam complaint handling mechanism.

In 2015, the ACCC worked in collaboration with the dating industry to review and update the guidelines. In addition to general updates to language and content to reflect the evolving nature of the online space, the revised guidelines also include recommendations that online dating sites:

- implement pro-active validation and authentication procedures to ensure the legitimacy of online dating profiles
- develop systems and counter measures to protect users' personal information against identity theft
- adopt the Office of the Australian Information Commissioner's data breach notification guide and encourage the implementation of a data breach response plan
- implement measures to target scam warnings to higher risk groups based on demographics and to consumers leaving the safety and security of the dating site.

A new section on consumer protection to address issues around clarity of terms and conditions and pricing has also been included in the guidelines. The guidelines were released in February 2016 and a copy can be downloaded from www.accc.gov.au.

Everyone is vulnerable at some stage to a scam

Many people may look at an online dating scam and wonder, 'How could someone fall for this?'

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

Some vulnerability factors include:

- Personal circumstances —people are more likely to fall for a scam if the ruse personally relates to them, particularly where it elicits an emotional response.
- Charitable nature—some people are more predisposed to want to help those in need, which makes them vulnerable to the many scams that are masked as pleas for help. For example, someone who has lost a loved one to an illness may be more vulnerable to scammers making pleas for financial help to cover costs associated with a medical emergency.
- Urgency—people may respond to a scam when it creates a sense of urgency around something important. Often scammers will create fictitious situations such as having been detained in a foreign jurisdiction and needing immediate help with legal expenses, or they will claim that a fee needs to be paid within 48 hours to release funds before the government confiscates them.
- Other scams prey on different vulnerabilities. A small business that has unsophisticated accounting systems may inadvertently pay a fraudulent invoice. Someone being offered a phoney tax rebate may think this is timely because of mounting bill pressures. Some people just have a 'nothing ventured, nothing gained' attitude to life.
- Many of us find ourselves in a position when personal circumstances make us more vulnerable including:
    - Time-poor—when a person or business is pressured in terms of available time, they may respond to a scam before realising what it is.
    - Financial troubles—when people are experiencing financial difficulties, they may be more likely to ignore cues that an offer is a scam.
    - Gambling or risk-taking personality–some personality types are more likely to accept an offer and see where it will take them, before realising that it is a scam.

There is a common misconception that only the gullible and greedy fall victim to a scam, however, many professional and well-educated people have been taken in. Scammers are particularly good at presenting themselves in a convincing light and will use any information they can to persuade their victims to part with their money. The more detail they have about your personal circumstances, the greater the risk of becoming a victim.

By raising awareness of scams and the importance of keeping your personal details secure, the ACCC hopes to alert people to the pitfalls and protect the Australian community against fraud.

4. Small business scams

In 2015, reports by those who identify as a small business totalled 3585 with $2 883 809 reported lost. While a report may be made by a small business the scammer may not have specifically targeted the small business. Scams known to target small businesses include false billing scams, buying and selling scams for office supplies, overpayment scams and computer hacking to obtain personal information or install malware.

Table 10: Overview of scam types reported to the ACCC in 2015 by scam category and those identifying as a small business

Scam category	Amount lost	Number of contacts	Contacts reporting loss	Conversion rate
Investment schemes	$1 092 495	20	5	25%
Other buying & selling scams	$394 886	593	92	16%
False billing	$232 850	716	94	13%
Other business, employment & investment scams	$223 059	294	37	13%
Hacking	$213 990	98	5	5%
Other upfront payment & advanced fee frauds	$153 749	273	24	9%
Dating & romance	$152 250	6	3	50%
Fake trader websites	$116 864	63	25	40%
Classified scams	$73 037	113	15	13%
Nigerian scams	$61 300	37	4	11%
Remote access scams	$43 089	17	3	18%
Reclaim scams	$39 118	75	3	4%
Overpayment scams	$17 495	95	3	3%
ID theft involving spam or phishing	$16 964	277	7	3%
Computer prediction software & sports investment schemes	$15 214	3	2	67%
Fake charity scams	$10 522	102	16	16%
Job & employment	$10 411	46	5	11%
Phishing	$7 740	350	6	2%
Health & medical products	$3 475	31	2	6%
Hitman scams	$1 790	19	1	5%
Ransomware & malware	$1 622	138	4	3%
Mobile premium services	$946	15	9	60%
Pyramid schemes	$369	7	1	14%
Unexpected prize & lottery scams	$324	55	2	4%
Inheritance scams	$0	61	0	0%
Travel prize scams	$0	19	0	0%
Insufficient detail provided to identify scam	$250	62	1	2%
Grand total	**$2 883 809**	**3 585**	**369**	**10%**

Buying and selling scams targeting small businesses often involve the scammer sending a ‘bill’ for printer cartridges or other office supplies in the hope that a busy small business will pay without checking whether the request is legitimate. False billing scams usually arrive as a request for advertising in a business directory or purchase of a domain name that will be deceptively similar to a renewal of existing services. Overpayment scams targeting small businesses can involve making orders for products with stolen credit cards and then quickly cancelling the order but asking for a refund to be paid to a different account.

Often these typical small business scams will result in one-off payments and losses from which a business can recover. However, hacking, malware and targeted phishing now present significant risks to businesses.

Scams that should be of greater concern to businesses are those that look to exploit information technology vulnerabilities. This is an especially important issue for small businesses not only because financial losses can be tens of thousands of dollars, but also because of reputational risks in the event that the personal information of customers is compromised.

Data security—it's your business

Two of the more significant and emerging scams posing a threat to businesses in 2015 were the business email compromise scam and ransomware.

Business email compromise scam

The business email compromise scam is a more recent concern which has particularly affected businesses based in Europe and the USA but has been seen here as well. The average loss reported to the US Internet Crime Complaint Centre was $130 000 USD and they experienced a 270 per cent increase in reports of this scam in 2015.

These scams primarily target businesses that have overseas partnerships with suppliers and regularly make wire transfer payments to Chinese businesses, although the scammers may not themselves be located in China.

The scam involves an email purportedly coming from an upper management email address advising of new payment arrangements requiring a transfer of funds to a new account. These emails look legitimate as they appear to come from the correct email address and closely resemble legitimate emails by copying their formatting and style.

This scam can only function through the scammer getting access to the business' email address, whether through a virus or successful phishing attack. The scam can also operate outwardly, targeting your customers with a request to update payment details. Often the scam goes undetected until the legitimate supplier asks why they have not been paid.

The best way to prevent falling victim to this scam is to:

- implement sound financial security procedures that include a two-step verification process for wire transfer payments and be suspicious of requests for secrecy or pressure to take action quickly
- independently check and verify any request for updates to payment information
- install security software and keep it up-to-date.

Ransomware

Ransomware scams affect everyone, however if a business is hit by one, it can cripple the company and cost thousands.

Ransomware is a type of virus that infects computer systems and encrypts the device to prevent user access until payment is made to unlock it.

The money that is demanded for ransomware scams may be relatively small when compared with the cost of losing access to important business data, lost time and customer confidence. Some businesses even report missing out on important contracts due to the time wasted dealing with such scams. In light of this, many businesses consider making the payment the best decision. However, even if payment is made the virus may not be removed and only serves to encourage this criminal conduct.

Ransomware scams are delivered in a variety of ways but the most common is through email. The emails often appear to be from legitimate companies such as Australia Post regarding an undelivered package or a utility provider about an unpaid bill. It has also been known to be delivered through emails posing as the Australian Federal Police seeking payment for fines. Invariably, the emails will ask the recipient to follow a link or open an attachment causing malicious software to be downloaded.

Protecting yourself from these viruses can be easy if you:

- Back-up your data and keep this back-up offline to prevent infection. If ransomware is installed, you can restore factory settings and re-install software and data from the stand alone hard disk. Such devices are relatively inexpensive and good insurance.
- Do not open attachments or click on links in emails or social media messages you've received from strangers. Check email addresses as these will often reveal that the email doesn't come from the organisation it claims.
- Keep your antivirus software up-to-date because security software companies regularly detect new variations of these viruses and implement patches to thwart them.
- Ensure employees are alerted to possible scams and know how to spot a fake email.
- If a computer is infected, disconnect it immediately from your network and seek technical advice.

5. The top 10: 2015's most significant scams

5.1 Overview of the most common scam types reported to the ACCC

In 2015, the ACCC continued receiving contacts about a broad range of scams targeting Australians. Table 11 provides an overview of all scam types reported to the ACCC in 2015 in order of number of contacts per category.

A list of scam categories by state and territory is provided at appendix 2.

Table 11: Overview of scam types reported to the ACCC in 2015 in order of contact levels

Scam category	Amount reported lost	Contacts	Contacts reporting no loss	Contacts reporting loss	Less than $10K lost	Greater than $10K and less than $100K lost	Greater than $100K lost	Conversion rate
Phishing	$363 270	15 430	15 249	181	172	9	0	1.2%
Reclaim scams	$1 331 063	12 589	12 402	187	163	23	1	1.5%
Other upfront payment & advanced fee frauds	$3 899 312	11 502	10 609	893	808	83	2	7.8%
ID theft involving spam or phishing	$1 816 361	9 328	9 010	318	285	30	3	3.4%
Other buying & selling scams	$3 959 363	7 767	5 703	2 064	1 968	95	1	26.6%
Remote access scams	$729 165	5 855	5 476	379	368	11	0	6.5%
Ransomware & malware	$388 167	4 439	4 285	154	144	10	0	3.5%
False billing	$616 239	4 103	3 721	382	369	13	0	9.3%
Inheritance scams	$4 391 630	3 775	3 697	78	35	36	7	2.1%
Unexpected prize & lottery scams	$1 337 296	3 683	3 425	258	235	20	3	7.0%
Other business, employment & investment scams	$2 261 762	3 366	3 042	324	269	54	1	9.6%
Hacking	$710 797	3 132	2 904	228	211	17	0	7.3%
Classified scams	$856 442	2 851	2 409	442	419	23	0	15.5%
Fake trader websites	$1 458 858	2 735	1 148	1 587	1 567	19	1	58.0%
Dating & romance	$22 737 257	2 620	1 759	861	529	275	57	32.9%
Job & employment	$952 742	2 456	2 210	246	214	32	0	10.0%
Overpayment scams	$179 112	1 506	1 381	125	121	4	0	8.3%
Investment schemes	$24 447 716	1 262	886	376	170	153	53	29.8%
Fake charity scams	$67 544	995	883	112	112	0	0	11.3%
Nigerian scams	$4 549 807	980	839	141	104	32	5	14.4%
Mobile premium services	$19 821	826	499	327	327	0	0	39.6%
Hitman scams	$456 396	816	788	28	21	5	2	3.4%
Travel prize scams	$163 141	725	656	69	67	2	0	9.5%
Scratchie scams	$284 324	565	546	19	11	8	0	3.4%
Computer prediction software & sports investment schemes	$5 534 878	426	156	270	95	167	8	63.4%
Health & medical products	$196 271	410	254	156	152	4	0	38.0%
Pyramid schemes	$951 721	259	227	32	28	3	1	12.4%
Psychic & clairvoyant	$256 166	59	30	29	26	1	2	49.2%
Insufficient data provided	$25 145	741	735	6	5	1	0	0.8%
Grand total	**$84 941 766**	**105 201**	**94 929**	**10 272**	**8995**	**1130**	**147**	**9.8%**

5.2 The top 10 scams in 2015 ($ reported loss)

In 2015, the top scams reported to the ACCC in terms of reported loss were investment schemes, dating and romance and various forms of advanced fee fraud. Table 12 shows the top 10 scam categories* by reported loss for 2015.

Table 12: Overview of scam types reported to the ACCC in 2015 in order of reported loss

Scam category	Amount reported lost	Contacts	Contacts reporting no loss	Contacts reporting loss	Less than $10K lost	Greater than $10K and less than $100K lost	Greater than $100K lost	Conversion rate
Investment schemes	$24 447 716	1 262	886	376	170	153	53	29.8%
Dating & romance	$22 737 257	2 620	1 759	861	529	275	57	32.9%
Computer prediction software & sports investment schemes	$5 534 878	426	156	270	95	167	8	63.4%
Nigerian scams	$4 549 807	980	839	141	104	32	5	14.4%
Inheritance scams	$4 391 630	3 775	3 697	78	35	36	7	2.1%
Other buying & selling scams	$3 959 363	7 767	5 703	2 064	1 968	95	1	26.6%
Other upfront payment & advanced fee frauds	$3 899 312	11 502	10 609	893	808	83	2	7.8%
Other business, employment & investment scams	$2 261 762	3 366	3 042	324	269	54	1	9.6%
ID theft involving spam or phishing	$1 816 361	9 328	9 010	318	285	30	3	3.4%
Fake trader websites	$1 458 858	2 735	1 148	1 587	1 567	19	1	58.0%
Unexpected prize & lottery scams	$1 337 296	3 683	3 425	258	235	20	3	7.0%
Reclaim scams	$1 331 063	12 589	12 402	187	163	23	1	1.5%
Job & employment	$952 742	2 456	2 210	246	214	32	0	10.0%
Pyramid schemes	$951 721	259	227	32	28	3	1	12.4%
Classified scams	$856 442	2 851	2 409	442	419	23	0	15.5%
Remote access scams	$729 165	5 855	5 476	379	368	11	0	6.5%
Hacking	$710 797	3 132	2 904	228	211	17	0	7.3%
False billing	$616 239	4 103	3 721	382	369	13	0	9.3%
Hitman scams	$456 396	816	788	28	21	5	2	3.4%
Ransomware & malware	$388 167	4 439	4 285	154	144	10	0	3.5%
Phishing	$363 270	15 430	15 249	181	172	9	0	1.2%
Scratchie scams	$284 324	565	546	19	11	8	0	3.4%
Psychic & clairvoyant	$256 166	59	30	29	26	1	2	49.2%
Health & medical products	$196 271	410	254	156	152	4	0	38.0%
Overpayment scams	$179 112	1 506	1 381	125	121	4	0	8.3%
Travel prize scams	$163 141	725	656	69	67	2	0	9.5%
Fake charity scams	$67 544	995	883	112	112	0	0	11.3%
Mobile premium services	$19 821	826	499	327	327	0	0	39.6%
Insufficient data provided	$25 145	741	735	6	5	1	0	0.8%
Grand total	**$84 941 766**	**105 201**	**94 929**	**10 272**	**8 995**	**1 130**	**147**	**9.8%**

Table 13 provides a comparison of the losses between 2014 and 2015. In 2015, investment schemes took over dating and romance as the scam with the greatest losses. Investment schemes almost doubled while dating and romance scams dropped in losses by over $5 million. This table demonstrates the significant shifts which can occur in the space of a year.

Table 13: Comparison of the top 10 scam report levels 2014 and 2015

Top 10 scams by reported loss	2015	2014
Investment schemes	$24 447 716	$12 462 624
Dating & romance	$22 737 257	$27 904 562
Computer prediction software & sports investment schemes	$5 534 878	$9 039 340
Nigerian scams	$4 549 807	$2 193 094
Inheritance scams	$4 391 630	$3 888 275
ID theft involving spam or phishing	$1 816 361	$773 269
Fake trader websites	$1 458 858	$2 134 163
Unexpected prize & lottery scams	$1 337 296	$1 890 265
Reclaim scams	$1 331 063	$980 165
Job & employment	$952 742	$938 196

* The Top 10 scam categories exclude three 'Other' scam categories as these contain a range of scams not easily classified under generic headings.

The following sections summarise the top 10 scams by monetary loss, and include victim stories which are drawn from real-life examples of scams reported to the ACCC. Names and details have been changed.

#1. Investment Scams

Number of scam reports:
1262

Per cent of total reported loss:
29%

Per cent of total scams reported:
1.2%

Number of consumers reporting losses:
376

Total losses reported to Scamwatch:
$24 447 716

Total losses reported to ACORN:
$16 865 905

Total reported losses to Scamwatch and ACORN:
$41 313 621

Scam conversion rate:
30%

Most affected age group:
45+ 81%

Gender:
Female: 33%
Male: 67%

Contact modes:
Phone 50%
Email 17%
Internet 12%

In 2015, investment scams replaced dating and romance scams as the highest category in terms of loss reported to the ACCC. The ACCC received 1262 reports about investment scams with 376 reporting losses, an increase of 19 per cent from 2014. Financial losses almost doubled from $12 462 624 in 2014 to $24 447 716 in 2015, the largest growth of any category.

The conversion rate of 30 per cent is much higher than the overall 10 per cent average for all scams in 2015. With high potential profits from these scams, scammers can afford to invest significant time and resources which has led to a number of large individual losses to investment scams this year. Six people reported losing $1 million dollars or more to an investment scam.

Typically operating offshore, scammers adopt a number of strategies to convince their victims that their offer is real. They often employ high-pressure sales tactics, fake websites, slick public offer documents and convincing but fake annual reports. Investment scammers present professionally, have polished scripts and will spend as long as necessary to convince a potential victim of the legitimacy of their offer. When successful, a skilled scammer will sound like a knowledgeable professional and, in some cases, they have even convinced experienced investors to part with their money.

One common strategy for scammers is to sell fake initial public offerings for well-known companies seeking to publicly list on the share market. The use of current events lends further credence to the scam and helps to convince their victims to purchase shares at a price lower than is being predicted in the media. Once payment is made for the shares, the scammers disappear and can't be contacted.

Victim’s story: Scammers crack Arthur and Heather’s nest egg

Arthur and Heather were just a few years away from retirement. They had saved well and built up a healthy superannuation fund. However, when Arthur received a glossy brochure in the mail from a company called ‘Cutting Edge Investments’ offering a unique investment opportunity, they considered the possibility of growing their nest egg a little more. The brochure claimed it was offering exclusive access to the first batch of shares for a well-known international company’s initial public offering (IPO). The brochure made it sound like an exclusive offer to only a select set of people, who could buy shares at a reduced cost ahead of everyone else, and that the shares were sure to increase in value very quickly. There were examples of other company’s IPOs from recent years, which showed how much money was made by those who bought shares in similar deals.

Arthur and Heather didn’t know much about the stock market but they had heard about this IPO on the news, and the brochure put everything in terms that were easy to understand. They decided to visit the website listed on the brochure and then called a number they found.

The scammers were very smooth and well spoken. They explained the deal in a way that made it sound almost too good to be true and applied a little pressure to give Arthur and Heather a push towards making a decision quickly. They were also able to convince Arthur and Heather to invest significantly more than what they were considering.

Arthur and Heather sent $15 000 to Cutting Edge Investment’s headquarters in Hong Kong and even told a few close friends to consider doing the same. The scammers sent Arthur and Heather a receipt email with all the details and told them to enjoy the returns they were about to receive. They also offered a further reduced price on an additional set of shares if they bought within the next 12 hours. Arthur and Heather paid an additional $5000.

When the day of the IPO came, Arthur and Heather were keenly watching the figures online but none of it matched up with what they were told over the phone. There was also no mention of the ‘special advanced shares’ which they had bought. They immediately tried to call Cutting Edge Investments but only got a recording stating the number was disconnected. By this time, the scammers had taken Arthur and Heather’s money, as well as hundreds of thousands of dollars from other victims.

‘Always consult a reputable AFS licenced financial consultant before parting with money and beware of schemes that seem too good to be true because they almost always are. Check out moneysmart.gov.au for a list of companies you shouldn’t deal with.’ ACCC Deputy Chair Delia Rickard

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Do not give your details to an unsolicited caller or reply to emails offering financial advice or investment opportunities—just hang up or delete the email.
2. Be suspicious of investment opportunities that promise a high return with little or no risk.
3. Check if a financial advisor is registered via the ASIC website. Any business or person that offers or advises you about financial products must be an Australian Financial Services (AFS) licence holder.
4. Check ASIC’s list of companies you should not deal with. If the company that called you is on the list—do not deal with them. And remember, just because a company is not on the list doesn’t mean it is legitimate.
5. Do not let anyone pressure you into making decisions about your money or investments and never commit to any investment at a seminar—always get independent legal or financial advice.
6. Do not respond to emails from strangers offering predictions on shares, investment tips, or investment advice.
7. If you feel an offer to buy shares might be legitimate, always check the company’s listing on the stock exchange for its current value and recent shares performance. Some offers to buy your shares may be well below market value.
8. If you are under 55, watch out for offers promoting easy access to your preserved superannuation benefits. If you illegally access your super early, you may face penalties under taxation law.

#2. Dating and romance scams

Number of scam reports:
2620

Per cent of total reported loss:
27%

Per cent of total scams reported:
2.5%

Number of consumers reporting losses:
861

Total losses reported to Scamwatch:
$22 737 257

Total losses reported to ACORN:
$14 863 826

Losses detected through scam disruption projects:
$17 100 000

Total scam losses – Scamwatch, ACORN and disruption:
$54 701 083

Scam conversion rate:
33%

Most affected age group:
55-64 37%

Gender:
Female: 53%
Male: 47%

Contact modes:
Internet 26%
Email 25%
Social media 24%

In 2015, reported losses for dating and romance scams totalled $22 737 257, a decline of 19 per cent and second behind investment scams in terms of losses. The ACCC received 2620 reports of dating and romance scams in 2015, up 5 per cent from the previous year but with fewer people reporting losses. However, financial losses continue to remain substantially disproportionate to contacts, with dating and romance scams making up only 2 per cent of all scam-related contacts and average losses in excess of $26 000.

Dating and romance scams generally start with the victim meeting someone online. The scammers say they come from a western country and claim to be overseas for work reasons or because of a familial situation which required them to go there, for example to take care of a loved one or claim an inheritance. The scammer quickly attempts to establish a relationship and often declares their love early in the relationship. Once this is accomplished, they begin their requests for money.

Excuses for why the victim needs to send money are elaborate and varied but the most common of these is for travel expenses so they can come to meet their partner. There is always a story about some barrier or event which prevents the scammer being able to travel to Australia and then a subsequent request for money to resolve the fictitious situation. Victims believe they are helping pay for airline tickets, military leave passes, visa applications, medical expenses or government fees. The requests for money are never-ending, their stories become more complicated and promises are never kept.

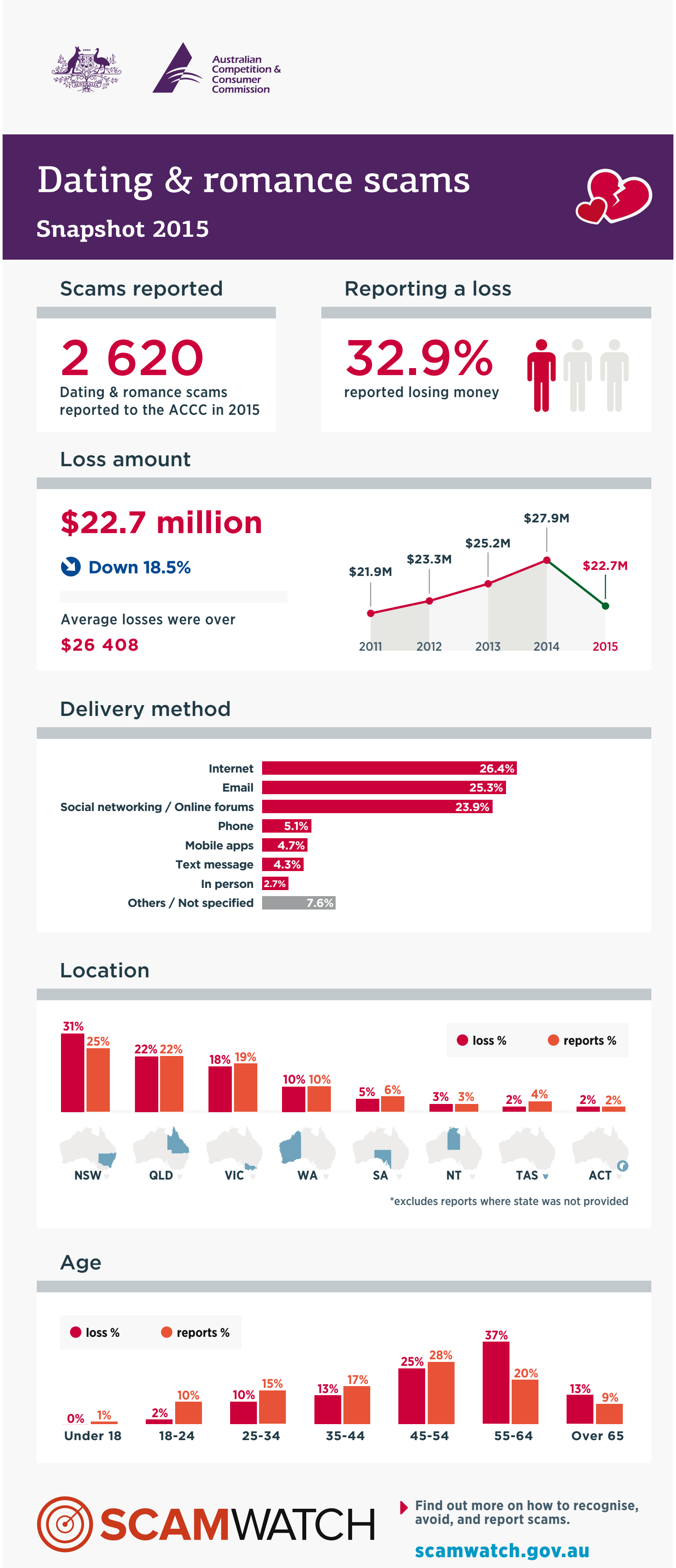
Scammers use a number of different approach methods to contact their victims. They will often use legitimate dating websites before quickly moving the victim to other communication channels like emails, where they are less likely to be detected. Contact methods reported to Scamwatch show 26 per cent were online and 25 per cent by email.

Scammers are also targeting victims through social networking sites, where they ‘like’ them and then express shared interests based on personal information gleaned from their profile. Almost 24 per cent of dating scams reported meeting through social networking sites or online forums.

In 2015, the average reported loss from a dating and romance scam was just under $26 000. Around one third of victims reported losses over $10 000. With such a high return, it is not surprising that scammers are prepared to invest the time and energy into building a romantic connection.

Figure 6 is an infograph which provides an overview of dating and romance scams in 2015.

Figure 6: Dating and Romance scam infograph[12]



Australian Competition & Consumer Commission

Dating & romance scams

Snapshot 2015

Scams reported

2 620

Dating & romance scams reported to the ACCC in 2015

Reporting a loss

32.9%

reported losing money

Loss amount

$22.7 million

Down 18.5%

Average losses were over

$26 408

Delivery method

Location

*excludes reports where state was not provided

Age

SCAMWATCH

Find out more on how to recognise, avoid, and report scams.

scamwatch.gov.au

[12] This chart refers only to Scamwatch reports.

Victim's story: Marco's generosity shows no return

As a widower, Marco thought he would never find another partner and wasn't looking. One day when Marco logged into Skype to chat to his sister overseas, he was contacted out of the blue by 'Alana' who said she was seeking friendship. Against his better judgement, Marco decided to respond.

Alana claimed to be an American living in Ghana to look after her sick grandmother and studying to be a nurse. Marco had no intention of starting a relationship with anyone but decided to consider Alana a kind of pen-pal. Alana and Marco started to chat on a daily basis and seemed to get along very well despite the substantial age difference between them.

Their relationship grew but Marco kept his relationship with Alana to himself because he thought his family would not approve. He continued to chat and had concerns things were moving very quickly but Alana seemed genuine. Within a few months, the relationship became all-consuming for Marco. He would chat with Alana at least twice a day, sometimes for hours at a time. They had the odd fight just like a real couple but whenever Alana didn't chat to him for a day or two he would miss her enormously. He stopped visiting his local club quite as often and eventually not at all, losing contact with many dear friends. Alana sent more pictures which were increasingly intimate in nature.

When Alana asked Marco if she could come to visit him in Australia, Marco took this on as a personal project. He didn't care how much he sent to get her to Australia. He paid for Alana's airline tickets through a travel agent and a number of other fees such as a doctor who provided a medical certificate and a clerk at the local police station who provided Alana with a background check. Alana explained these were all standard steps for obtaining a visa to visit Australia. However, Marco found out later that all of these payments went to other scammers that were part of the scheme.

A few days before Alana was due to board a plane, Marco received an email claiming to be from a doctor at a hospital. The doctor said that Alana was in a car accident and that she urgently needed surgery. He was told that Alana had no identifying information and that the last person in her chat history on her laptop was Marco, so they were reaching out to him for payment before they could proceed. Marco paid the money as quickly as possible fearing Alana was fighting for her life.

No sooner had Alana recovered from her accident, she was again requesting money for her tickets being stolen. On another occasion, she allegedly made it to the airport but was held up by customs who claimed her police check was out of date and she could not travel unless she obtained another one. Excuse after excuse meant Marco paid more and more money. Over a period of several years, Marco had given away most of his retirement fund trying to get Alana to Australia.

In 2015, Marco received a letter from the ACCC warning him he might have fallen into a scam and inviting him to call and discuss the matter. He didn't respond but the letter confirmed for him what he had felt deep down all along. Alana wasn't real and despite the continuing requests for money, he had no money left to send.

'Don't let scammers use your charitable nature against you. Genuine and well-meaning people get drawn into scams in which they lose their money and themselves', ACCC Deputy Chair Delia Rickard.

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Do an image search of your admirer to help determine if they really are who they say they are. You can use image search services such as Google or TinEye.
2. Be alert to things like spelling and grammar mistakes, inconsistencies in their stories and other signs that it's a scam, like their camera never working if you want to Skype each other.
3. Be cautious when sharing personal pictures or videos with prospective partners, especially if you've never met them before. Scammers are known to blackmail their targets using compromising material.
4. Be wary of requests for money. Never send money, give banking details or copies of important personal documents to anyone you don't know or trust.

#3. Computer prediction software and sports investment schemes

Number of scam reports:
426

Per cent of total reported loss:
6.5%

Per cent of total scams reported:
<1%

Number of consumers reporting losses:
270

Total losses reported to Scamwatch:
$5 534 878

Scam conversion rate:
63%

Most affected age group:
45+ 76%

Gender:
Female: 27%
Male: 73%

Contact modes:
Phone 56%

In 2015, losses to computer prediction software and sports investment schemes reduced by 39 per cent from $9 million to $5.5 million dollars. This was accompanied by a slight reduction in reports. However, the conversion rate grew a further 10 per cent to 63 per cent, meaning more people lost money but in smaller amounts.

Computer prediction software and sports investment schemes often follow a simple formula, where they call victims and claim that they have software which can predict sporting events, financial markets or share price movements. They will then attempt to sell the software, a subscription to use the software or attempt to convince the victim to invest in a fund managed by the scammers. Often these calls involve claims of guaranteed and high returns.

People who have been approached with offers of such schemes have reported that the software or system does not work at all or does not operate as promised. Generally very low or no returns are received and if the company does claim a profit has been generated, it is impossible to get the money out of the scheme. After a period, investors report that the company can no longer be contacted and refuses to deal with its problems. Eventually the bogus company disappears without a trace.

Any claims of accurately predicting sports outcomes or stock market movemnets should be treated with extreme caution.

Victim’s story: Sure fire winner backfires

Steve was at home sick one day when he received a phone call from a telemarketer. He usually hung up on telemarketers but this one seemed different. The man on the line was very well spoken and told Steve about an investment opportunity which required a small upfront commitment but has yielded great returns for his other clients. Steve was told that for just $5,000 he could buy a licence to a computer program which is connected to a sophisticated server and successfully predicts the correct winner in sporting events 68 per cent of the time. This would mean that in the long run, if Steve followed the recommendations generated by the computer program, and made careful, controlled bets he would come out on top.

This seemed too good to be true, but the telemarketer explained the system in terms that appeared logical and realistic. The system would automatically make small bets on a broad range of international sporting events 24 hours a day. Steve was also told that the company selling this program could not use it to make enormous profits themselves due to government regulations but they were able to sell licences. If he didn’t like it, he could ask for a refund within the first month and get all of his money back.

Steve cautiously made the payment of $5000 and was sent a login and password for a website which hosted the betting prediction system, along with $500 bonus credit to get him started. He set the system to make bets automatically and left it overnight. The next day he logged in and the system showed his $500 had turned into $680. Steve made a withdrawal of $100 to see if he could get his money back as promised and, after a few days delay, $100 landed in his bank account.

Steve was now totally convinced that the system truly worked. Over the next two weeks, he put more and more money into the system and when he logged in, it always showed that while some bets failed, over all he was coming out on top. After a month, the system stopped updating. He tried to call the business to ask if there was some kind of error but he couldn’t get through to anyone. Steve sent emails with no response until finally his emails just returned with status ‘undeliverable’. Like his money, the company had vanished.

‘No matter how impressive the sales pitch, there is no such thing as a sure bet,’ACCC Deputy Chair Delia Rickard.

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Be wary of high pressure and slick sales techniques. Do not let anyone push you into making decisions about money or investments —always get independent financial advice.
2. If you receive a call from a salesperson trying to sell you a sports investment ‘opportunity’— just hang up.
3. Don’t be enticed by reports of past performance or graphs showing high returns. Scammers lie!
4. Remember: no one can guarantee that you will make money by gambling.

#4. Nigerian scams

Number of scam reports:
980

Per cent of total reported loss:
5%

Per cent of total scams reported:
1%

Number of consumers reporting losses:
141

Total losses reported to Scamwatch:
$4 549 807

Scam conversion rate:
14%

Most affected age group:
55+ 70%

Gender:
Female: 55%
Male: 45%

Contact modes:
Email 56%

In 2015, this classic scam continued to attract victims who parted with just over $4.5 million, doubling on 2014 numbers. This growth was largely due to a few large individual losses and overall has a relatively low conversion rate, suggesting that most of us are aware of these scams and their methods.

Originally many of these scams emanated from Nigeria and are sometimes referred to as '419' scams, taken from the section of the Nigerian Criminal Code outlawing the practice. In reality, the scams can come from anywhere in the world.

These scams are a form of advance fee fraud in which the scammer claims they have some money, often an inheritance or funds left behind by a corrupt politician, but they are unable to access it due to legal issues or some type of local conflict. Often the story will reference real world events. The scammer claims they are desperately looking for someone to provide bank account details so they can offload the money to a safe country and they will share the wealth when it is safe.

Like any upfront fee scam, the scammer soon asks for money to be paid before the transfer can be processed. These usually come in the form of requests to pay fake taxes, bank fees or as proof required by foreign 'anti-terrorism and money laundering laws'. The scam will progress to introduce a number of characters such as lawyers, bankers and government officials, all of whom require payment before the funds can be released.

Victim's story: Ann threw good money after bad until it was too late

Ann received an email from an unknown sender and was about to delete it when the title grabbed her interest. 'Transfer approval—Robert Jones'. Judging by the subject line, this email appeared to have gone to the wrong person.

Ann opened the email out of curiosity to see what it was about. The email appeared to be about a money transfer to someone regarding the transfer of $560 000 in relation to an oil pipeline project. The email claimed that it was the final attempt to shift the money and that the initial offer of a 15 per cent commission ($84 000) was still on the table. If 'Robert Jones' didn't respond, another 'partner' would be sought. The email also explained a complicated procedure which required the 'partner' to 'host' the money for tax purposes in their bank account. The explanation sounded complex but the role of the 'partner' was to hold the money in order to avoid excessive taxes in Nigeria. Ann thought that perhaps she had stumbled upon a once in a lifetime stroke of luck and she might be able to put her hand up as a 'partner'.

Ann responded to the email asking for more information and quickly got a response stating the mail was supposed to go to 'Robert Jones' but now he was too late and that it was very fortunate that Ann could become a 'partner'—she just had to meet a few basic criteria. The only catch was that the process required Ann to pay a small fee to the oil company to 'register as a partner'. Ann thought that a fee of just a few hundred dollars to collect $84 000 seemed like a good idea and if it turned out to be a scam, she would have only lost a small amount. When Ann paid the 'fee', the scammers thanked her and promised the money was on the way, only to inform her a few days later that she needed to pay another fee. The scammers asked for a series of fees and taxes, but promised to increase the commission to 17.5 per cent and later to 20 per cent.

The scammers had convinced her it was all real and shown her the money sitting in an account with her name. It just wasn't accessible until she paid yet another fee for some strange anti-terrorism and money laundering certificate. She truly thought that in the very near future she would come into a sum of money that would change her life.

Ann had invested so much money she couldn't afford to cut her losses. Unfortunately, she only realised just who she was dealing with when she had sent all her savings and the scammers demanded she borrow money off friends and family and threatened to expose her if she didn't.

'If you receive an email offering you a large sum for your help and a small fee, delete it. It is a scam,'ACCC Deputy Chair Delia Rickard

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Never send money or give credit card details, online account details or copies of personal documents to anyone you don't know or trust and never by email.
2. Do not agree to transfer money for someone else. Money laundering is a criminal offence.
3. Remember there are no get-rich-quick schemes: if it sounds too good to be true, it probably is.
4. Avoid any arrangement with a stranger that asks for up-front payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. It is rare to recover money sent this way.
5. If you think you have provided your account details, passport, tax file number, licence, Medicare or other personal identification details to a scammer, contact your bank, financial institution, or other relevant agency immediately.

#5. Inheritance scams

Number of scam reports:
3 775

Per cent of total reported loss:
5%

Per cent of total scams reported:
3.6%

Number of consumers reporting losses:
78

Total losses reported to Scamwatch:
$4 391 630

Scam conversion rate:
2%

Most affected age group:
55+ 79%

Gender:
Female: 54%
Male: 46%

Contact modes:
Email 43%
Mail 42%

Inheritance scams have a very low conversion rate but represent over $4.3 million in losses. While many scams are moving into digital channels, the classic approach of sending a letter is still a common method of delivery. Scammers using letters to target their victims accounted for 50 per cent of all losses in this category and 42 per cent of reports in 2015. Email accounted for 35 per cent of losses and 43 per cent of reports.

In either case, the initial letter or email will claim to be from a lawyer or banker, usually in Europe, who has a late client who happened to share the same surname as the recipient, or in the case of a banker is aware of an unclaimed account. The letter states the scammer has been searching for a genuine heir to the money but has been unsuccessful and the money will be lost if they fail. The scammer will then suggest that the victim can stand in as they have the same name as the deceased but in order for the process to appear legal, a series of fees and taxes must first be paid by the successor.

The very low conversion rate suggests that most people who receive these letters or emails dismiss them. However, those who consider the offer seriously and send money often lose significant amounts averaging more than $50 000 each.

This scam is often accompanied by requests for personal information under the pretext of filing paperwork to claim the inheritance. These can include photocopies of passports, bank account details, tax file numbers and Medicare numbers leaving victims vulnerable to identity theft.

Victim Story: The only thing John inherited was a debt

John had heard a lot about scams on the internet. He has an email filter active on his email account that gets rid of hundreds of spam and scam emails every month. He also makes sure to never give away his details to strangers online. However, when he received a letter supposedly from a barrister from Portugal he didn't apply the same scepticism.

The letter appeared legitimate because of its professional looking letterhead and a stamp with a seal from the 'European Barrister's Association'. The letter informed him that a distant relative had recently passed away and that since no legal heir could be found locally, they were searching overseas. The surname was the same and the letter stated that John was the closest relative they could find. It was an unusual surname and if it was true, John stood to inherit $23 million dollars.

The letter appeared well written and John did recall an uncle once telling him something about the history of their family in Europe. Since John had just turned 75, perhaps he really was the oldest living relative of the family. John cautiously responded to the letter by sending an email to the address provided. The 'barrister' replied to John and told a convincing story about the inheritance being real. All John had to do was to comply with a few local laws that required proof of his identification and some minor fees.

John sent his information and paid the fees to the lawyer, only to find that various complications meant he needed to pay more. The barrister told John the bank in Spain where the money was being held refused to release the money unless John paid for its release, but that his contact there could sort it out. John was later told that the money was now being held by customs officials in Brussels and a tax was required to approve its transfer out of Europe. The barrister claimed he would travel there personally to sort it out but needed some money to help cover expenses.

John was kept on the hook with promises that the inheritance was just one more payment away. However, within a few months he had sent over $20 000 to three different countries and eight different names. When John started to question the barrister about all these issues, the barrister became aggressive and told John he would be a fool to back out of the deal after coming so far.

Eventually John finally stopped sending money after his family intervened but not before sending over $45 000 in total. Some of this he had borrowed against the family home. Having provided a wealth of his details to scammers, he was now also receiving more scam emails and letters than ever.

'Scammers use a multitude of techniques, embrace all modes of communication and operate using sophisticated networks across multiple jurisdictions to hide their activity. Staying alert and being cautious to any suspicious offer or proposal is the key to avoiding scams,' ACCC Deputy Chair Delia Rickard.

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Avoid any arrangement with a stranger that asks for up-front payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. It is rare to recover money sent this way.
3. Seek advice from an independent professional such as a lawyer, accountant or financial planner if in doubt.
4. Do an internet search using the names or exact wording of the letter/email to check for any references to a scam —many scams can be identified this way.
5. If you think it's a scam, don't respond—scammers will use a personal touch to play on your emotions to get what they want.
6. Remember there are no get-rich-quick schemes: if it sounds too good to be true, it probably is.

#6. ID theft involving spam or phishing

Number of scam reports:
9328

Per cent of total reported loss:
2.1%

Per cent of total scams reported:
9%

Number of consumers reporting losses:
318

Total losses reported to Scamwatch:
$1 816 361

Scam conversion rate:
3%

Most affected age group:
18-24 41%

Gender:
Female: 54%
Male: 46%

Contact modes:
Phone 55%
Email 31%

In 2015, losses reported to Scamwatch for identity theft involving spam or phishing were $1.8 million but actual losses are known to be significantly more. Reports to ACORN show online hacking and identity theft losses of more than $28 million. The Attorney-General's report, Identity Crime and Misuse in Australia 2013-14, says identity crime continues to be one of the most common crimes and estimates that the annual economic impact of identity crime exceeds $2 billion.[13]

Although this scam type only has a three percent conversion rate, identity theft can result in significant monetary losses and its consequences can take months or even years to repair, especially if it affects a person's credit rating.

While these approaches might not directly ask for money or banking information, they provide a scammer with a wealth of other information which can later be used for highly targeted and more sophisticated scam attempts. The misuse of personal information underpins many of the scams reported to Scamwatch including: the creation of fake profiles in dating scams; using an unusual surname to lure a victim into an inheritance scam; or even just to give some credibility to a reclaim scam to make someone think they are truly entitled to a rebate. The business email compromise scam is a classic example where a business's information is misused to deceive a company into redirecting payments to scammers pretending to be legitimate suppliers (see further discussion at page 23).

Scammers use a variety of techniques and approaches to obtain personal information from unsuspecting victims. A common approach reported in 2015 involves scammers imitating telco companies asking for personal details over the phone. The scammers tell people that there has been an error on their account and they need to confirm their personal details to ensure its security. In the course of such calls, a skilled scammer might extract a full name, date of birth, bank account details and a driver's licence number. These details can then be used to access online bank accounts or to attempt a range of fraudulent activity, like taking out loans or credit cards in your name.

Another common approach involves an email with an offer of discounts or gift vouchers for major Australian retailers for simply completing a survey. Everyone should be aware of the importance of keeping their personal details secure, and carefully consider who they give this information to.

Fraud Week 2015 focused on ID theft and encouraged Australians to get smarter with their data. The initiative pointed out that whilst there are times when personal details are required for legitimate reasons, such as signing up to a new service or shopping online, everyone should stop and think twice before providing such information.

[13] See: https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Trends-in-Identity-Crime.aspx.

Victim Story: Betty's holiday plans unravel

Betty was 68 years old and living comfortably but carefully on her retirement funds. She liked to travel and promised herself a holiday when she retired but just hadn't quite managed to save enough. In fact, all she had done about the holiday was get a new passport. When Betty was browsing the internet, she came across a competition to win a holiday and thought to herself that this might just be the lucky break she needed.

To enter the competition, Betty was required to complete an entry form that asked her questions about her travel preferences together with a lot of personal details. This included her bank account details and a copy of her passport. The entry form explained that bank details were required in the event she won the prize that included spending money of $5000. The details would let the company transfer winnings to her nominated account and a photocopy of her passport was required so her flights could be booked straight away. Betty thought it was all just a part of a legitimate consumer survey and the explanations seemed genuine. The competition also required her to create a username and password to access the survey. Betty used the same password she uses for all her online accounts—it was easier to remember that way. She submitted her details and entered the competition.

A month had passed by and Betty had forgotten all about the competition. That was until she was contacted by her bank who advised her of suspicious activity on her account. The bank informed her that a series of out of the ordinary transfers were being made to overseas accounts. The bank also informed her that a new credit card had been ordered and was already $3000 in debt.

The bank asked if Betty had provided her bank account details or password to anyone recently and she realised it must have been the competition she impulsively entered. The bank cancelled the credit card and attempted to reverse the latest transactions but was unable to retrieve Betty's money. In the few months since providing her personal details to the scammers, they had hacked into her bank account, taken most of her savings and were clearly using her identity to create new credit cards.

'Your personal data is a valued commodity—and one that you cannot put too high a price on when it comes to protecting it. Unfortunately, scammers also recognise the value of your personal information and will go to great lengths to steal it,' ACCC Deputy Chair Delia Rickard.

*All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Be very careful about how much personal information you share on the internet or through social networking sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.
2. Do not click on any links or open attachments from emails claiming to be from your bank or another trusted organisation and asking you to update or verify your details—just press delete.
3. If in doubt, independently source contact details and do not use those provided. Call and check using details you get from the phone book, past bill or your banking cards.
4. Do an internet search using the names or exact wording of the email or message to check for any references to a scam—many scams can be identified this way.
5. Look for the secure symbol. Secure websites can be identified by the use of 'https:' rather than 'http:' at the start of the internet address, or a closed padlock or unbroken key icon at the bottom right corner of your browser window. Legitimate websites that ask you to enter confidential information are generally encrypted to protect your details.
6. Choose passwords that would be difficult for others to guess, and update them regularly. Don't use the same password for every account, and don't share them with anyone.

#7. Fake trader websites

Number of scam reports:
2735

Per cent of total reported loss:
1.7%

Per cent of total scams reported:
2.6%

Number of consumers reporting losses:
1587

Total losses reported to Scamwatch:
$1 458 858

Scam conversion rate:
58%

Most affected age group:
25–44 66%

Gender:
Female: 57%
Male: 43%

Contact modes:
Internet 50%
Email 23%

In 2015, Australians reported losses of almost $1.5 million to fake trader websites.

This scam generally affects a younger demographic of people who are confident shopping online. The reality is that scammers are able to create very convincing versions of legitimate retail websites using exceptional offers at prices too good to be true.

Reports indicate that fake trader scams spike in the last quarter of the year with almost 50 per cent of losses occurring from September to December. It is not surprising that scammers take advantage of Christmas spending and target savvy internet shoppers looking for an online bargain.

As has been seen with other scams, scammers are also using social media to find victims. Scam Facebook pages offering unbeatable prices on popular fashion, beauty products, jewellery and even puppies were reported to the ACCC in 2015.

If you find a bargain online, check carefully before you provide banking details or pay by credit card. Sending money via wire transfer or other unusual payment method is often a tell-tale sign of a scam.

Victim Story: Online rental accommodation might not always be cheaper

Chelsea had been searching online for a holiday home rental in Rockhampton at a reasonable price but availability was limited and she was finding it difficult to find anything. She entered her name and email on a few sites to express her interest for several rentals but didn't get any response.

A few days later she received an email from what appeared to be a well-known website that advertises holiday accommodation.

Chelsea followed the link provided in the email and was directed to a professional looking webpage that advertised a suitable holiday home for a great price at just the right time. This was much cheaper than any of the other places she had been looking at.

Keen to secure the house for the dates of her trip, she made a booking on the spot and paid the entire amount upfront on her credit card.

Two weeks passed and Chelsea did not receive any confirmation of her booking, though the funds had been deducted from her bank account. She performed a Google search to get a phone number for the booking company and called them to follow up on her reservation. Chelsea was advised that there was no record of a booking in her name. The address of the holiday house in Rockhampton she thought she had booked turned out to be a vacant milk bar and its address had never been listed on the website.

It soon became clear to Chelsea that she had been scammed. The email was not sent by the legitimate company and the link had directed her to a fake website. Lucky for Chelsea, she was able to get a chargeback from her bank because she had used her credit card.

Looking back on it, there were signs Chelsea missed in her excitement to seal the deal: the email contained a number of spelling mistakes and was poorly worded and the sender used a personal email address, not a company address associated with the legitimate booking company.

'When making online payments, only pay for items using a secure payment service—look for a URL starting with 'https' and a closed padlock symbol or use a payment provider such as PayPal,'ACCC Deputy Chair Delia Rickard.

*All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Avoid any arrangement that asks for up-front payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. It is rare to recover money sent this way.
2. Check if the site has a refund or returns policy, and that their policies sound fair. The better online shopping and auction sites have detailed complaint or dispute handling processes in case something goes wrong.
3. When using retail websites, find out exactly who you are dealing with. If it is an Australian company, you are in a much better position to sort out the problem if something goes wrong.
4. When buying from an online classifieds website, only pay when you have physically inspected or received the goods. If you have any doubts about the product or the person selling it, don't go ahead with the deal.
5. When using online auction websites, check all comments about the seller you are considering buying from. Never trade outside of the auction website.
6. Do an internet search to see what others have said about a website you're interested in. Use exact phrases from the website or the internet address to do the search.

SCAMWATCH

Don’t let fake sellers ruin Christmas

In December 2015, Scamwatch warned Australian consumers to beware of fake sellers in the lead up to Christmas.

Those shopping online were alerted to an increase in fake online sellers looking to cash in on the festive shopping season. A key warning sign to look out for is the method of payment offered by the seller. Wire transfers, pre-loaded debit cards and even bitcoin are favoured by many scammers. Because they are rarely used by legitimate retailers, these payment methods should be a warning that it might be a scam.

Consumers should always take care to find out exactly who they are dealing with and consider the benefits of buying from a reputable, local retailer, either in-store or using their online facilities. Your ability to resolve issues should things go wrong are far better with reputable brands you know and trust.

Read more at www.scamwatch.gov.au.

#8. Unexpected prize & lottery scams

Number of scam reports:
3683

Per cent of total reported loss:
1.6%

Per cent of total scams reported:
3.5%

Number of consumers reporting losses:
258

Total losses reported to Scamwatch:
$1 337 296

Scam conversion rate:
7%

Most affected age group:
65+ 80%

Gender:
Female: 55%
Male: 45%

Contact modes:
Email 31%
Text message 24%

Unexpected prize and lottery scams have a low conversion rate of just 7 per cent. This means that most people approached with an email or text message claiming they have won something see it for the scam it is. However, sometimes when people find themselves in financial difficulty or down on their luck, the promise of a windfall can seem too good to pass by.

Many victims of unexpected prize scams are initially sceptical but tell themselves they will just pay once to see what happens. They think that, at worst, they might lose a relatively small sum but if true, they could become instant millionaires. This way of thinking can lead to a spiral of paying just one more fee until they become more and more invested in the scam and have greater expectations that their investment will pay off. Even if only one payment is made to a scammer, this still means money is being sent to criminals who will be encouraged to attempt the scam on others.

An alarming statistic from 2015 is that the majority of losses (80 per cent) for this scam were suffered by those aged 65 and over. At a time when most Australians are entering retirement and living off a lifetime of savings, some are losing significant amounts to scammers. In 2015, 23 people reported spending more than $10 000 each in pursuit of lottery winnings that never existed.

Victim's story: Matthew's second 'prize'

Matthew received a letter in the mail from a Malaysian company that contained two scratchie lottery tickets ('scratchies'). At first Matthew was suspicious because businesses don't usually send people scratchies. However, after scratching one of the tickets to uncover the words 'try again', Matthew felt the tickets were just some advertising gimmick. He then scratched the second ticket to reveal he was the winner of the second prize worth $50 000.

Matthew followed the instructions on the winning scratchie and phoned an overseas number to claim his prize. Matthew was congratulated on his win and told that it was a real prize and that he was a few steps away from collection. He was informed that he would need to pay a small upfront fee of $450 to cover transfer costs. Once this was paid, he would receive the money into his nominated account for which he provided details. Given the large sum of money Matthew was expecting to receive, $450 seemed reasonable so he paid the amount.

The next day, Matthew was contacted and asked for a further payment of $300 for tax-related fees. He was told that the amount could not be subtracted from the winnings for complex legal reasons. Matthew reasoned that since the transaction involved an international transfer of prize winnings, the need to pay tax-related fees was probably true. He was also asked to send some personal information such as a copy of his driver's licence to prove his identity to the tax office. He paid the $300 and sent the personal information.

Over the next few days, Matthew made four more payments of varying amounts—each time believing it would be the last. Before he knew it, he had made payments totalling $3000.

Looking back, Matthew realised he had been scammed. The scratchies weren't genuine and there was no real prize money to be won.

'If someone asks you to pay money up-front in order to receive a prize or winnings, it's almost always a scam,'ACCC Deputy Chair Delia Rickard.

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Do an internet search using the names or exact wording on the scratchie card to check for any references to a scam—many scams can be identified this way.
2. Remember: you cannot win a lottery or competition unless you entered it.
3. If someone asks you to pay money up-front in order to receive a prize or winnings, it's almost always a scam. Legitimate lotteries do not require you to pay a fee to collect winnings.
4. Be careful of competitions that use phone numbers beginning with '190'. These are charged at a premium rate (sometimes even for receiving a message) and can be very expensive.
5. Never send money or give credit card details, online account details, or copies of important personal documents to anyone you don't know or trust and never by email.

#9. Reclaim scams

Number of scam reports:
12 589

Per cent of total reported loss:
1.6%

Per cent of total scams reported:
12%

Number of consumers reporting losses:
187

Total losses reported to Scamwatch:
$1 331 063

Scam conversion rate:
1.5%

Most affected age group:
55+ 55%

Gender:
Female: 61%
Male: 39%

Contact modes:
Phone 68%

In 2015, Australian consumers were hit with a number of reclaim scams resulting in 12 589 reports and over $1.3 million in losses. This is an increase from the $980 165 reported lost in 2014.

Reclaim scams usually involve a phone call from someone claiming to be a government or business representative stating that due to some error, you are owed money. The scammers may claim to be from the Australian Taxation Office or perhaps a made-up department like the 'Reclaims Department'. However, in order to claim the money, a fee must be paid upfront for 'administration' or 'legal costs'. Once this is paid there is no getting it back and often the scammer will try to obtain personal information in the process of 'processing the claim' which can later be used for identity theft.

A more recent twist to this scam involves the use of threats, which could be fines, arrests, cancellation of benefits or even deportation, which was used in an immigration variation of this scam. The scam usually involves the scammer posing as a government official and cold calling people. Several reports to the ACCC described the caller stating that unless immediate action was taken to make a payment, a police car would be sent to arrest them.

Thankfully this scam has a very low conversion rate of only 1.5 percent, which means most people can identify it as a scam and do not lose any money. However, scammers still see value in continuing this scam because even though only a small percentage pays, their intimidating tactics still yield significant returns. The use of cheap telecommunications facilities such as voice-over internet protocol means the scammers can make more calls and not worry if the vast majority of Australians hang up on them. The returns from the 1.5 per cent who do pay more than adequately cover their costs.

Victim's story: Anthony trusted his better judgement and avoided a scam

Anthony received a phone call on his landline from a person claiming to be from well-known legal firm. The scammer advised Anthony that due to overcharged bank fees going back a number of years, the law firm had successfully taken a class action against his bank and Anthony was now eligible to a refund of $4000. Anthony thought he recalled hearing something like that on the news and stayed on the phone to find out more.

Anthony was asked to confirm his full name and address so that his identity could be verified. The scammer seemed to know these details, stating his personal information correctly.

The scammer then proceeded to inform Anthony that before the money could be released a routine payment of $250 was required for administrative fees. This required Anthony to send money overseas via a money remittance service. Anthony asked why an Australian government fee needed to be sent overseas and the scammer explained that the service was outsourced to a legal team overseas to save the Australian public money. Once Anthony had made payment he would need to phone the caller's supervisor on the number provided and the supervisor would finalise the transaction.

Anthony was struck with the thought 'Why can't the fees be deducted from the money I'm supposed to be receiving?' He also wondered why he would need to make a separate phone call to another person for the transaction to be processed. Anthony was now suspicious. He ended the call and visited the Scamwatch site to check if the phone call was legitimate.

Following advice he read on Scamwatch, Anthony contacted his bank using the telephone number on his bank statement. The bank advised him that there was never a class action and that the call was a well-known scam. Making the decision to stop and check when he was unsure, saved Anthony losing money to the scammers.

'If you receive a phone call out of the blue from someone claiming to be from a government department, take their details and check against information you source independently,' ACCC Deputy Chair Delia Rickard.

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Verify the identity of the contact by calling the relevant organisation directly—find them through an independent source such as a phone book or online search. Do not use the contact details provided in the message sent to you.
2. Remember, government departments will never contact you asking you to pay money upfront in order to claim a fee, rebate or any other money that is yours.
3. Avoid any arrangement with a stranger that asks for up-front payment via money order, wire transfer or international funds transfer. It is tell-tale sign of a scam.
4. If you receive a phone call threatening arrest or a fine, hang up and contact the police.

#10. Job & employment scams

Number of scam reports:
2456

Per cent of total reported loss:
1.1%

Per cent of total scams reported:
2.3%

Number of consumers reporting losses:
246

Total losses reported to Scamwatch:
$952 742

Scam conversion rate:
10%

Most affected age group:
25-44 69%

Gender:
Female: 54%
Male: 46%

Contact modes:
Email 60%
Internet 14%

In 2015, Australians lost almost $1 million to job and employment scams. A common form of job and employment scam uses popular job search websites offering relatively easy, stay-at-home jobs advertised as 'administration' positions. The job description will often refer to 'managing customer accounts'. Victims are sent forms to fill out and contracts to sign, which gives the fake job an air of legitimacy and allows the scammer to gather personal information at the same time. In reality, these are money laundering schemes requiring the victim to move money through their personal bank account to an overseas account. This is an illegal activity and could result in legal action being taken against you.

Other employment-related scams may require you to do something simple such as stuffing envelopes or assembling a product using materials that you have to buy from the 'employer'. To accept the job, you will be asked to pay for a starter kit or materials relevant to the job or scheme. If you pay the fee, you may not receive anything or what you do receive is not what you expected or were promised. For example, instead of a 'business plan', you may be sent instructions for how to get other people to join the same scheme.

Last year also saw a number of reports regarding working visa scams targeting foreign students seeking work in Australia and foreign workers looking to obtain working visas. These scams generally involved job seekers being fed incorrect information about how to obtain a visa and how to pay for one. Not only do victims lose money but they also give away a wealth of personal information.

> Money laundering is a key risk to Australia—it is the common element in almost all serious and organised crime. Money laundering enables criminals to hide and accumulate wealth, avoid prosecution, evade taxes, increase profits through re-investment and fund further criminal activity.
>
> Recent estimates by the Australian Crime Commission suggest that the level of money laundered in and through Australia is at least $10 billion a year. However, the full cost of money laundering to the Australian community is likely to be much higher when lost tax revenues and the full scope of unreported proceeds of crime is taken into account.[14]

[14] See https://crimecommission.gov.au/publications/intelligence-products/crime-profile-fact-sheets/money-laundering.

Victim's story: Work at home scheme not what it seems

Peter retired five years ago and was managing his retirement funds but thought he could do with a little extra income to fund some travel. He had worked hard for 50 years and found it difficult to get through a day finding enough to keep himself busy. When Peter saw an advertisement on a job seeking website offering a few hours of work at home for a tidy wage, he thought this would be just the ticket.

Peter applied for the position by sending a resume including his phone number, address, full name and other personal details. The scammers replied to Peter a few days later stating that after a competitive recruitment process he had won the position. He was directed to set up a bank account in his name which he could use to handle 'customer accounts' and to provide his new 'employer' with log in details so they could provide him feedback on his performance.

Peter set about diligently making the 'transfer orders' as they came in. Over the next few months, Peter moved over $10 000 in small amounts to various accounts as ordered by the scammers, each time making a small commission. The transfer orders came via emails in attachments which Peter opened without giving it a second thought. Peter didn't realise that the money he was moving came from the criminal proceeds of overseas organised crime gangs, and that the attachments he was opening had installed a key logger on his computer which captured every keystroke he made on his keyboard. Eventually, the transfer orders started to come less and less often and then dried up completely.

Peter then noticed that his personal bank account had been accessed and $32 000 was extracted and moved overseas in small amounts over the space of two days. The scammers had used the key logger to capture Peter's bank account password and logged into it, changing the daily withdrawal limit as well as the mobile number that the bank uses to send an SMS with the verification code for overseas money transfers.

In the end, Peter lost $32 000 of his own money, a wealth of his personal information and helped criminals clean their dirty money.

'Don't get involved with any job offers that require you to pay money upfront or move money between accounts,' ACCC Deputy Chair Delia Rickard.

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Be suspicious of unsolicited 'work from home' opportunities or job offers, particularly those that offer a 'guaranteed income' or require you to pay an upfront fee.
2. Never agree to transfer money for someone else—this could be money laundering which is illegal.
3. If the job involves making or selling a certain type of product or service, find out if there is really a market for it.

6. Research

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

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

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

6.1 Australian Institute of Criminology research

The Australian Institute of Criminology (AIC) released two scam-related pieces of research in 2015. The first examined identity crime, while the other study reported on online fraud.

Identity crime and misuse in Australia: results of the 2014 online survey

In 2014, the AIC was commissioned by the Attorney-General's Department to undertake another national survey concerning identity crime and misuse as part of the National Identity Security Strategy. The report, released in September 2015, built on the previous year's work in this field.

> 'The results of this survey confirm prior research that misuse of personal information remained a continuing problem in Australia in 2014, with one in five survey respondents reporting misuse at some time in their lives. .. [M]ore than half had experienced financial losses for which they were not compensated. In addition, they experienced a range of non-financial losses including loss of personal time, as well as mental and emotional consequences, sometimes requiring treatment. Victims also indicated changes in their personal and online behaviour as a result of their experiences, thus detracting from the positive benefits of online consumer activity.'[15]

Australasian Consumer Fraud Taskforce: Results of the 2013 online consumer fraud survey[16]

The Australian Institute of Criminology (AIC), as a member of the ACFT and chair of the research subgroup, holds an annual consumer fraud survey to:

- obtain a snapshot of the public's exposure to consumer fraud and scams,
- assess their impact; and
- determine how victims respond and to identify emerging scam typologies.

The findings are then used to inform fraud prevention activities.

Based on findings from the 2013 survey, the AIC's report, released in February 2015, developed recommendations for future education and awareness campaigns. It was suggested that future campaigns should focus on:

- developing a greater understanding of the consequences of consumer fraud, not just the financial impact, but the psycho-social aspects and the lasting effects that falling victim to a scam may have;
- changing the perception that scams (a type of consumer fraud) are not victimless crimes and victims are not necessarily gullible, greedy or doing something illegal;
- educating the public on what to do if they have been the victim of a scam or if they are receiving a large amount of scam invitations. The survey has continually found that respondents are unaware of to whom they should report consumer fraud.[17]

[15] Identity crime and misuse in Australia: Results of the 2014 online survey, http://www.aic.gov.au/publications/current%20series/rpp/121-140/rpp130.html

[16] Australasian Consumer Fraud Taskforce: Results of the 2013 online consumer fraud survey, Australian Institute of Criminology, February 2015

[17] Ibid, p. 26.

6.2 Attorney-General's Department: Identity security

On 9 September 2015, the Minister for Justice and Minister Assisting the Prime Minister for Counter-Terrorism, the Hon Michael Keenan MP, released the report *Identity Crime and Misuse in Australia 2013-14.* A copy of the report can be found at www.ag.gov.au.

The report was developed by the Attorney-General's Department in collaboration with the Australian Institute of Criminology (AIC), and in consultation with a range of relevant government agencies, under the auspices of the National Identity Security Strategy.

> 'The report indicates that identity crime continues to be one of the most common crimes in Australia. Estimating that the annual economic impact of identity crime exceeds $2 billion, the report also supports findings from the Australian Crime Commission that identity crime continues to be a key enabler of serious and organised crime.'[18]

6.3 Australian Bureau of Statistics' personal fraud survey

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

"In the 12 months prior to interview in 2014–15, an estimated 1.6 million Australians experienced personal fraud, or 8.5 per cent of the population aged 15 and over. This is an increase from the proportion of persons who experienced personal fraud in 2010–11 (6.7 per cent)."[19]

[18] https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Trends-in-Identity-Crime.aspx

[19] See: http://www.abs.gov.au/AUSSTATS%5Cabs@.nsf/0/1FF970676E24FDFECA2574740015CA71?Opendocument

7. Education and awareness raising initiatives

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

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

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

This chapter outlines ACCC initiatives to help the Australian community protect themselves from scams.

7.1 Scamwatch

The Scamwatch website (www.scamwatch.gov.au) seeks to educate the public on how to recognise and avoid scams, as well as providing advice on what to do if they have been scammed. It also acts as a portal for the public to report scams.

In July of 2015, the ACCC launched the new Scamwatch website with improved presentation and accessibility for users. A new key feature of the site is the capacity to access information on the type, quantity and losses due to scams being reported to Scamwatch.

A survey was conducted after the launch with users responding positively to the fresh presentation, usability and currency of information on the site. There has also since been an increase in traffic in 2015 with the website receiving 1 556 384 unique visits, an increase of 219 515 or 16 per cent from 2014. Figure 7 shows that Scamwatch visits have consistently increased since the ACCC assumed responsibility for the site in 2006, with a doubling of visits since 2011.

Scamwatch visitors were predominantly located in Australia. However, people located around the world also visited the website, including from the United States, United Kingdom and Canada.

Figure 7: Unique visitors to the Scamwatch website from 2006 to 2015

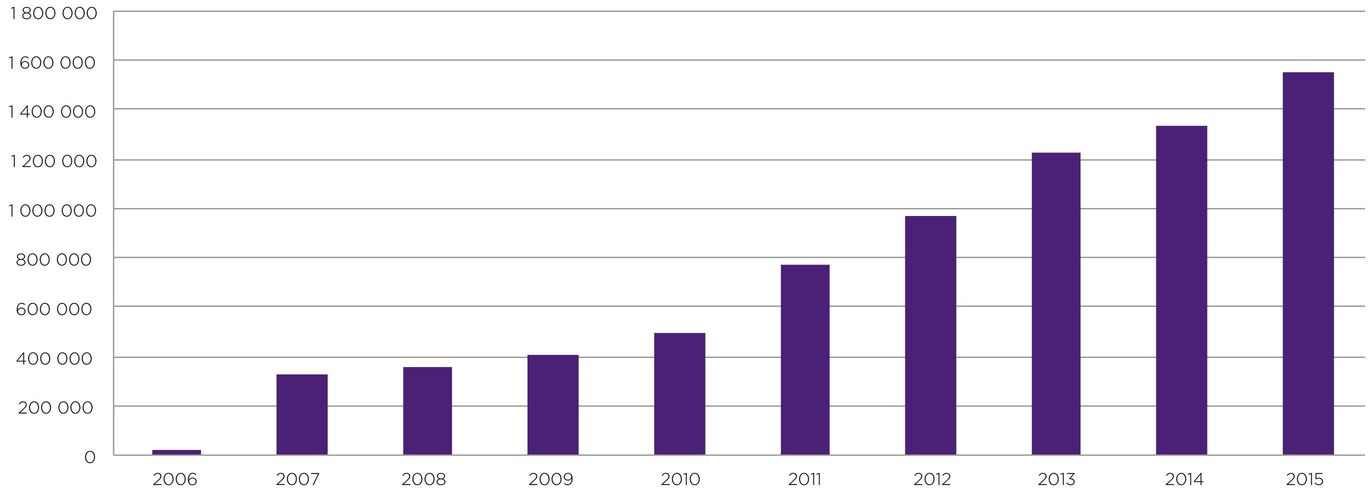
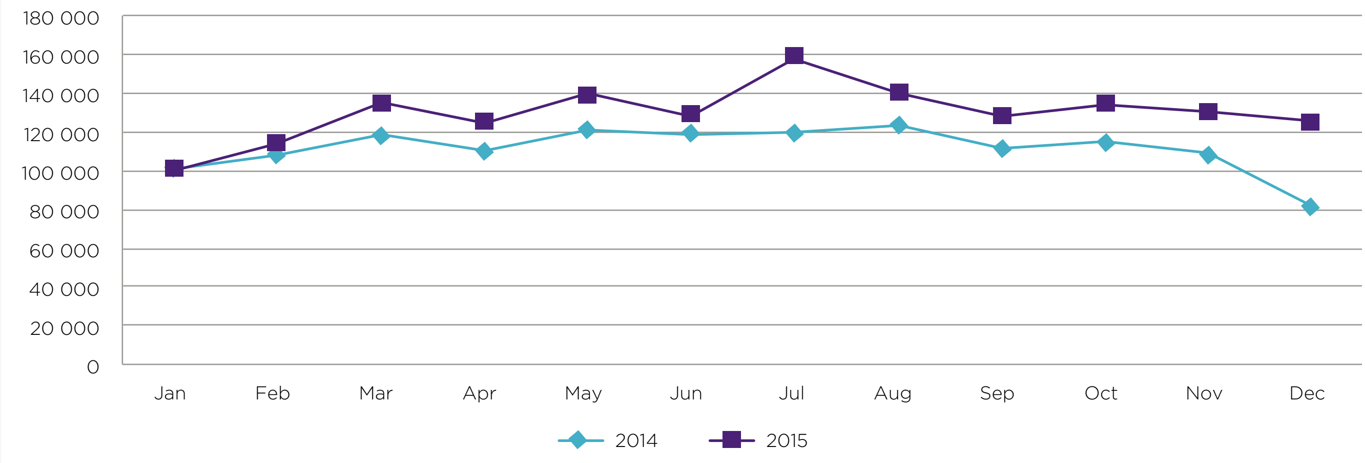


Figure 8 shows that in 2015 Scamwatch attracted on average more unique visits per month compared to 2014, with a significant increase in visits in July as a result of the launch of the new website. Typically, unique visits to the Scamwatch site decline over the Christmas period and this has been a consistent trend over a number of years.

Figure 8: Comparison of monthly visits to the Scamwatch website in 2014 and 2015



Consumers and small businesses can also receive information and advice over the phone by calling the Scamwatch hotline.

Scamwatch has significant brand awareness amongst the community with the federal, state and territory government departments, media, consumer groups and private companies directing people to the website for information on scams.

Scamwatch also operates as the web portal for the Australasian Consumer Fraud Taskforce, promoting initiatives such as its annual National Consumer Fraud Week campaign. More information about the Taskforce is provided at section 8.1.

Scamwatch radar alert service

Scamwatch runs a free subscription service whereby subscribers receive email alerts, known as 'Scamwatch radars', on emerging scams.

In 2015 the subscriber network reached 38 241 subscribers, an increase of 6 per cent from 2014.

The ACCC issued 16 Scamwatch radars in 2015 to warn Australians about the imminent risk of scams, including those relating to current events such as Christmas, Valentine's Day and tax time at the end of the financial year.

A full list of Scamwatch radar alerts issued in 2015 is provided at Appendix 3.

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

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

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

Scamwatch Twitter(@Scamwatch_gov)

The ACCC also operates a Scamwatch Twitter profile: @Scamwatch_gov. This social media platform allows Scamwatch to reach consumers, small businesses and the media in real time as scams emerge and refresh warnings of existing scams.

In 2015, Scamwatch Twitter posted 238 tweets to its 9934 followers on the following topics:

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

Join the Scamwatch Twitter community

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

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

7.2 Other educational resources on scams

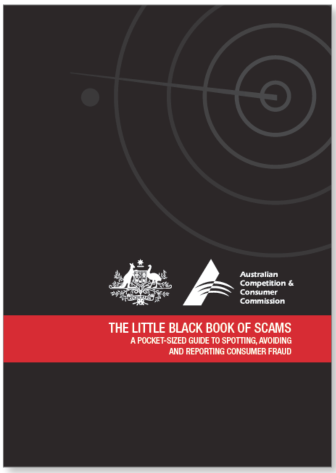
The ACCC has also produced a range of educational resources to educate consumers and small businesses about how to identify a scam and avoid being duped. Additional scam related resources for consumers and businesses are also noted in Appendix 4.

The Little Black Book of Scams

The ACCC's *Little Black Book of Scams* is its primary educational resource, and the ACCC's most popular publication. In 2015 over 235 000 copies of the book were distributed throughout the community. This is an average of over 19 000 copies per month. The electronic publication was also downloaded 4041 times.

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

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


Australian Competition & Consumer Commission
THE LITTLE BLACK BOOK OF SCAMS
A POCKET-SIZED GUIDE TO SPOTTING, AVOIDING AND REPORTING CONSUMER FRAUD

Small business scams factsheet launched

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

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

The factsheet was downloaded over 700 times in 2015.

7.3 Media and communications activity

The ACCC recognises the important role of the media in helping to raise community awareness about scams activity. In 2015, the ACCC continued to proactively generate media interest in scams targeting Australians.

The Australasian Consumer Fraud Taskforce's National Consumer Fraud Week campaign is the key annual scams public awareness raising initiative for the ACCC. As with previous years, the release of the Targeting Scams report during Fraud Week received significant media coverage in 2015.

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

8. Domestic and international collaboration

The ACCC recognises that combating scams is a shared responsibility between government, industry and individuals. At the government level a coordinated response is required with collaboration between local and overseas entities essential to effectively deal with the global reach of scams.

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

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

8.1 The Australasian Consumer Fraud Taskforce

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

The Taskforce's main functions are to:

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

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

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

National Consumer Fraud Week

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

2015 campaign—'Get smarter with your data'

The 2015 Fraud Week campaign, '*Get smarter with your data*', ran from Monday 18 May to Sunday 24 May and focused on identity theft. The campaign's aim was to raise awareness of what personal information Australians make accessible online and what steps they can take to protect this data.

Stolen personal information underpins almost every scam reported. Scammers steal not only money from their victims but also their data which they then use to commit identity theft or to sell to other scammers.

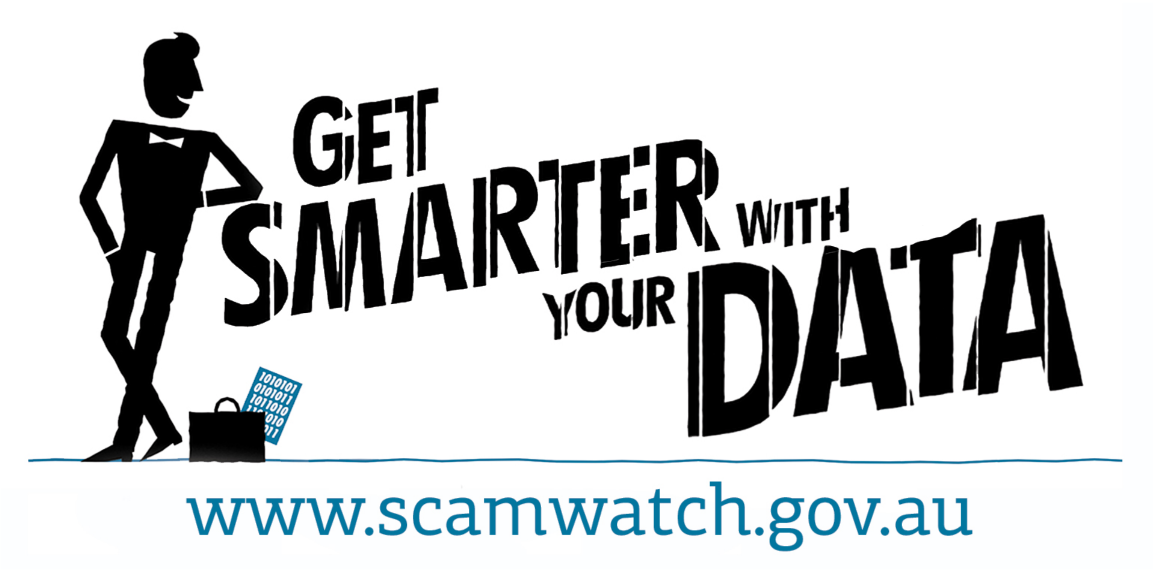
Campaign highlights included:

- the release of the ACCC's 2014 Targeting Scams Report and
- the production of a short animated film describing the threat of data theft and the strategies people can use to protect themselves (http://scamwatch.gov.au/news/national-consumer-fraud-week-2015)

The launch of the ACCC's 2014 Targeting Scams Report generated significant media interest, which was used to promote Fraud Week. In the first two days of the campaign, most major news outlets covered Fraud Week, focusing on poor data security practices and general scam statistics reported to the ACCC.

The Fraud Week campaign was supported by a diverse range of partners including various government agencies, businesses, community groups and industry bodies.

Figure 9: 2015 National Consumer Fraud Week emblem



2016 campaign— 'Wise up to scams'

The Taskforce's 2016 Fraud Week campaign, *'Wise up to scams'*, will run in the week commencing 16 May 2016. The campaign will focus on scams targeting the 55+ age demographic, particularly investment scams and dating and romance scams.

The Australasian Consumer Fraud Taskforce recognised that significant losses were reported to Scamwatch from scams that target this demographic, including investment and online dating scams. With access to a greater level of wealth, it is not surprising that this demographic is targeted by scammers.

To support the campaign, the ACFT will use Fraud Week to generate mainstream and social media interest to raise awareness of scams. It will also work with a number of private sector and not-for-profit partners to promulgate messages on how to identify and avoid scams.

8.2 The International Consumer Protection and Enforcement Network

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

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

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

8.3 Australian Transaction Reports and Analysis Centre partnership

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

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

Intelligence from AUSTRAC is an integral component of the ACCC's Scam Disruption project where it is used to identify Australian residents that send funds to high risk jurisdictions. The information is then used to warn them that they may have fallen victim to a scam — see section 3.1 for more information.

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

8.4 Australian Cybercrime Online Reporting Network (ACORN)

On 26 November 2014 the Australian Government launched the Australian Cybercrime Online Reporting Network (ACORN) as part of its response to cybercrime.

ACORN is a national online system that allows the public to securely report instances of cybercrime. It is a key initiative under the National Plan to Combat Cybercrime, which sets out how Australian agencies, including the ACCC, are working together to make Australia a harder target for cybercriminals.

ACORN has been designed to make it easier to report cybercrime and help develop a better understanding of cybercrime affecting Australians. Intelligence and threat assessments on ACORN data are assessed by the Australian Crime Commission to assist in the development of a clearer national picture. The system also refers reports to law enforcement and government agencies to help them respond quickly to acts of cybercrime.

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

Further information about ACORN is available at www.acorn.gov.au.

ACORN Data

In 2015 ACORN received 25 612 scam reports with a total loss of $127.5 million.[20] 40 per cent of reports to ACORN indicated a loss. This is a significantly higher conversion rate than the 9.8 per cent of reports received by Scamwatch. Investment scams, nigerian scams and dating and romance scams were some of the largest categories for losses with relatively few reports—consistent with analysis of ACCC data.

ACORN data also shows significant losses caused by online identity theft and online accounts being hacked, respectively accounting for $14.1 million and $13.9 million. Reports in these categories often involve the victim's bank account being illegally accessed and money withdrawn.

Table 14: ACORN Top 5 Scam Categories

Scam Category	Amount reported lost	Contacts	Contacts reporting loss	Conversion rate
Offered an investment opportunity	$16 865 905	253	201	79.4%
Asked to pay money upfront or transfer money ('Nigerian' scam)	$15 423 176	2 039	913	44.8%
Dating or romance scam	$14 863 826	572	328	57.3%
Online identity theft	$14 135 469	3 654	733	20.1%
An online account has been hacked into	$13 995 347	1 064	699	65.7%

[20] This analysis specifically excludes those reports where they identify as having reported to Scamwatch and those that did not identify whether or not they had reported elsewhere.

Appendix 1: Glossary of scam terms

Attempts to gain your personal information (fake bank or telco, computer hacking, ID theft)

Hacking

Scammers often use information obtained from phishing scams and other sources to hack into your email, banking or social media accounts. Once they have compromised your accounts, they can change passwords preventing you from accessing your accounts. Scammers often then send out messages impersonating you either directing people to fake websites or claiming that you are stuck overseas and requesting that your friends send money.

Phishing

'Phishing' refers to emails, text messages or websites that trick people into giving out their personal and banking information. These messages pretend to come from legitimate businesses, normally banks or other financial institutions or telecommunications providers. The scammers try to obtain valuable personal information like passwords, bank account or credit card numbers.

ID theft involving spam or phishing

This category is used to capture data where ID theft involving spam or phishing has occurred and a fake identity has been created.

Buying, selling or donating (classifieds, business listings, auction, health, fake business etc.)

Classified scams

Scammers use online classified and auction sites to advertise (often popular) products for sale at cheap prices. They will ask for payment up front and often claim to be overseas. The scammer may try to gain your trust with false but convincing documents and elaborate stories.

Fake charity scams

Scammers take advantage of natural disasters and other events by impersonating charities and requesting donations.

Fake trader websites

Fake websites offer goods for sale, often advertised at very cheap prices. They will accept payments from you but never deliver the items ordered. These websites often look very similar or almost identical to genuine retail sites.

False billing

A false billing scam is a scam that targets small businesses, trying to bill them for a service such as advertising. The scam might come as a proposal for a subscription disguised as an invoice. Another common approach used by scammers is to ring a firm asking to confirm details of a service that they claim has already been booked. The scammer might try to convince them that they have used the scammer's product in the past. Scammers might also try to intimidate businesses by threatening legal action.

Health and medical products

These scams try to make money by exploiting people who have a medical condition or who are worried about their health. The scammers offer solutions or cures where none exist or promise to simplify complex health treatments.

Mobile premium services

These scams try to attract you with offers for 'free' goods, asking you to enter an online competition or complete a survey. Scammers ask for your mobile number to complete this task. What you may not realise is that by accepting the offer, you are actually subscribing to a service that will keep sending you SMS messages and add the cost of these to your phone bill.

Overpayment scams

Scammers target people selling over online classified or auction sites. The scammer will make a payment for a greater amount than the price of the good. The scammer will invent an excuse for the overpayment e.g. the extra money is meant to cover the fees of an agent or extra shipping costs. The scammer will then ask you to refund the excess amount or forward it on to a third party, usually through online bank transfer or wire transfer. The scammer is hoping to gain payment before you discover that the original payment is fraudulent.

Psychic and clairvoyant

Psychic and clairvoyant scammers approach you foreshadowing a positive upcoming event or claiming that you are in some sort of trouble and offering a solution. This 'solution' could be winning lottery numbers, a lucky charm, the removal of a 'curse' or 'jinx', or ongoing 'protection'. The scammer will tell you that they can help you in return for a fee/s. If you refuse to pay, some scammers may threaten to invoke a curse or bad luck charm.

Remote access scams

The scammer contacts you claiming that your computer is infected and that they need remote access to check. The scammer may try to convince you to purchase anti-virus software to remove the infection. The fee may be a one-off payment or an ongoing subscription.

Other buying and selling scams

Any other scam not identified in the preceding nine scam categories where something is supposedly bought or sold. Preference is given to classifying scams into more specific categories where this is possible.

Dating and Romance (including Adult Services)

Dating and romance scams

Dating and romance scams are particularly convincing because they appeal to your romantic or compassionate side. They play on emotional triggers to get you to provide money, gifts or personal details.

Jobs and investment (sport, high return, pyramid scheme, employment)

Computing prediction software and sports investment schemes

Sports investment schemes can include computer prediction (betting software) or betting syndicates. Salespeople try to convince you that their fool proof system can guarantee you a profit on sporting events like football or horse racing. These schemes are often camouflaged as legitimate investments.

Investment schemes

These scams use highly sophisticated websites to trick consumers into thinking investment offers are legitimate. In many cases scammers contact you through unsolicited phone calls and emails. Scammers claim that the investment will provide attractive returns and use high pressure sales tactics.

Job and employment

Job and employment scams target people looking for a new job or a change of job. They often promise an inflated income (sometimes they even guarantee it) for little effort or they demand an upfront payment before the job is yours. These scams can involve you engaging in money laundering, which is a crime.

Pyramid schemes

Pyramid schemes are illegal and very risky 'get-rich-quick' schemes. Promoters at the top of the pyramid make their money by having people join the scheme. In a typical pyramid scheme, a member pays to join. If the only returns from a scheme are entirely or substantially reliant on the member convincing other people to join up, then it is an illegal pyramid scheme.

Other business, employment and investment scams

Other business, employment and investment scams.

Threats and extortion (malware and software by email, malware and software by phone, hitman etc.)

Hitman scams

Hitman scams involve scammers sending death threats claiming to be from 'hitmen' hired to kill you unless you send them cash.

Ransomware and malware

Ransomware and malware involves a scammer placing harmful software onto your computer. Malware can give scammers access to your computer, collect personal information or just cause damage to the computer. Often the malware will cause the computer to freeze or lock and scammers will demand a payment to have the computer unlocked. These scams can target both individuals and businesses.

Unexpected money (inheritance, helping a foreigner, fake government or bank, loan opportunity)

Inheritance scams

An inheritance scam is when a scammer contacts you unexpectedly to tell you that you've been left, or are entitled to claim, a large inheritance from a distant relative or wealthy benefactor who has died overseas. Scammers will often pose as a lawyer, banker or other foreign official and will advise that the deceased left no other beneficiaries.

Nigerian scams

A 'Nigerian' scam is a form of upfront payment or money transfer scam. They are called Nigerian scams because the first wave appeared to emerge from Nigeria. They now come from anywhere in the world. The scammers offer you a share in a large sum of money that they want to transfer out of their country for a range of reasons e.g. to release money trapped in central banks during civil wars or coups. Alternatively they may tell you about massive inheritances that are difficult to access because of government restrictions or taxes.

Reclaim scams

Scammers contact a victim pretending to be from the government, utility company, bank or other well-known entity and ask for an upfront fee to reclaim money. Reasons this money is owed can include overcharged bank fees, tax refunds or compensation.

Other upfront payment and advanced fee frauds

Scammers commonly try to get you make advance payments for promises that never materialise. These promises vary but can include providing you with a loan or promising to return funds previously lost in an early scam.

Unexpected prizes (lottery, travel, scratchie)

Scratchie scams

Scratchie scams involve receiving a package in the mail which will commonly contain colourful travel brochures and a number of scratchie cards. One card will always be a winner, although not always first prize. When you call the number provided in the package, the scammer will ask for fees or taxes to be paid usually via a wire transfer service.

Travel prize scams

Travel prize scams often involve scammers claiming you have won a free holiday or travel related products. In fact all you have won is the chance to purchase accommodation or flight vouchers, which often fail to disclose that other terms apply and may involve additional costs, limited availability or other restrictions.

Unexpected prize and lottery scams

The scammer may tell you that you have won something substantial (such as a large sum of money, or shopping vouchers) and that all you have to do is send money or provide personal information to claim the winnings. Alternatively scammers may be asking you to buy into a fake lottery or competition.

Appendix 2: Scam tables by state and territory

Where possible the ACCC collects data about the geographic location of people reporting scams. Appendix 2 provides a breakdown of 2015 scam categories by state and territory.

Australian Capital Territory

Scam category level 2	Amount reported lost	Contacts	Contacts reporting loss	Less than $10k lost	Greater than $10k lost	Contacts reporting no loss	Conversion rate
Inheritance scams	$568 000	111	2	0	2	109	1.8%
Dating & romance	$565 505	95	35	26	9	60	36.8%
Investment schemes	$263 134	37	13	9	4	24	35.1%
Other buying & selling scams	$143 331	230	77	74	3	153	33.5%
Computer prediction software & sports investment schemes	$141 311	11	8	3	5	3	72.7%
Other upfront payment & advanced fee frauds	$114 830	300	21	17	4	279	7.0%
Classified scams	$92 340	107	24	22	2	83	22.4%
Job & employment	$76 490	99	14	12	2	85	14.1%
Other business employment & investment scams	$51 246	111	7	6	1	104	6.3%
Nigerian scams	$36 200	34	5	2	3	29	14.7%
Fake trader websites	$35 598	97	69	69	0	28	71.1%
ID theft involving spam or phishing	$26 286	300	7	7	0	293	2.3%
Ransomware & malware	$20 745	143	5	4	1	138	3.5%
Unexpected prize & lottery scams	$12 177	105	7	7	0	98	6.7%
Phishing	$10 264	517	7	7	0	510	1.4%
Reclaim scams	$9 560	330	6	6	0	324	1.8%
Health & medical products	$9 297	20	10	10	0	10	50.0%
Hacking	$7 721	72	10	10	0	62	13.9%
Remote access scams	$5 789	137	3	3	0	134	2.2%
Overpayment scams	$2 911	40	5	5	0	35	12.5%
Fake charity scams	$1 958	30	5	5	0	25	16.7%
Hitman scams	$1 790	29	1	1	0	28	3.4%
False billing	$1 702	157	10	10	0	147	6.4%
Travel prize scams	$1 172	34	1	1	0	33	2.9%
Mobile premium services	$755	23	8	8	0	15	34.8%
Pyramid schemes	$500	10	1	1	0	9	10.0%
Psychic & clairvoyant	$–	1	0	0	0	1	0.0%
Scratchie scams	$–	8	0	0	0	8	0.0%
Iscufficient data provided	$–	19	0	0	0	19	0.0%
Grand total	**$2 200 612**	**3 207**	**361**	**325**	**36**	**2 846**	**11.3%**

New South Wales

Scam category level 2	Amount reported lost	Contacts	Contacts reporting loss	Less than $10K lost	Greater than $10K lost	Contacts reporting no loss	Conversion rate
Investment schemes	$7 186 650	299	89	38	51	210	30.0%
Dating & romance	$7 138 064	648	233	142	91	415	36.0%
Nigerian scams	$2 287 678	210	25	16	9	185	12.0%
Computer prediction software & sports investment schemes	$1 356 152	106	67	26	41	39	63.0%
Other buying & selling scams	$1 268 026	2 225	614	579	35	1 611	28.0%
Inheritance scams	$1 108 362	1 025	24	14	10	1 001	2.0%
Other upfront payment & advanced fee frauds	$1 067 423	3 708	269	243	26	3 439	7.0%
Other business employment & investment scams	$804 479	897	88	72	16	809	10.0%
Remote access scams	$375 208	1 996	137	132	5	1 859	7.0%
Unexpected prize & lottery scams	$370 626	1 024	69	62	7	955	7.0%
Fake trader websites	$310 744	858	488	482	6	370	57.0%
ID theft involving spam or phishing	$291 038	2 932	108	101	7	2 824	4.0%
Classified scams	$223 239	799	120	114	6	679	15.0%
Hacking	$198 739	997	78	74	4	919	8.0%
Reclaim scams	$194 247	4 389	52	49	3	4 337	1.0%
Job & employment	$182 365	581	63	58	5	518	11.0%
Phishing	$180 954	5 021	65	60	5	4 956	1.0%
False billing	$154 687	1 219	117	114	3	1 102	10.0%
Psychic & clairvoyant	$111 525	24	15	14	1	9	63.0%
Hitman scams	$91 838	195	8	6	2	187	4.0%
Ransomware & malware	$85 553	1 410	41	39	2	1 369	3.0%
Health & medical products	$55 987	122	36	35	1	86	30.0%
Scratchie scams	$44 847	112	2	0	2	110	2.0%
Pyramid schemes	$40 975	51	9	8	1	42	18.0%
Overpayment scams	$40 905	422	43	43	0	379	10.0%
Travel prize scams	$28 409	248	20	20	0	228	8.0%
Fake charity scams	$24 957	313	33	33	0	280	11.0%
Mobile premium services	$5 389	228	89	89	0	139	39.0%
Insufficient data provided	$210	244	2	2	0	242	1.0%
Grand total	**$25 229 276**	**32 303**	**3 004**	**2 665**	**339**	**29 299**	**9.0%**

Northern Territory

Scam category level 2	Amount reported lost	Contacts	Contacts reporting loss	Less than $10K lost	Greater than $10K lost	Contacts reporting no loss	Conversion rate
Dating & romance	$658 263	76	27	18	9	49	36.0%
Computer prediction software & sports investment schemes	$300 000	5	1	0	1	4	20.0%
Other upfront payment & advanced fee frauds	$100 461	114	28	25	3	86	25.0%
Other buying & selling scams	$83 044	112	34	33	1	78	30.0%
Investment schemes	$71 009	17	7	3	4	10	41.0%
Other business employment & investment scams	$68 067	31	5	3	2	26	16.0%
Nigerian scams	$39 920	58	22	21	1	36	38.0%
Inheritance scams	$31 004	65	5	4	1	60	8.0%
Overpayment scams	$25 026	19	4	3	1	15	21.0%
False billing	$24 855	58	5	4	1	53	9.0%
Classified scams	$21 610	32	8	7	1	24	25.0%
Fake trader websites	$12 024	50	37	37	0	13	74.0%
Job & employment	$8 641	26	8	8	0	18	31.0%
Unexpected prize & lottery scams	$5 306	54	6	6	0	48	11.0%
ID theft involving spam or phishing	$4 200	70	5	5	0	65	7.0%
Hacking	$2 700	29	2	2	0	27	7.0%
Reclaim scams	$1 218	47	3	3	0	44	6.0%
Fake charity scams	$1 042	17	3	3	0	14	18.0%
Travel prize scams	$594	10	1	1	0	9	10.0%
Ransomware & malware	$522	37	1	1	0	36	3.0%
Mobile premium services	$430	11	5	5	0	6	45.0%
Health & medical products	$407	4	2	2	0	2	50.0%
Remote access scams	$329	38	2	2	0	36	5.0%
Phishing	$ -	114	0	0	0	114	0.0%
Hitman scams	$ -	6	0	0	0	6	0.0%
Psychic & clairvoyant	$ -	1	0	0	0	1	0.0%
Pyramid schemes	$ -	0	0	0	0	0	0.0%
Scratchie scams	$ -	4	0	0	0	4	0.0%
Insufficient data provided	$ -	8	0	0	0	8	0.0%
Grand total	**$1 460 672**	**1113**	**221**	**196**	**25**	**892**	**20.0%**

Queensland

Scam category Level 2	Amount reported lost	Contacts	Contacts reporting loss	Less than $10K Lost	Greater than $10K lost	Contacts reporting no loss	Conversion rate
Investment schemes	$8 444 124	281	84	28	56	197	30.0%
Dating & romance	$5 096 528	578	177	112	65	401	31.0%
Computer prediction software & sports investment schemes	$1 329 350	109	77	27	50	32	71.0%
Other buying & selling scams	$763 129	1 851	421	404	17	1 430	23.0%
Other upfront payment & advanced fee frauds	$761 185	2 411	157	140	17	2 254	7.0%
Unexpected prize & lottery scams	$673 124	833	62	55	7	771	7.0%
Fake trader websites	$652 441	541	305	299	6	236	56.0%
ID theft involving spam or phishing	$438 597	2 083	64	54	10	2019	3.0%
Nigerian scams	$427 023	221	29	24	5	192	13.0%
Reclaim scams	$399 467	3 547	51	41	10	3 496	1.0%
Other business employment & investment scams	$393 492	700	97	85	12	603	14.0%
Inheritance scams	$375 493	901	14	6	8	887	2.0%
Hacking	$211 845	680	50	45	5	630	7.0%
Classified scams	$204 207	753	108	102	6	645	14.0%
Job & employment	$108 178	503	39	35	4	464	8.0%
Remote access scams	$101 114	1 277	82	81	1	1 195	6.0%
False billing	$92 083	940	81	80	1	859	9.0%
Overpayment scams	$45 181	394	22	20	2	372	6.0%
Health & medical products	$40 962	93	32	30	2	61	34.0%
Scratchie scams	$31 322	123	5	4	1	118	4.0%
Hitman scams	$31 260	152	3	2	1	149	2.0%
Phishing	$27 619	3 445	35	35	0	3 410	1.0%
Psychic & clairvoyant	$23 201	11	5	4	1	6	45.0%
Travel prize scams	$16 485	146	14	14	0	132	10.0%
Ransomware & malware	$15 297	974	27	27	0	947	3.0%
Fake charity scams	$8 433	250	24	24	0	226	10.0%
Mobile premium services	$4 938	192	75	75	0	117	39.0%
Pyramid schemes	$3 699	71	7	7	0	64	10.0%
Insufficient data provided	$23 785	165	2	1	1	163	1.0%
Grand total	**$20 743 562**	**24 225**	**2 149**	**1 861**	**288**	**22 076**	**9.0%**

South Australia

Scam category level 2	Amount reported lost	Contacts	Contacts reporting loss	Less than $10K lost	Greater than $10K lost	Contacts reporting no loss	Conversion rate
Dating & romance	$1 190 300	166	57	37	20	109	34.0%
Investment schemes	$703 068	91	31	19	12	60	34.0%
Nigerian scams	$543 319	77	11	9	2	66	14.0%
Other upfront payment & advanced fee frauds	$279 441	854	62	55	7	792	7.0%
Computer prediction software & sports investment schemes	$245 222	34	20	8	12	14	59.0%
Other buying & selling scams	$196 357	549	130	124	6	419	24.0%
Other business employment & investment scams	$193 573	238	19	14	5	219	8.0%
ID theft involving spam or phishing	$115 386	658	17	15	2	641	3.0%
Reclaim scams	$113 238	470	8	5	3	462	2.0%
Inheritance scams	$75 100	359	2	1	1	357	1.0%
Classified scams	$70 952	211	33	31	2	178	16.0%
Fake trader websites	$67 615	195	113	111	2	82	58.0%
Remote access scams	$45 753	425	30	28	2	395	7.0%
Unexpected prize & lottery scams	$42 109	375	18	16	2	357	5.0%
False billing	$41 299	330	32	31	1	298	10.0%
Hitman scams	$29 853	77	7	6	1	70	9.0%
Phishing	$24 873	1 258	15	14	1	1 243	1.0%
Job & employment	$23 239	216	11	10	1	205	5.0%
Scratchie scams	$20 500	115	2	1	1	113	2.0%
Hacking	$19 857	248	16	15	1	232	6.0%
Ransomware & malware	$16 870	319	12	11	1	307	4.0%
Travel prize scams	$13 328	58	8	8	0	50	14.0%
Health & medical products	$11 001	33	15	15	0	18	45.0%
Overpayment scams	$7 239	84	9	9	0	75	11.0%
Fake charity scams	$2 195	67	9	9	0	58	13.0%
Pyramid schemes	$827	26	1	1	0	25	4.0%
Mobile premium services	$735	64	27	27	0	37	42.0%
Psychic & clairvoyant	$150	4	1	1	0	3	25.0%
Insufficient data provided	$250	54	1	1	0	53	2.0%
Grand total	**$4 093 649**	**7 655**	**717**	**632**	**85**	**6 938**	**9.0%**

Tasmania

Scam category level 2	Amount reported lost	Contacts	Contacts reporting loss	Less than $10K lost	Greater than $10K lost	Contacts reporting no loss	Conversion rate
Dating & romance	$436 770	54	20	11	9	34	37.0%
Investment schemes	$410 101	33	8	3	5	25	24.0%
Computer prediction software & sports investment schemes	$105 429	13	6	1	5	7	46.0%
Scratchie scams	$75 587	65	6	4	2	59	9.0%
Job & employment	$49 500	36	3	1	2	33	8.0%
Other business employment & investment scams	$46 400	107	2	1	1	105	2.0%
Other upfront payment & advanced fee frauds	$36 675	351	21	20	1	330	6.0%
Unexpected prize & lottery scams	$32 597	102	8	7	1	94	8.0%
Other buying & selling scams	$32 590	184	44	44	0	140	24.0%
ID theft involving spam or phishing	$27 765	255	8	6	2	247	3.0%
Nigerian scams	$27 000	23	1	0	1	22	4.0%
Inheritance scams	$23 254	90	2	1	1	88	2.0%
Fake trader websites	$8 511	65	40	40	0	25	62.0%
Remote access scams	$7 239	129	5	5	0	124	4.0%
Phishing	$6 046	416	4	4	0	412	1.0%
Hacking	$5 383	65	3	3	0	62	5.0%
Overpayment scams	$4 609	36	2	2	0	34	6.0%
Ransomware & malware	$2 765	123	6	6	0	117	5.0%
Reclaim scams	$2 700	209	3	3	0	206	1.0%
Travel prize scams	$2 624	20	3	3	0	17	15.0%
Classified scams	$2 135	65	4	4	0	61	6.0%
Fake charity scams	$1 417	38	2	2	0	36	5.0%
False billing	$1 215	111	7	7	0	104	6.0%
Health & medical products	$522	8	4	4	0	4	50.0%
Mobile premium services	$196	25	7	7	0	18	28.0%
Hitman scams	$ -	36	0	0	0	36	0.0%
Psychic & clairvoyant	$ -	0	0	0	0	0	0.0%
Pyramid schemes	$ -	7	0	0	0	7	0.0%
Insufficient data provided	$ -	12	0	0	0	12	0.0%
Grand total	**$1 349 030**	**2 678**	**219**	**189**	**30**	**2 459**	**8.0%**

Victoria

Scam category level 2	Amount reported lost	Contacts	Contacts reporting loss	Less than $10K lost	Greater than $10K lost	Contacts reporting no loss	Conversion rate
Dating & romance	$4 093 975	496	158	88	70	338	32.0%
Investment schemes	$2 907 685	319	71	35	36	248	22.0%
Inheritance scams	$1 288 067	706	19	7	12	687	3.0%
Other upfront payment & advanced fee frauds	$1 225 105	2 332	206	187	19	2 126	9.0%
Nigerian scams	$1 001 428	184	25	15	10	159	14.0%
Computer prediction software & sports investment schemes	$864 740	78	47	15	32	31	60.0%
Other buying & selling scams	$800 304	1 639	467	448	19	1 172	28.0%
Other business employment & investment scams	$413 367	756	62	52	10	694	8.0%
Reclaim scams	$402 666	2 589	51	45	6	2 538	2.0%
False billing	$268 607	844	91	84	7	753	11.0%
Fake trader websites	$268 220	592	338	333	5	254	57.0%
ID theft involving spam or phishing	$242 544	1 929	72	65	7	1 857	4.0%
Job & employment	$164 781	515	51	44	7	464	10.0%
Hacking	$155 874	674	45	40	5	629	7.0%
Unexpected prize & lottery scams	$145 152	768	60	55	5	708	8.0%
Psychic & clairvoyant	$121 049	13	6	5	1	7	46.0%
Ransomware & malware	$119 712	842	35	32	3	807	4.0%
Classified scams	$118 570	571	98	96	2	473	17.0%
Scratchie scams	$112 018	112	3	1	2	109	3.0%
Phishing	$107 104	2 950	42	39	3	2 908	1.0%
Remote access scams	$99 518	1 276	82	81	1	1 194	6.0%
Health & medical products	$72 627	77	36	35	1	41	47.0%
Hitman scams	$58 155	152	6	5	1	146	4.0%
Travel prize scams	$43 126	135	11	10	1	124	8.0%
Overpayment scams	$27 014	334	25	24	1	309	7.0%
Pyramid schemes	$16 625	48	6	5	1	42	13.0%
Fake charity scams	$14 285	175	18	18	0	157	10.0%
Mobile premium services	$3 528	185	71	71	0	114	38.0%
Insufficient data provided	$-	141	0	0	0	141	0.0%
Grand total	**$15 155 846**	**21 432**	**2 202**	**1 935**	**267**	**19 230**	**10.0%**

Western Australia

Scam category level 2	Amount reported lost	Contacts	Contacts reporting loss	Less than $10K lost	Greater than $10K lost	Contacts reporting no loss	Conversion rate
Investment schemes	$3 152 592	140	49	19	30	91	35.0%
Dating & romance	$2 296 072	275	79	48	31	196	28.7%
Computer prediction software & sports investment schemes	$935 274	53	35	12	23	18	66.0%
Inheritance scams	$779 350	443	7	2	5	436	1.6%
ID theft involving spam or phishing	$648 479	1034	27	23	4	1 007	2.6%
Other buying & selling scams	$541 008	849	208	196	12	641	24.5%
Other upfront payment & advanced fee frauds	$258 141	1279	90	84	6	1 189	7.0%
Job & employment	$228 876	338	28	22	6	310	8.3%
Other business employment & investment scams	$210 208	481	35	29	6	446	7.3%
Reclaim scams	$206 092	943	10	8	2	933	1.1%
Ransomware & malware	$126 623	537	26	23	3	511	4.8%
Hitman scams	$123 500	152	2	1	1	150	1.3%
Hacking	$107 274	348	22	20	2	326	6.3%
Remote access scams	$93 715	547	37	35	2	510	6.8%
Classified scams	$78 769	294	42	40	2	252	14.3%
Pyramid schemes	$77 708	31	5	4	1	26	16.1%
Fake trader websites	$77 417	264	154	153	1	110	58.3%
Nigerian scams	$69 296	108	11	9	2	97	10.2%
Travel prize scams	$55 216	65	9	8	1	56	13.8%
Unexpected prize & lottery scams	$51 397	357	21	20	1	336	5.9%
False billing	$24 375	426	35	35	0	391	8.2%
Overpayment scams	$10 117	160	9	9	0	151	5.6%
Fake charity scams	$9 747	91	15	15	0	76	16.5%
Phishing	$6 370	1 593	12	12	0	1 581	0.8%
Health & medical products	$3 846	42	16	16	0	26	38.1%
Mobile premium services	$3 700	93	44	44	0	49	47.3%
Psychic & clairvoyant	$ -	2	0	0	0	2	0.0%
Scratchie scams	$ -	21	0	0	0	21	0.0%
Insufficient data provided	$900	66	1	1	0	65	1.5%
Grand total	**$10 176 062**	**11 032**	**1 029**	**888**	**141**	**10 003**	**9.3%**

Appendix 3: Scamwatch radars

Donate safely to bushfire appeals

January 2015: Scamwatch is encouraging Australians who are considering donating to bushfire appeals to make sure they double check whether the appeal or its organisers are legitimate so that their generosity reaches victims, not scammers.

Beware of fake vouchers that end up costing you more

January 2015: Scamwatch is urging consumers to be alert to scammers offering fake vouchers in exchange for financial and other personal information.

Invoice email scam now targeting Australian businesses

January 2015: Scamwatch is warning Australian businesses to beware of an invoice email scam seeking payment re-direction.

This Valentine's Day, protect your heart when seeking love online

February 2015: This Valentine's Day, Scamwatch is warning the online dating community to beware of any love interest who asks for money.

Fake rebate scams on the rise

March 2015: In February the ACCC received a spike in contacts about fake rebate schemes so we are warning people to be aware of calls from a fake government department claiming you are owed money.

Beware of NBN scams

March 2015: Scamwatch is warning consumers and businesses to be aware of NBN-related scams seeking to get your personal details or asking you to buy equipment you don't need.

Telephone calls alleging fake arrest warrants used to scam money

April 2015: Scamwatch is warning consumers to be aware of calls from scammers falsely claiming to be from the Commonwealth Director of Public Prosecutions (CDPP) or Australian Tax Office (ATO).

Immigration scam targets migrants

April 2015: Scamwatch is warning consumers to be aware of calls from scammers claiming to be from the 'Department of Immigration' threatening you with deportation and demanding money.

Fake debt collectors

May 2015: Scamwatch is warning of phone calls from scammers claiming to collect debts.

Would you like to hear about how small businesses are being targeted by scammers?

June 2015: Scamwatch invites small businesses to view a video of a recent public event.

Don't let scammers 'tax' you this tax time

August 2015: With tax time in full swing, Scamwatch is again urging consumers and small businesses to be aware of scammers taking advantage of the busy nature of tax time to target you.

Beware of fake lottery and competition 'wins' on social networking platforms

August 2015: Scamwatch is warning consumers to beware of fake lotteries or competitions on social networking platforms, with scammers using popular platforms to pedal these empty wins.

Beware of scammers continuing to pose as Microsoft with fake upgrade claims

October 2015: Scamwatch is warning consumers to beware of scammers pretending to be from Microsoft, with the latest round of scams based around the current Microsoft Windows 10 system upgrade.

Don’t let fake sellers ruin Christmas’ ‘Beware of scammers imitating Centrelink officers

November 2015: The ACCC is warning consumers to beware of scammers imitating Centrelink officers to trick you into handing over your money or personal details.

Don’t let fake sellers ruin Christmas

December 2015: Scamwatch is warning Christmas shoppers to be cautious when looking online for gifts.

Beware of scammers delivering malware this Christmas

December 2015: Watch out for fake parcel delivery scams arriving in your inbox this Christmas.

Appendix 4: Other scam-related educational materials

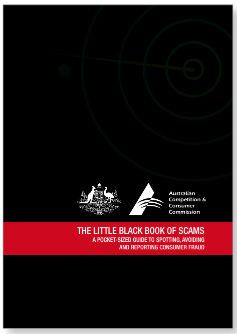
Scamwatch

SCAMWATCH

Scamwatch website (www.scamwatch.gov.au)

Scamwatch Twitter profile (@Scamwatch_gov)
https://twitter.com/scamwatch.gov

Publications



Australian Competition & Consumer Commission

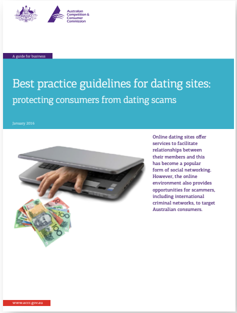
THE LITTLE BLACK BOOK OF SCAMS

A POCKET-SIZED GUIDE TO SPOTTING, AVOIDING AND REPORTING CONSUMER FRAUD

The Little Black Book of Scams

WHAT YOU NEED TO KNOW ABOUT: Small business scams

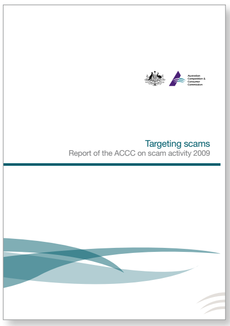
ACCC Small business scams factsheet



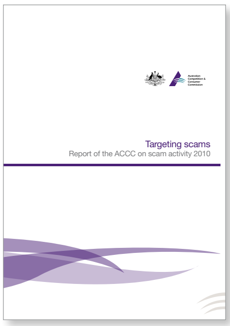
Best practice guidelines for dating sites: protecting consumers from dating scams

Best practice guidelines for dating websites

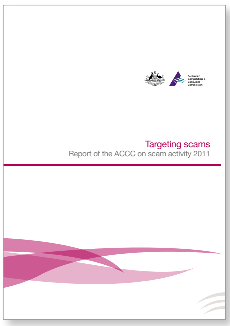
Annual reports



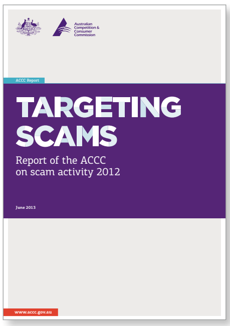
Targeting scams
Report of the ACCC on scam activity 2009



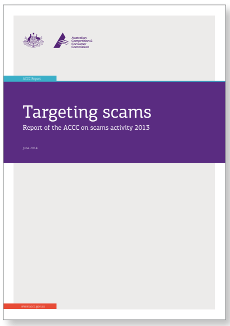
Targeting scams
Report of the ACCC on scam activity 2010



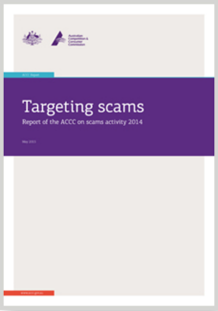
Targeting scams
Report of the ACCC on scam activity 2011



TARGETING SCAMS
Report of the ACCC on scam activity 2012



Targeting scams
Report of the ACCC on scams activity 2013



Targeting scams
Report of the ACCC on scams activity 2014

Targeting scams: Report of the ACCC on scam activity—2009, 2010, 2011, 2012, 2013 and 2014

2015 Fraud Week campaign resources

Get smarter with your data

https://www.youtube.com/watch?v=BL7WJM342Uc

2015 National Consumer Fraud Week emblem

Appendix 5: ACFT Members

Taskforce members

Australian Government

Attorney-General's Department

Australian Bureau of Statistics

Australian Communications and Media Authority

Australian Competition and Consumer Commission (Chair)

Australian Federal Police

Australian Institute of Criminology

Australian Securities and Investments Commission

Australian Taxation Office

Department of Communications and the Arts

New Zealand Government

New Zealand Commerce Commission

New Zealand Ministry of Consumer Affairs

State and territory governments

Australian Capital Territory Office of Fair Trading

Consumer Affairs and Fair Trading, Department of Justice Tasmania

Consumer Affairs Victoria

Department of Commerce Western Australia

Fair Trading Queensland

Northern Territory Consumer Affairs

New South Wales Fair Trading

Office of Consumer and Business Affairs SA

Representatives of the state and territory police

New South Wales Police Service

Queensland Police Service

Northern Territory Police Force

State and Territory Police Commissioners