Australian
Competition &
Consumer
Commission

ACCC Report

Targeting scams

Report of the ACCC on scams activity 2016

May 2017

www.accc.gov.au

Foreword

Delia Rickard

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

In 2016, the ACCC and the Australian Cybercrime Online Reporting Network (ACORN) received a combined 200 103 reports about scams. Losses reported to Scamwatch, ACORN and from other scam disruption programs totalled almost $300 million. This figure is by no means conclusive of the total cost of scams as many victims do not report their experiences—in fact in April 2016 the Australian Bureau of Statistics published results of its Personal Fraud survey, which estimated the total amount lost to personal fraud to be closer to $3 billion. These figures are staggering and serve as a pointed reminder of how damaging scams are on our society.

The ACCC received 155 035 scam reports—a sharp increase of 47 per cent compared to 2015. Despite the considerable increase in reports, financial losses to scams have decreased by two per cent, with $83.6 million reported lost.

This year's report highlights emerging trends in scam activities and in particular, the techniques, approach and methods used by scammers to deceive their victims. It also highlights the education and disruption activities undertaken by the ACCC to combat scams.

Combined ACCC and ACORN losses to dating and romance and investment scams reached $42 million and $59 million respectively. As with 2015, dating and romance and investment scams continued to produce the biggest financial losses, with $25.5 million (dating and romance) and $23.6 million (investment scams) reported lost to the ACCC alone. It's not difficult to see why Australians are losing money to these scams—they are often very sophisticated, targeted and involve long term grooming. Those aged between 55–64 were the most susceptible to dating and romance scams, whereas those aged between 45–54 were most affected by investment scams.

One of the most concerning trends has been the four-fold increase in hacking scams, from $700 000 in 2015 to $2.9 million in 2016. Businesses have shouldered the brunt of these scams, with over half ($1.7 million) being attributed to businesses in 2016, a substantial increase from the $213 990 lost in 2015. While the digital economy presents many opportunities and efficiencies for businesses it also presents significant risks. Scams targeting businesses are becoming increasingly sophisticated using modern technology to make fake emails, invoices and websites appear legitimate to even the astute business person. These scams can have devastating effects on businesses, undoing years of hard work, eroding confidence in their brand, increasing operational costs and in extreme cases may even cripple those businesses.

The consumer market is also changing—the digital age, while benefiting consumers, is also providing scammers with the opportunity to try new tricks. If consumers follow the platforms, so will the scammer. This is most telling in the number of reports the ACCC received in relation to online scams. Online scams—those executed via the internet, email, social networks and mobile apps—outnumbered phone based scams with an increase of 130 per cent (72 105 reports) over 2015. Losses to online scams accounted for 58 per cent ($48.4 million) of total losses. Social media was a particularly busy platform used by scammers to lure victims, netting losses of $9.5 million in 2016 compared to $3.8 million in 2015, with email based scams also being highly profitable.

A continuing challenge that the ACCC and other regulators face in scam prevention is the ability to keep up with new and devious methods scammers use to contact victims. Scams continue to come in many shapes and sizes, however new and emerging issues have been identified throughout 2016 which are discussed in the report. Dating and romance scams have now evolved on social media platforms, and often involve blackmail through sextortion. In 2016, we also saw the increase of requests for payment via iTunes or gift cards and the rise of threat based scams (often impersonating government agencies) to scare victims into parting with their money. While this report highlights new and emerging scams, it is clear that the old '419' scams continue to be a problem. These scams are often reported to ACORN and once again feature in ACORN's top five scam categories by financial loss.

The ACCC continues to combat scams through education, awareness raising and disruption. Key achievements in 2016 includes the growing success of the Scamwatch website with a record of 1 837 458 unique users—an increase of 18 per cent from 2015; revision of the Little Black Book of Scams and yet another successful delivery of the National Consumer Fraud Week campaign 'Wise Up To Scams' focused on raising awareness of scams targeting older Australians.

While scammers are professionals at evading the law, with many operating from overseas or otherwise unidentifiable, the ACCC does take enforcement action where appropriate to deter and discourage scammers targeting Australians. In 2016, the ACCC commenced action against ABG Pages Pty Ltd alleging misleading and deceptive or scam-like conduct in its dealings with small businesses.

The ACCC is also determined to find other innovative ways to counter scammers' evasive behaviour, with disruption a key tool in this approach. The ACCC continued its disruption project in 2016, which involves using financial intelligence to identify people transferring money offshore to high risk jurisdictions and warn them about scams. In 2016, we also commenced work with business enablers such as financial institutions, telecommunication providers and Facebook to develop better scam prevention systems to make it harder for scammers to access victims or receive money from them. This work will continue with great rigour in 2017. Supporting this will be ongoing educational efforts, with the Australasian Consumer Fraud Taskforce's 2017 Fraud Week campaign, 'Spot social media scams', asking people to be safe on social media.

Through education and awareness, the ACCC, together with our partners will continue to work towards reducing the harm to Australian consumers caused by scammers from around the world.

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 05/17_1162

www.accc.gov.au

Snapshot of 2016[1]

Losses reported to Scamwatch & ACORN and scam disruption programs

- In 2016, the ACCC and the Australian Cybercrime Online Reporting Network (ACORN) received a combined 200 103 reports about scams. Losses reported to Scamwatch, ACORN and detected in other scam disruption programs totalled almost $300 million.

Breakdown of ACCC scam reports and financial losses

- 2016 was marked by a sharp increase in scam reporting, continuing an upward trend from 2015. The ACCC received 155 035 scam reports, a 47 per cent increase over 2015.
- The total financial loss from scams reported to the ACCC was $83 563 599—a slight decrease from 2015 reported losses. Of this, online scams accounted for 58 per cent ($48.4 million) of all reported losses.
- Over 52 per cent of people who lost money reported losing less than $500. The average loss was $7226.
- The top three scam categories reported to the ACCC were phishing (attempts to gain personal information), advance fee frauds (send money up-front to receive a reward) and false billing scams, accounting for 36 per cent of all scams recorded in 2016.[2]
- Dating and romance and investment scams had the highest reported financial losses of nearly $25.5 million and $23.6 million respectively.
- Combined ACCC and ACORN reported losses totalled nearly $42 million for dating and romance scams and $59 million for investment scams.
- Reports of losses from computer prediction software and sports investment scams collectively decreased by 68 per cent from $5.5 million in 2015 to $1.8 million in 2016. Losses reported as a result of hacking scams on the other hand, experienced the greatest increase from $700 000 in 2015 to $2.9 million in 2016.

Demographics

- The amount of money reported lost to scams tended to increase with the victim's age. The over 65 age group reported the highest financial loss of $13.6 million, where age was provided.
- Where gender was provided, females made more scam reports than males (44 per cent to 39 per cent); however reported financial losses were greater for males ($35.6 million), accounting for 43 per cent of total losses.
- Females reported losing more to dating and romance scams with $11.9 million in losses, while males were more affected by investment scams ($13.2 million).
- In 2016, reported financial losses suffered by Indigenous peoples totalled over $1.4 million based on 1499 reports, increasing by 21 per cent from 2015.

Scam contact methods

- The most popular contact methods used by scammers in 2016 were phone and email, accounting for 39 per cent and 35 per cent respectively of all reported contact.
- Phishing scams and identity theft were the most prevalent of all phone scams with 19 344 reports. Cold calling investment scams resulted in the highest reported losses for phone based scams with $11.5 million reported lost based on 879 reports.
- Online scams (delivered via the internet, email, social networks and mobile apps) collectively outnumbered phone based scams. Overall, online scam reports increased by 130 per cent from 2015. This is due to an 85 per cent increase in reports of scams facilitated via email and an 80 per cent increase in reports of social media based scams.
- Social media was a particularly active contact method with reported losses of $9.5 million in 2016 compared to $3.8 million in 2015. Most of those losses were caused by dating and romance scams.

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

[2] Please see Appendix 1 for a glossary of scam terms. Definitions of all Scamwatch categories can also be found on the Scamwatch website at (www.scamwatch.gov.au).

- Phishing and ransomware were the most common email based scams.[3]

Emerging scams in 2016

- Emerging trends in 2016 included increasing scams through social media, scams using iTunes and other gift cards, threat-based and impersonation scams and a rise in scams targeting businesses.

Scams through social media

- In 2016, one third of dating and romance scam victims reported that they had come into contact with a scammer through a social media platform.
- Sextortion is an emerging scam that utilises social media to gain access to victims. It is a form of blackmail in which compromising images of the victim are used to extort money. In 2016 Scamwatch received over 440 reports from victims of sextortion.

Scams using iTunes and other gift cards

- In 2016, reports to Scamwatch indicated that scammers were using iTunes and other gift cards as a new source of payment. Most of these reports related to tax scams.
- Over 20 000 reports were made to Scamwatch about this type of scam. Of these, 280 reported a total loss of over $1.4 million and at least 60 per cent indicated that they paid the scammer with iTunes gift cards.

Threat based and impersonation scams

- Threat-based and impersonation scams often involve the impersonation of a government agency and the use of threats (fines, arrest, deportation) to coerce the victim into paying money.
- Scamwatch received over 24 400 reports about a variety of threat-based scams, with total reported losses over $1.6 million.

Business scams

- 5953 reports were submitted on behalf of businesses with nearly $3.8 million reported lost to scams. Of this, over $2 million was reported lost by micro and small businesses. The average loss was $10 631.
- The highest reported losses were to computer hacking ($1.7 million), investment schemes ($980 626) and other buying and selling scams ($532 509).

Disruption & enforcement

- In 2016, the ACCC's key disruption activities focused on relationship scams and working with intermediaries, including banks, telecommunication providers and social media platforms to bolster their scam prevention efforts.
- The ACCC continued its Scam Disruption project, with over 2834 letters sent to potential scam victims in 2016. Of those that were sent a letter, 74 per cent stopped sending money within six weeks. Similar disruption projects operated by other agencies continued in South Australia (SA) and Western Australia (WA).
- In 2016 the ACCC instituted proceedings against a trader allegedly involved in misleading and deceptive or scam-like conduct.

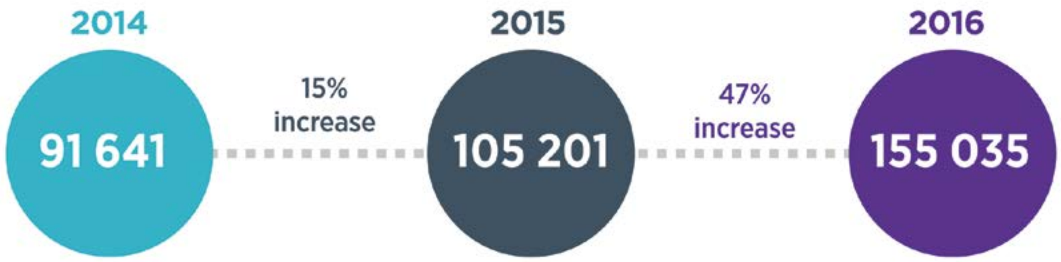
[3] Ransomware is a type of malware that blocks or limits access to computer files and demands a ransom to be paid to the scammer for the files to be unlocked.

Education and engagement

- *The little black book of scams* was revised in 2016 to include new information about trending scams, such as threat and penalty scams, and new techniques used by scammers to defraud victims.
- The ACCC continued to publish Scamwatch radar alerts to its subscription base. A total of 13 Scamwatch alerts were published in 2016, with 11 of those also issued as media releases on the ACCC's mainstream website, resulting in wider media coverage.
- The ACCC hosted a community barbecue in Katherine, Northern Territory, to raise awareness of common techniques used by scammers targeting Indigenous communities across rural and regional Australia.
- The 2016 National Consumer Fraud Week campaign 'Wise up to scams' was successfully delivered in May. It focused on raising awareness of scams targeting older Australians (55+) through extensive promotion and media coverage.

1. 2016 scam trends[4]

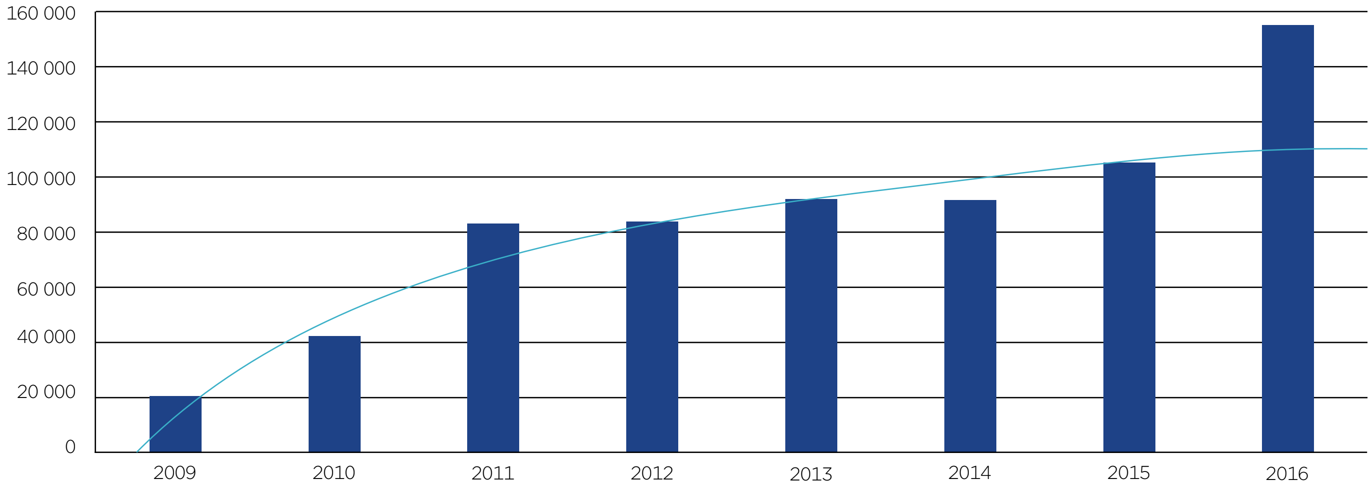
1.1 Scam reports



In 2016, the ACCC received 155 035 scam reports, a 47 per cent increase on the 105 201 reports received in 2015—the largest increase in reports since 2011. Scamwatch reports indicate that bulk email scams were the main driver of this increase.

Figure 1 provides a comparison of scam reports to the ACCC over the past eight years. It shows an early upward trend with a slower increase in report levels from 2012–15 and a sharp increase in reports in 2016.

Figure 1: Number of scam-related reports to the ACCC 2009 to 2016



[4] Unless otherwise indicated, all data is based on reports provided to the ACCC by webform or over the phone. While the ACCC undertakes quality assurance processes to ensure data reliability, reports are not individually verified and some may contain response or data processing errors.

Table 1 provides an overview of scams reported to the ACCC in 2016 by scam category.

The top three scam categories reported to the ACCC were phishing, advance fee frauds and false billing scams. These three categories accounted for 36 per cent of all scams reported to Scamwatch.

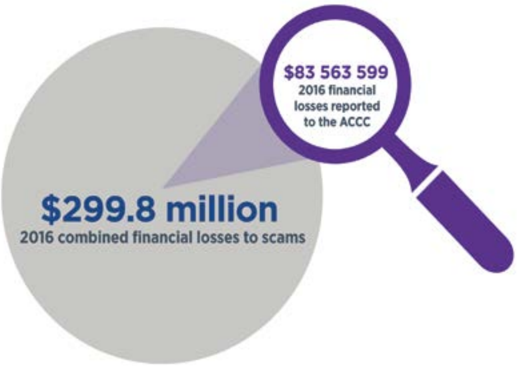
Table 1: Overview of scam categories reported to the ACCC in 2016 by number of reports

Scam category	Amount reported lost	Reports	Reports with loss	Reports with no loss	Less than $10k lost	Greater than $10k and less than $100k lost	Greater than $100k lost	Conversion rate
Phishing	$373 860	24 925	194	24 731	187	7	0	0.8%
Other upfront payment & advance fee frauds	$6 499 604	16 830	957	15 873	871	84	2	5.7%
False billing	$659 835	14 634	565	14 069	552	13	0	3.9%
Reclaim scams	$1 168 222	13 366	219	13 147	196	20	3	1.6%
ID theft involving spam or phishing	$715 896	12 731	206	12 525	188	18	0	1.6%
Other buying & selling scams	$4 128 104	9 827	1 873	7 954	1 790	79	4	19.1%
Unexpected prize & lottery scams	$1 450 803	6 950	266	6 684	237	26	3	3.8%
Other business, employment & investment scams	$2 742 443	6 500	380	6 120	312	65	3	5.8%
Remote access scams	$1 422 834	6 369	475	5 894	443	32	0	7.5%
Ransomware & malware	$241 881	6 210	227	5 983	224	3	0	3.7%
Fake trader websites	$1 278 219	4 603	2 010	2 593	1 991	19	0	43.7%
Dating & romance	$25 480 351	4 109	1 017	3 092	685	257	75	24.8%
Hacking	$2 851 145	4 050	216	3 834	167	42	7	5.3%
Classified scams	$923 798	3 125	444	2 681	425	19	0	14.2%
Inheritance scams	$3 512 270	3 063	92	2 971	61	23	8	3.0%
Job & employment	$1 127 011	2 855	221	2 634	199	20	2	7.7%
Overpayment scams	$256 580	2 804	161	2 643	157	4	0	5.7%
Mobile premium services	$40 354	2 030	742	1 288	742	0	0	36.6%
Investment schemes	$23 631 338	1 766	503	1 263	248	180	75	28.5%
Nigerian scams	$1 404 108	1 498	221	1 277	190	28	3	14.8%
Scratchie scams	$769 835	1 339	50	1 289	28	22	0	3.7%
Hitman scams	$124 780	1 283	27	1 256	23	4	0	2.1%
Fake charity scams	$110 008	1 172	84	1 088	80	4	0	7.2%
Travel prize scams	$150 936	1 016	82	934	79	3	0	8.1%
Health & medical products	$81 691	734	148	586	148	0	0	20.2%
Pyramid schemes	$250 439	393	41	352	36	5	0	10.4%
Computer prediction software & sports investment schemes	$1 784 795	319	114	205	74	37	3	35.7%
Psychic & clairvoyant	$382 459	173	29	144	24	4	1	16.8%
Insufficient data provided	$0	361	0	361	0	0	0	0.0%
Grand total	**$83 563 599**	**155 035**	**11 564**	**143 471**	**10 357**	**1 018**	**189**	**7.5%**

Appendix 1 includes a glossary of scam terms. Alternatively, definitions of all scam categories can be found on the Scamwatch website (www.scamwatch.gov.au).

1.2 Financial losses to scams[5]

In 2016, the total financial loss from scams reported to the ACCC was $83 563 599. Losses decreased by less than two per cent on the amount reported in 2015 ($84 941 766). However, losses reported to Scamwatch and ACORN, combined with losses detected through various scam disruption programs totalled almost $300 million (see shaded box titled 'Scamwatch losses—tip of the iceberg' on page 7).

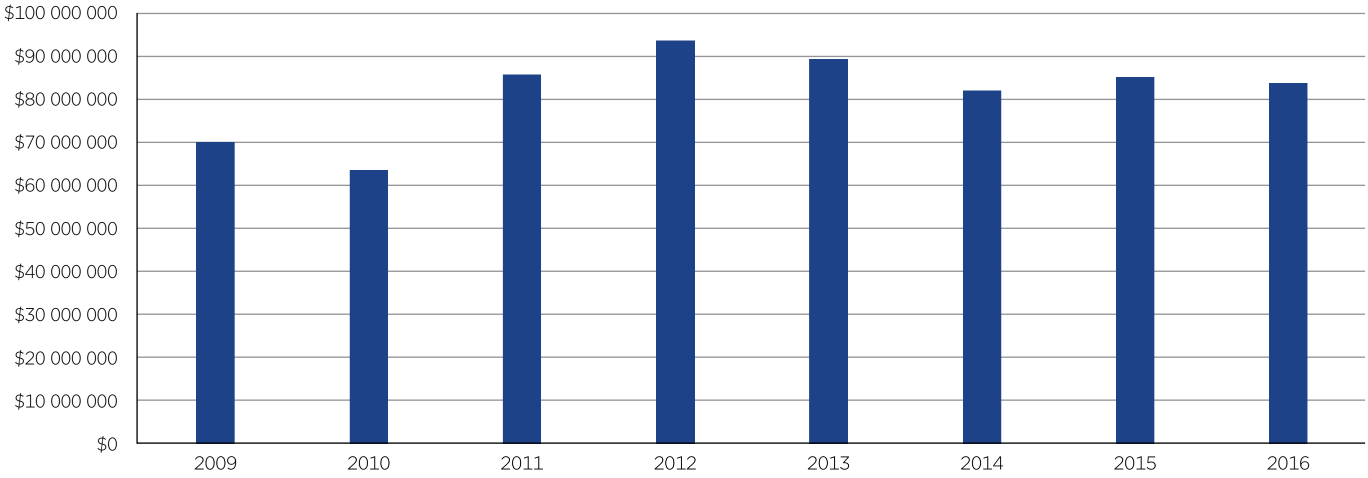


In 2016, Scamwatch reports revealed some significant variations in specific scam categories compared to 2015. Losses due to computer prediction software and sports investment scams decreased by 68 per cent from $5.5 million to $1.8 million. The hacking category experienced the greatest increase in reported losses, quadrupling from $700 000 in 2015 to $2.9 million.

- In 2016, 92.5 per cent of people who reported to the ACCC reported not losing any money, an increase from 90 per cent in 2015. This may suggest increasing community awareness of how to identify, avoid and report scams.
- A number of high-loss scams were reported in 2016. Of those who reported a financial loss, 10 per cent lost over $10 000 and 355 people reported losing $50 000 or more. Ten people reported a loss between $50 000 and $1 million and two people reported a loss over $1 million. The average loss was $7226.
- Over 52 per cent of people who lost money reported losing less than $500, which indicates that the most common scams are 'high volume, low value'—these are scams that are delivered to large numbers of recipients but cause smaller losses per victim.
- Reported losses to online scams totalled $48.4 million, accounting for 58 per cent of all reported financial losses in 2016.

Figure 2 provides a comparison of scam-related financial losses reported to the ACCC over the past eight years.

Figure 2: Reported financial losses to the ACCC from 2009 to 2016



[5] Financial losses include any monetary losses reported to the ACCC in 2016.

Scamwatch losses—tip of the iceberg

Financial losses to scams are considerably higher than what is reported to Scamwatch each year, as many victims do not report their loss at all or report it to another agency. Where losses are reported to have occurred online, people may report more of these to ACORN. The ACCC's tracking of scam trends does not provide a complete picture given many consumers will report scams to specific organisations like ACORN as well as other regulatory agencies.

ABS Personal Fraud Survey—2014–15

In April 2016, the Australian Bureau of Statistics (ABS) published results from its Personal Fraud Survey conducted throughout Australia from July 2014 to June 2015. This was the third survey of personal fraud in Australia. The first was conducted in 2007 and the second in 2010–11.

The survey found that 1.6 million Australians, or around 8.5 per cent of the population aged 15 years and over was a victim of personal fraud, such as card fraud, identify theft or other scams in the 12 months prior to interview in 2014–15. Just over half of the Australian population (10.4 million people) aged 15 and over were exposed to at least one scam and an estimated 126 300 persons in Australia were victims of identity theft. Nationally, four per cent (449 100) of persons exposed to a scam also responded to at least one scam, by either supplying personal information, money or both, or by seeking more information in relation to the request.

The total estimated financial loss as a result of all personal fraud incidents was $3 billion.

More information about the survey is available at www.abs.gov.au.

2016 ACORN statistics[6]

The Australian Cybercrime Online Reporting Network (ACORN) receives a large number of online scam reports. In 2016, ACORN received 45 068 scam reports with a total loss of $204 705 578 (over and above losses reported to Scamwatch). Of all reports, 38 per cent indicated a loss—a significantly higher number of reports compared to the 7.5 per cent of reports received by Scamwatch. Investment scams, online identity theft and hacking were some of the largest categories for losses reported by ACORN. A table of the top five scam categories reported to ACORN is provided at Table 2 below.

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 (see section 4.1). Many of these victims don't report their loss to the ACCC. A combined estimate of losses to this unreported scam activity is approximately $11.5 million.

An aggregate of losses reported to Scamwatch and ACORN, together with unreported losses detected through scam disruption programs show approximate overall losses of almost $300 million. This figure specifically excludes reports to ACORN where the person or business identified as having reported to Scamwatch.[7]

Table 2: Overview of 2016 ACORN data—top five scam categories

Scam Category	Amount reported lost	Reports	Reports with loss	Conversion rate
Offered an investment opportunity	$35 132 883	354	274	77.4%
Online identity theft	$23 450 818	5 443	2 441	44.8%
An online account has been hacked into	$20 794 276	1 370	1 093	79.8%
Dating or romance scam	$16 394 669	1 056	473	68.0%
Asked to pay money upfront or transfer money ('Nigerian' scam)	$15 563 301	2255	1128	50.0%

[6] Any ACORN figures reported are based on the ACCC's review of the data. While the ACCC undertakes quality assurances processes to ensure data reliability, ACORN reports are not individually verified by the ACCC.

[7] The combined loss of $300 million includes reports to ACORN by people who did not identify whether they had reported to another agency. In the 2015 Report the ACCC did not include those who did not specify whether they reported the scam to another agency. Using a consistent methodology, the ACCC estimated the total combined losses in 2015 were $234 million, which compares to the total combined losses for 2016 of $300 million.

Table 3 provides an overview of scam categories by financial loss as reported to the ACCC in 2016.

The top two scam categories in terms of money lost were dating and romance and investment scams. These two categories accounted for 59 per cent of all reported financial losses. Combined ACCC and ACORN reported losses totalled nearly $42 million for dating and romance scams and $59 million for investment scams.

Table 3: Overview of scam categories reported to the ACCC in 2016 by financial loss

Scam category	Amount reported lost	Reports	Reports with loss	Reports with no loss	Less than $10k lost	Greater than $10k and less than $100k lost	Greater than $100k lost	Conversion rate
Dating & romance	$25 480 351	4 109	1 017	3 092	685	257	75	24.8%
Investment schemes	$23 631 338	1 766	503	1 263	248	180	75	28.5%
Other upfront payment & advance fee frauds	$6 499 604	16 830	957	15 873	871	84	2	5.7%
Other buying & selling scams	$4 128 104	9 827	1 873	7 954	1 790	79	4	19.1%
Inheritance scams	$3 512 270	3 063	92	2 971	61	23	8	3.0%
Hacking	$2 851 145	4 050	216	3 834	167	42	7	5.3%
Other business employment & investment scams	$2 742 443	6 500	380	6 120	312	65	3	5.8%
Computer prediction software & sports investment schemes	$1 784 795	319	114	205	74	37	3	35.7%
Unexpected prize & lottery scams	$1 450 803	6 950	266	6 684	237	26	3	3.8%
Remote access scams	$1 422 834	6 369	475	5 894	443	32	0	7.5%
Nigerian scams	$1 404 108	1 498	221	1 277	190	28	3	14.8%
Fake trader websites	$1 278 219	4 603	2 010	2 593	1 991	19	0	43.7%
Reclaim scams	$1 168 222	13 366	219	13 147	196	20	3	1.6%
Job & employment	$1 127 011	2 855	221	2 634	199	20	2	7.7%
Classified scams	$923 798	3 125	444	2 681	425	19	0	14.2%
Scratchie scams	$769 835	1 339	50	1 289	28	22	0	3.7%
ID theft involving spam or phishing	$715 896	12 731	206	12 525	188	18	0	1.6%
False billing	$659 835	14 634	565	14 069	552	13	0	3.9%
Psychic & clairvoyant	$382 459	173	29	144	24	4	1	16.8%
Phishing	$373 860	24 925	194	24 731	187	7	0	0.8%
Overpayment scams	$256 580	2 804	161	2 643	157	4	0	5.7%
Pyramid schemes	$250 439	393	41	352	36	5	0	10.4%
Ransomware & malware	$241 881	6 210	227	5 983	224	3	0	3.7%
Travel prize scams	$150 936	1 016	82	934	79	3	0	8.1%
Hitman scams	$124 780	1 283	27	1 256	23	4	0	2.1%
Fake charity scams	$110 008	1 172	84	1 088	80	4	0	7.2%
Health & medical products	$81 691	734	148	586	148	0	0	20.2%
Mobile premium services	$40 354	2 030	742	1 288	742	0	0	36.6%
Insufficient data provided	$0	361	0	361	0	0	0	0.0%
Grand total	**$83 563 599**	**155 035**	**11 564**	**143 471**	**10 357**	**1 018**	**189**	**7.5%**

Dating and romance and investment scams are extremely damaging scam types as they generally result in high financial losses. Reports to the ACCC indicate that dating and romance scams in particular are more targeted, involve personalised approaches and often include long-term grooming of victims. Fake documents and social media profiles also assist in making the scam appear legitimate. Ultimately, this targeted approach builds trust and lulls victims into feeling more secure, setting them up to lose large sums of money.

Provision of age data is not a mandatory reporting requirement and therefore it may be difficult to draw definitive conclusions about the age groups most affected by these scams. However, where age was reported, Scamwatch reports indicate that Australians aged between 55–64 were most affected by dating and romance scams, while those aged 45–54 were most affected by investment scams.

- Dating and romance scams—the 55–64 group reported losing $4.7 million and the over 65s lost $4.2 million. Where gender was reported, females reporting losing almost $12 million, 70 per cent more than males ($7 million).
- Investment scams—the 45–54 group reported losing nearly $4.8 million. Where gender was reported, males lost almost triple the amount of money reported by female victims, $13.2 million and $4.9 million respectively.

Table 4: Comparison of scam-related monetary losses reported to the ACCC in 2016 and 2015

Loss categories $	2016	Percentage 2016	2015	Percentage 2015
1–99	2 541	22.0%	1 982	19.3%
100–499	3 546	30.7%	3 387	33.0%
500–999	1 402	12.1%	1 192	11.6%
1000–9999	2 868	24.8%	2 433	23.7%
10 000–49 999	852	7.4%	959	9.3%
50 000–499 999	343	3.0%	296	2.9%
500 000–999 999	10	0.1%	15	0.1%
1 million–10 million	2[8]	0.02%	8	0.1%
Grand total	**11 564**	**100%**	**11 086**	**100%**

In 2016, a large loss of $1.6 million to an online investment scam was reported to the ACCC. Fraudsters use the internet to make investment scams appear legitimate. Glossy brochures, sophisticated websites and online press releases are common techniques used by investment scammers to create an illusion of authenticity.

Victim's story: Chris' confidence in his cousin leads to a questionable investment

Chris received a private Facebook message from a person he believed to be his cousin, Anthony. The scammer, using Anthony's profile picture sent Chris a link which said that Chris could receive a million dollars in only a few days by investing through an online trading platform. Chris, believing the scammer to be his cousin, invested $450 000 immediately and the online trading platform allocated him a number of shares. The scammer then contacted Chris stating that he needed to pay fees and taxes before he could claim his $1 million. Chris, transferred $7000 at first, then $20 000 and finally $40 000. Alarmed by the number of transfers, Chris' bank manager knew something was wrong and advised him to stop paying the scammer immediately. However, it was too late. Chris had lost over $500 000, based on the recommendation of someone he thought he could trust.

Note: The story above is based on one or more real scam reports received by the ACCC. For privacy purposes the names of the victims have been changed.

[8] The ACCC has received two reports of losses over $1 million. While the ACCC undertakes quality assurances to ensure data reliability, these losses have not been individually verified.

1.3 Scam contact methods

According to ACCC reports, phone and email were the most dominant contact methods used by scammers in 2016. While phones have historically been the single most popular contact method of scammers, the increasing online presence of businesses and consumers means that emails are now almost as common.

Table 5 provides a comparison of all scam contact methods reported to the ACCC in 2016 and 2015. Scammers are quickly adapting to technology in their communication methods. Contact by email, internet, social media and mobile applications (collectively 'online scams') have become the most commonly used technology, as well as the most effective.

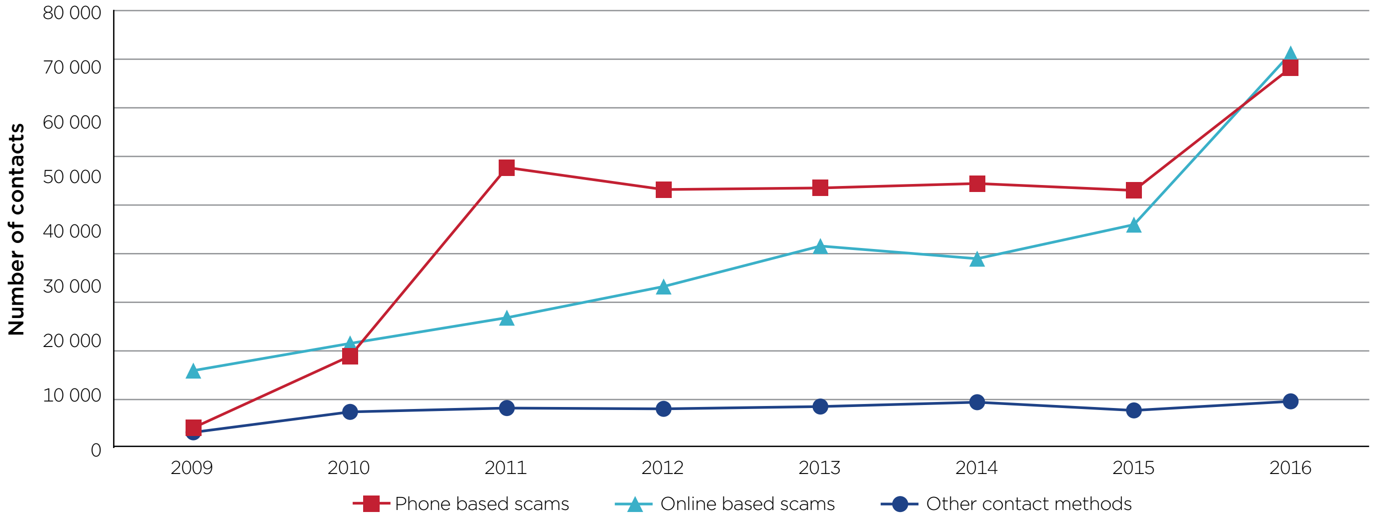
☎ Phone 39% **59 930** reports

✉ Email 35% **54 068** reports

Table 5: Scam contact methods during 2016 and 2015 based on reports to the ACCC

Scammer contact mode	2016 reports	Percentage 2016	2015 reports	Percentage 2015
Phone	59 930	39%	43 070	41%
Email	54 068	35%	29 151	28%
Internet	12 088	8%	8 394	8%
Text message	9 537	6%	3 985	4%
Mail	6 433	4%	5 059	5%
Social networking / online forums	4 762	3%	2 653	3%
In person	1 905	1%	1609	2%
Mobile apps	1 187	1%	599	1%
Fax	138	0%	151	0%
N/A	4 987	3%	10 530	10%
Grand total	**155 035**	**100%**	**105 201**	**100%**

Figure 3: Scam contact methods 2009 to 2016 based on reports to the ACCC



Phone based scams (landline and mobile)

In 2016, phone based scams (phone and text messages) continued to be a popular contact method reported to the ACCC, rising by 48 per cent to 69 467 with losses totalling $24.9 million. Scamwatch reports indicate that this rise may be linked to increases in phone based threat and impersonation scams (see section 2.2). The rise of internet calling technology (also referred to as voice over internet protocol or VoIP) and caller ID spoofing makes it easy and cost-effective for scammers to access victims' money or phish for personal information without being traced.

Of all phone based scams reported to the ACCC, phishing scams and identity theft were the most prevalent scam categories in 2016 with 19 344 reports. Phishing scams can occur in a number of ways; however most commonly the caller pretends to be a well-known organisation such as a government department or utility provider seeking to update personal or account information.

Cold calling investment scams resulted in the highest reported losses for phone based scams with $11.5 million lost based on 879 reports. Most of these reported losses related to offers of investment opportunities in binary options or the opportunity to buy shares at lower than market rates.[9] Advance fee fraud phone calls were next in line, netting $4.6 million in reported losses from 11 660 reports.

2016 emerging scam: high end goods landline scam

An emerging phone based scam has involved scammers cold calling on a landline and advising unsuspecting victims that their credit card has had unauthorised use. The scammer tells the victim to hang up and call their bank or the police. The scammer waits on the line and the victim dials their bank or the police not realising that the scammer has stayed on the phone line. The scammer then obtains enough banking information to access accounts or convinces the victim to transfer money to the scammer. Scams can play out over a series of calls with a number of scammers, or those that merely remain on the line.

Online scams (internet, email, social networks and mobile apps)

In 2016, the ACCC received more reports about online scams than phone based scams, reflecting the growing threat of online fraud.

Reports of online scams increased by 130 per cent from 31 308 in 2015 to 72 105 in 2016. This is due to considerable increases in reports of scams facilitated via email (85 per cent) and social networks (80 per cent).

2015
31 308
reports
Online scams
130%
2016
72 105
reports

There were 54 068 reports of email based scams, with the most common reports relating to phishing and ransomware. Reports of social media related scams increased by 79 per cent from 2653 reports in 2015 to 4762 in 2016, with dating and romance scams accounting for almost a third (28 per cent) of those reports.

Reported losses to online scams amounted to $48.4 million, nearly double that of phone based scams. Social media was a particularly active contact method with reported losses of $9.5 million in 2016 compared to $3.8 million in 2015. Most reported losses on social media were caused by dating and romance scams ($7.5 million lost), as scammers are increasingly targeting victims through social media platforms. Fake trader websites were next in line with at least $53 000 reported lost.

[9] Binary options involve predicting the movements of commodity, asset or index prices over a short time. They are speculative, high risk products that are almost impossible to predict, even for professionals.

The rise of the digital age has created opportunities for scammers to have greater global reach. Scamming victims by 'requesting friendships' on social networking sites or delivering malicious software has never been easier. The online environment gives scammers anonymity, the ability to phoenix, adopt different identities and even mask their physical location.

The ongoing and rapid evolution of mobile-enabled technology and communication channels means that new scams will continue to emerge online, increasing the need for the public to learn how to avoid them. The Australasian Consumer Fraud Taskforce's 2017 Fraud Week campaign 'Spot social media scams' will focus on raising public awareness of social media based scams (see section 5.2).

Victim's story: Dianne's dating dreams turn to dust

Dianne was 'friended' on Facebook by Emil. She accepted his friend request and they began chatting. Emil expressed his desire to be in a relationship with Dianne and said that as soon as he had returned from India for business, he would come to Australia to collect Dianne and take her back to America. Emil's business was in cargo transport and he was travelling to India for three months to sell $9 million worth of high-end motor vehicles.

Dianne was excited at the prospect of spending her life in a new country with Emil. Soon after they began chatting on Facebook, Emil advised her that the Indian government would not release his cargo until he paid the outstanding tariff of $150 000. He asked Dianne to help pay the $150 000, with promises that he would pay her back. Dianne initially gave Emil $800 and after he received this, he asked for a further $20 000. Dianne didn't have a lot of money and when she said she couldn't afford this Emil got very angry. He harassed her constantly trying to get money out of her, always insisting he still wanted to marry her. Dianne paid the further $20 000 and didn't hear back from Emil again. She realised that Emil was not her dream man, but a nightmare scammer.

Note: The story above is based on one or more real scam reports received by the ACCC. For privacy purposes, the names of the victims have been changed.

1.4 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

Table 6 shows the number of reports and total losses in each age category as a percentage of the total. Although provision of age data is not a mandatory reporting requirement, 52 per cent (80 207) of scam reports in 2016 included age.

Table 6: Age ranges provided by consumers reporting scams to the ACCC in 2016

Age range	Reports	Percentage of reports	Reports with loss	Reports with no loss	Reported loss	Conversion rate
Under 18	960	1%	163	797	$67 955	17.0%
18–24 years	5 444	7%	1 031	4 413	$1 263 819	18.9%
25–34 years	11 511	14%	1 810	9 701	$4 617 454	15.7%
35–44 years	12 126	15%	1 553	10 573	$6 566 748	12.8%
45–54 years	14 349	18%	1 444	12 905	$12 909 512	10.1%
55–64 years	15 192	19%	1 101	14 091	$12 388 905	7.2%
65 and over	20 625	26%	1 081	19 544	$13 576 997	5.2%
Not provided	74 828	48%	3 381	71 447	$32 172 209	4.5%
Grand total	**155 035**	**100%**	**11 564**	**143 471**	**$83 563 599**	**7.5%**

More reports provided an age in 2016 (52 per cent) than in previous years. Reports increased across all age groups, however reported losses did not increase at the same rate.

As a percentage of the total, each age range remained largely the same as 2015, with slight (1–2 per cent) increases in the 25–34, 35–44 and 45–54 age groups. The largest shift was the percentage of reports from the 65 and over age group, from 21 per cent in 2015 to 26 per cent in 2016.

Reported losses for those over 45 accounted for nearly 47 per cent of total losses, where age was provided. Scamwatch reports suggest that the mid to older demographic are being targeted by low volume high value scams, such as dating and romance and investment scams.

Of the known age groups, the over 65s reported the highest financial loss to Scamwatch, with dating and romance and investments scams collectively accounting for just over 50 per cent of their total reported loss. The 45–54 age group reported losing the most to investment scams, while those aged 55–64 were more affected by dating and romance scams. For those under 35, losses to dating and romance and buying and selling scams were the largest.

The relationship between age and consumer fraud victimisation

The Australian Institute of Criminology (AIC) released a report in November 2016 titled *The relationship between age and consumer fraud victimisation*. The paper explores how age and associated lifestyle patterns might interact with fraud and the likelihood of falling victim to different types of fraud. The AIC used a survey method with a sample size of 2695 in order to conduct their study.

Some key findings in this report include:

- Younger age groups are more likely to encounter scams on a wide variety of different technologies such as the internet or mobile phones, while older groups were more likely to encounter them mainly through email or landline.
- The 18–24 age group is more likely to provide personal details than middle aged to older Australians.
- The 65 and over age group was statistically more likely to send money when encountering fraud.
- Older groups were also more likely to fall victim to computer support fraud (remote access scams), due to their lower level of knowledge and confidence in using modern technologies.
- The 45– 55 age group was more likely to fall victim to dating and romance fraud. This may be due to lifestyle factors such as divorce or a sense of urgency to settle down with a partner.

The full report is available on: www.aic.gov.au.

Gender

Table 7: Gender breakdown of 2016 scam reports

Gender	Reported loss	Percentage of loss	Reports	Percentage of reports	Reports with loss
Female	$28 143 976	34%	68 822	44%	4 888
Male	$35 644 130	43%	59 790	39%	5 465
Not specified	$19 775 493	24%	26 423	17%	1 211
Grand total	**$83 563 599**	**100%**	**155 035**	**100%**	**11 564**

In 2016, 83 per cent of reports specified a response for gender. Of these, 44 per cent were from females and 39 per cent from males, however males lost more overall, accounting for 43 per cent of losses as compared to 34 per cent for females.

Females lost $11.9 million to dating and romance scams, accounting for 42 per cent of their total losses. Investment scams were the second highest loss category for females with $4.9 million lost. This order was reversed for males, who lost more to investment scams ($13.2 million) than dating and romance scams ($7 million).

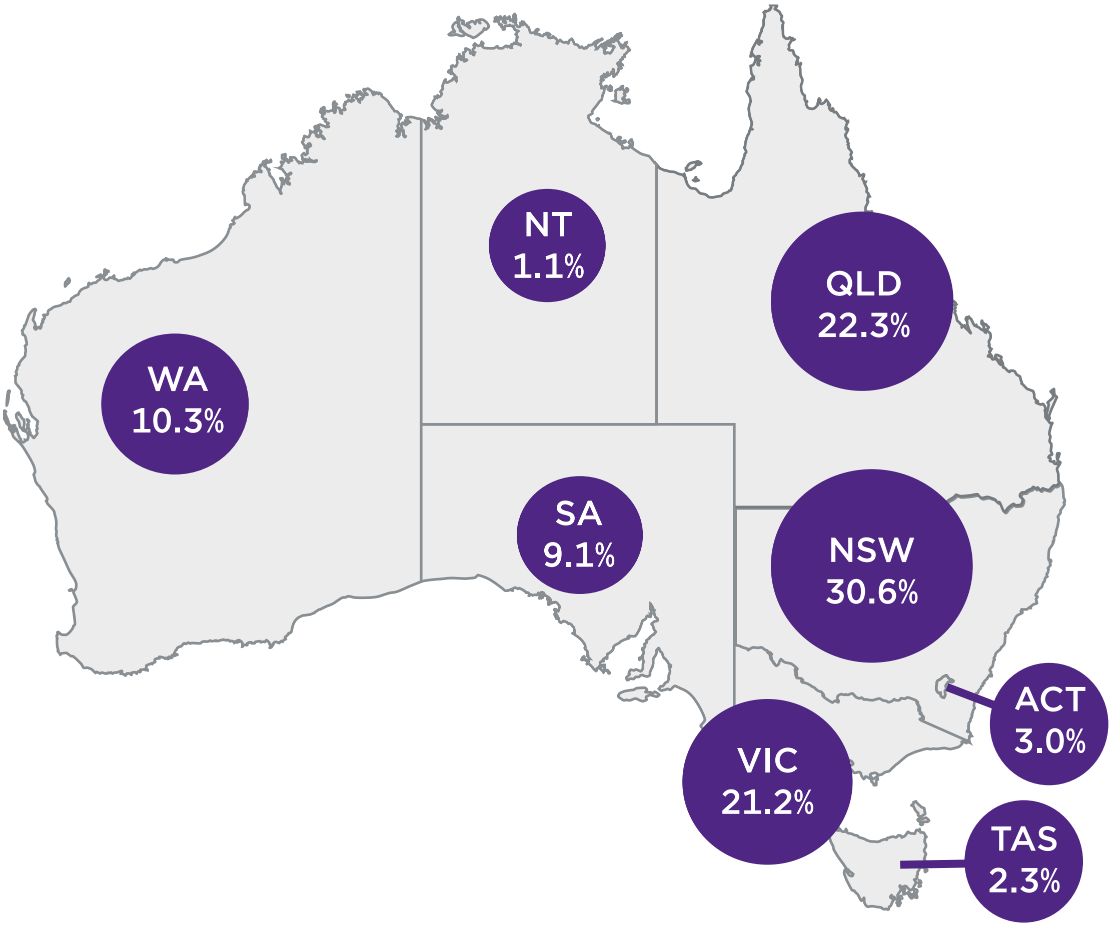
Geographic location

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

Figure 4 shows a comparison of scam reports received by the ACCC in 2016 from within Australia. Similar to 2015, the ACCC received the greatest number of scam reports from New South Wales (NSW), followed by Queensland (QLD) and Victoria (VIC). Western Australia (WA) represents about 10 per cent of the scam reports, with the remaining states and territories collectively accounting for nearly 16 per cent of all reports.

In addition to the above figures, the ACCC received 5232 scam reports from people based overseas. There were 470 reports that did not provide a location.

Figure 4: Scam reports by location 2016



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

Table 8 provides a comparison of scam reports and financial losses against the distribution of the Australian population as a whole. Reports and losses were largely consistent with the percentage of the Australian population by state and territory. The Australian Capital Territory (ACT) reported nearly double what might have been expected.

Table 8: Scam reports by location 2016

State	Percentage of total reports that were based in Australia	Percentage of reported loss where reports were based in Australia	Percentage of Australian population
NSW	30.5%	32.8%	32.0%
QLD	22.2%	22.7%	20.1%
VIC	21.1%	24.4%	25.2%
WA	10.3%	7.7%	10.8%
SA	9.1%	5.1%	7.1%
ACT	3.0%	2.8%	1.6%
TAS	2.3%	2.1%	2.1%
NT	1.1%	1.2%	1.0%
Not provided	0.3%	1.3%	N/A
Grand total	**100%**	**100%**	**100%**

2. Emerging scams: 2016 'top trending' scams

From the infamous '419' mass letter writing scams to the high-tech fraudsters of today, scammers are now well seasoned and sophisticated.[10]

With the evolution of society and technology, we also see scammers innovating and adapting scams. Today, scams can be easily distributed to millions of potential victims through a variety of platforms such as email, text messages, internet pop-ups and social media.

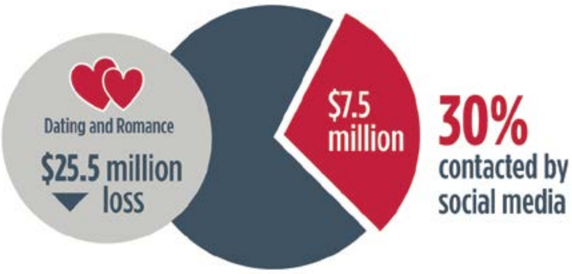
This chapter highlights ways in which scammers are continually adapting and evolving to seek financial returns. Technological advancements have assisted scammers to perfect their trade and access large numbers of victims quickly and easily. They have become increasingly opportunistic, preying on a victim's vulnerabilities, including their compassion, grief, loneliness and even their fear.

In 2016, we have seen scammers use more threatening tactics and make more covert payment requests in an attempt to outwit their victims.

2.1 Scams through social media

Social media is an increasingly popular platform that scammers use to identify and target victims. Scammers who use social media hide behind the anonymity of seemingly legitimate profiles, contact a large number of people and make what appear to be genuine connections.

In 2016, one third of dating and romance scam victims reported that they had come into contact with a scammer through a social media platform. Of the $25.5 million lost to dating and romance scams, approximately $7.5 million (30 per cent) involved contact over social media.



Victims contacted via social media will generally receive a friend request or a private message from someone they have never met before. The scammer may pretend to be a friend of a friend or express an interest in meeting new people. They attempt to develop a relationship very quickly with the victim and often urge the victim to move to other online platforms, such as Skype, to continue the scam.

Another type of emerging scam that utilises social media is sextortion. Sextortion is a subset of dating and romance scams in which the victim is lured into performing compromising acts which are recorded or photographed by the scammer. The material is used by the scammer to blackmail the victim into paying the amount requested. If the victim fails to pay, the scammer threatens to release the videos to the victim's social media pages, family and friends and on public spaces such as YouTube.

In 2016, reports to Scamwatch indicated that over 440 people had been victims of sextortion and of these, 351 victims reported that some form of social media was used to facilitate the scam. The victims of these scams were mostly male (93 per cent).

[10] 419 scams generally offer the victim a share in a large sum of money on the condition that the victim helps the scammer transfer the money out of the country. The '419' part of the name comes from the section of Nigeria's Criminal Code which outlaws the practice. These scams now come from anywhere in the world.

Victim's story: Daniel's dismal date with an online femme fatale

Daniel reported that a woman seeking a relationship had contacted him through a private message on Facebook and he instantly fell for her charm. The scammer was intimate with him on Facebook and they were regularly messaging for three days. At first Daniel thought something might not be right, but after moving to Skype and seeing the scammer in person, all hesitation was gone. During one Skype conversation, Daniel was filmed by the scammer while performing compromising acts in front of the camera. Almost immediately, the scammer's attitude changed and she threatened Daniel, stating that if he didn't pay a large sum of money, the video that had just been recorded would be shared on his Facebook profile so that all his friends and family could see. Daniel sent a wire transfer of almost $2000 immediately to the scammer in Manila. However, even after paying the scammer, the compromising video of Daniel was still shared on Facebook and YouTube for all his family and friends to see.

Note: The story above is based on one or more real scam reports received by the ACCC. For privacy purposes the names of the victims have been changed.

The ACCC provides tips on how consumers can protect themselves from these types of scams on its Scamwatch website (www.scamwatch.gov.au) and in its publication, *The little black book of scams* (www.accc.gov.au/publications/the-little-black-book-of-scams). A hard copy of this publication can be ordered from the website.

2.2 Threat-based and impersonation scams

Scammers will go to extraordinary lengths and use unscrupulous methods to take advantage of victims to steal their money and identity. One extreme example of this approach is threat-based and impersonation scams ('threat-based scams').

In 2016, Scamwatch received over 24 400 reports about a variety of threat-based scams, with total losses over $1.6 million.

In a threat-based scam, the scammer uses intimidation tactics to scare the victim and force them to comply with their demands either via phone or email. In these scams, the scammer adopts the identity of a person of authority, generally an employee of a 'government agency' and will use confidential information to make what appear to be genuine claims. The scammer will generally inform the victim that they owe money to the agency and will use threats (including the threat of fines, charges or arrest) to coerce the victim to comply with their demands.

In 2016, the ACCC received reports on a variety of threat-based scams which impersonated government agencies. Some of the most commonly impersonated agencies included the Department of Immigration and Border Protection (DIBP), Australian Taxation Office (ATO), the Commonwealth Department of Human Services (DHS) or Centrelink and the Australian Federal Police (AFP).

ATO scams

Tax scams accounted for the majority of threat based scams reported to the ACCC in 2016. The ACCC received over 20 000 reports with nearly $1.5 million lost.

These scams come in many guises but generally claim that the victim has underpaid their taxes and are required to repay the tax debt immediately or face frightening repercussions such as an arrest. Other scams that are particularly frequent during tax time include phishing emails, which aim to get the victim's personal details.

Scammers often use personal information found online to try and convince people they are legitimate. They usually ask for payment for an 'unpaid debt' via wire money transfer, credit or debit cards and even iTunes cards. The call appears to come from a local phone number, but most use VoIP phone numbers to disguise the fact that they are calling from overseas.

Victim’s story: Stuart’s nightmare audit

One day Stuart arrived home to a message on his answering machine which stated that he needed to call back the ATO or go to court for failure to respond to letters sent by registered post. Stuart was concerned as he had not received any correspondence from the ATO. Stuart called the number left on his answering machine and spoke to someone who claimed to be from the auditing department within the ATO. The scammer told Stuart that they had done a tax audit of his finances for the last five years and found some discrepancies in payments and that he actually owed the ATO money.

The scammer told Stuart an officer had sent him a notice, but as it had not been answered someone would be coming to arrest him and take him to court. This was going to happen unless he agreed to settle the outstanding amount owed straight away. The scammer told Stuart to buy $10 000 worth of preloaded cards and advised that once this had been done, the ATO officer would visit him at his house the next day and go through the audit to help Stuart identify where the issues had occurred in his tax payments.

Stuart told the scammer he was unaware of owing any money to the ATO as he always paid his tax on time. The scammer assured Stuart that he would explain everything the next day when he visits. The scammer asked Stuart to call him back and read out the pin and card numbers so they could clear his debt. At the end of the phone call Stuart was told not to contact anyone before their visit the next day. Stuart had given the scammer $10 000 for a debt he never owed.

Note: The story above is based on one or more real scam reports received by the ACCC. For privacy purposes the names of the victims have been changed.

Centrelink scams

In 2016, the ACCC received over 2200 reports of Centrelink scams with more than $27 000 reported lost. This is a significant increase from 2015, when there was $3500 reported lost and 560 reports.

In these scams, the victim reports receiving a phone call or email from someone claiming to be from the Commonwealth Department of Human Services or Centrelink advising that the victim is eligible for an increase in their pension or benefit. The scammer will either phish for personal details or will demand money in order for the benefit to be paid. To push the victim into paying money or handing over personal details, the scammer may even claim that their Centrelink benefits will be cut off if payment or personal details are not provided.

Victim’s Story: Paula’s pension payment in peril

One day Paula received a phone call from someone who said they were calling from Centrelink. The scammer told her that there had been an error in her pension payments. The scammer advised Paula that she was actually owed money, but first she would have to pay back her last pension payment before she would receive the money that she was owed.

The scammer asked Paula to pay the money back straight away on her credit card. However, Paula didn’t have a credit card to pay with so the scammers instructed her to purchase $600 worth of iTunes cards. Once she had purchased these, the scammer instructed Paula to call back and gave her ‘Centrelink’s’ phone number.

Paula went out and purchased the cards, when she got home she called the number that she had been given. Someone answered confirming that it was Centrelink. Paula was then directed to another scammer, who took the iTunes numbers and pin codes. Paula was given a receipt number of the transaction and an appointment was made for the next day at her local Centrelink office.

When Paula turned up to the Centrelink office for her appointment she was told that she had been scammed. Centrelink had never called her and there was no issue with her pension payments.

Note: The story above is based on one or more real scam reports received by the ACCC. For privacy purposes the names of the victims have been changed.

Migration scams

Migration scams target a vulnerable group of people, who are often socially isolated and from non-English speaking backgrounds. Cultural and economic barriers may also affect migrants' ability to seek the support they need to understand relevant regulations and procedures. This makes them particularly vulnerable to scams.

Scamwatch reports indicate that scammers target migrants and temporary visa holders claiming there are problems with their paperwork or visa status. They demand a fee to correct the problem and avoid deportation. These scammers often call repeatedly to harass their victim, and might even threaten to send police to the victim's house to arrest loved ones. Some may even claim that their loved ones have already been arrested or detained.

Victim's story: Indra is intimidated by immigration demands

Indra received a phone call from a scammer, Peter, on her landline. The scammer advised her that he was from the DIBP and wanted to know how her family had moved to Australia. The scammer had a translator ready to talk to Indra. This level of professionalism meant that Indra believed the caller was legitimate and that he was in a position of authority.

Indra was advised through the translator that her husband had been taken into police custody. Peter demanded that she immediately provide her mobile number. While still on the home telephone a second scammer, John proceeded to call her mobile phone. John advised that he was a police officer and he had her husband in custody. At this point, both of Indra's available phone lines were engaged and she was not able to contact her husband. She was instructed not to talk to anyone as they would also be arrested as an accomplice. Afraid to hang up either phone, she listened in fear as the scammers advised her that if she did everything they asked her husband would be released from custody that evening.

In order for her husband to be released Indra was required to make a payment of $2400 to the 'DIBP' through a money transfer at the post office. Indra attended her nearest post office and transferred the requested money. Upon calling her husband soon after she transferred the money, Indra realised that she had been scammed.

Note: The story above is based on one or more real scam reports received by the ACCC. For privacy purposes the names of the victims have been changed.

Threat-based ransomware scams

Threat-based scams that occur through email are commonly ransomware scams. The most reported ransomware scams targeting Australians in 2016 were delivered through fake emails purporting to be from Australia Post (4703 reports) and the Australian Federal Police (2224 reports). In Australia Post scams, victims reported receiving a fake email from Australia Post, stating they have an undelivered package. Some emails threaten that the victim will be charged a fee for holding the item and will ask the person to open an attachment, click a link or download a file to retrieve the package. If the victim follows these instructions, their files will encrypt, locking their computer. To unlock the computer, the scammer will often demand payment in the form of bitcoins (a form of online currency) or wire transfer.

The ACCC provides tips on how consumers can protect themselves from these types of scams on its Scamwatch website (www.scamwatch.gov.au) and in its publication, *The little black book of scams* (www.accc.gov.au/publications/the-little-black-book-of-scams). A hard copy of this publication can be ordered from the website.

2.3 Scams using iTunes and other gift cards

Traditional payment requests by scammers generally involve payment via bank transfer or wire transfer via a remittance agency such as Western Union or MoneyGram.

In 2016, reports to Scamwatch indicated that scammers were using iTunes and other gift cards as a new source of payment. iTunes cards and vouchers are sold by Apple and can only be used to purchase media available in the iTunes Store. Increasingly, scam victims are being asked to purchase a large number of iTunes gift cards and scratch off and provide the 16-digit code to the scammer. It is believed that scammers sell the voucher numbers on the online black market or put the credit onto ApplePay to purchase goods and services.[11]

Reports to Scamwatch suggest that this payment method was commonly used in ATO and Director of Public Prosecution (DPP) debt scams (also a form of 'threat-based scams'). In these scams, scammers impersonate the ATO or DPP and demand payment for outstanding debts to the ATO with threats of arrests if payment is not made. Over 20 000 reports were made to Scamwatch about this particular type of scam. Of these, 280 reported a total loss of $1 402 821 million and at least 60 per cent indicated that they paid the scammer with iTunes gift cards.

280 reports
$1 402 821 million loss
60% Paid with iTunes cards

In 2016, the ATO also reported that a significant number of victims were paying scammers using iTunes gift cards, primarily in relation to debt scams. Of those direct reports to the ATO, nearly 200 people reported having paid a total of $678 900 to scammers using iTunes gift cards. This was identified as being the most regular form of payment method used by people to pay scammers in relation to debt scams.[12] In 2016, the ATO worked with enforcement agencies and retailers including Apple to include scam warnings at the point of sale and on Apple's Australian iTunes website.

Similar payment requests were made in other scams, including government impersonation scams such as Centrelink and Migration scams.

Victim's story: Theo is troubled by outstanding taxes

Theo reported that a scammer, pretending to be from the 'ATO', advised him that he had an outstanding tax debt. The scammer advised that as Theo had failed to pay the debt, a warrant was issued for his arrest. The scammer said that the charges would be dropped and Theo could avoid being arrested if certain fees were paid. The scammer advised Theo to purchase iTunes gift cards totalling $5000 and directed him to specific outlets to purchase the cards. Theo purchased the cards and gave them to the scammer by reading back the numbers to the scammer over the phone. The scammer then advised him that they had reassessed the amount of tax owed and further payments were required. Theo, having lost all his money then turned to his family for assistance. It was only when his family contacted his accountant that he found out there was no debt outstanding and he had been the victim of a scam.

Note: The story above is based on one or more real scam reports received by the ACCC. For privacy purposes the names of the victims have been changed.

The ACCC provides tips on how consumers can protect themselves from these types of scams on its Scamwatch website (www.scamwatch.gov.au) and in its publication, *The little black book of scams* (www.accc.gov.au/publications/the-little-black-book-of-scams). A hard copy of this publication can be ordered from the website.

[11] Australian Taxation Office, *January to June and July to December 2016 Scam Report Power Point presentation;* 2016.

[12] Ibid.

2.4 Business scams

In 2016, the ACCC received 5953 reports from businesses, with $3 784 779 reported lost. This represents a 66 per cent increase in contacts and a 31 per cent increase in reported losses from 2015. The average loss was $10 631. Table 9 provides a breakdown of scam reports by business size.

Attacks on businesses continue to increase in frequency and sophistication. Increasingly, cyber attackers are using social engineering tactics to manipulate employees, access computer networks and masquerade as 'trusted insiders'.[13] The alarming increase in reports to the ACCC in 2016 suggests that such attacks, particularly through phishing, are a serious ongoing threat for businesses.

Table 9: Breakdown of scam reports by business size

Employees	Number of reports	Percentage of reports	Amount lost
Micro (0–4 staff)	1 787	30.02%	$1 166 025
Small (5–19 staff)	1 491	25.05%	$1 085 058
Medium (20–199 staff)	768	12.90%	$242 839
Large (over 200 staff)	352	5.91%	$153 257
Blank	1 555	26.12%	$1 137 600

The majority of reports to Scamwatch were from those identifying as a micro and small business. Of the $3.8 million lost, over $2 million were attributed to micro and small businesses.

Small businesses—in focus

All businesses are vulnerable to scams, however small businesses are particularly vulnerable given the impact scams can have on their bottom line. The damage caused by scams extends beyond financial, including losses in time and productivity in addition to causing significant stress to business owners and staff.[14] In March 2016, the Canadian Independent Federation of Business released a report outlining the impact of fraud on small businesses in Canada. Some of the key findings of the report include:

- One out of every five small business owners in Canada had been a victim of fraud in 2015, costing on average CAN$6200 per business.
- The most common scams to hurt small businesses are fraudulent payments, email scams and directory fraud.
- Small businesses spent an average of CAN$2900 on fraud prevention in the last year.
- Most small business owners reported that the stress and hassle of fraud are worse than the financial losses.
- When it comes to reporting scams, 44 per cent of small businesses victimised by fraud don't report it.

A full copy of the report can be found at www.cfib-fcei.ca.

[13] Social engineering, in the context of scams, refers to a technique used by fraudsters to trick, deceive or manipulate their victims into sending money or divulging confidential information.

[14] Canadian federation of Independent Business, *'Fraud—a big threat to small business'*, March 2016, viewed 10 April 2017, /www.cib-fcei.ca/cfib-documents/rr3391.pdf

Overview of scams impacting businesses

Appendix 3 provides an overview of scams reported by businesses to the ACCC by scam category. Much of the large increase in reported losses is attributable to hacking, including hacking to phish for personal information or install malware.

The commonly reported scams targeting businesses include false billing scams, buying and selling scams for office supplies as well computer hacking to obtain personal information or install malware. Notably, losses due to hacking increased from $213 990 in 2015 to $1 718 836 million in 2016.

Hacking
2015
$213 990
loss
2016
$1 718 836
loss

Table 10: Business reports by contact method

Contact method	Reports	Percentage
Email	4 019	68%
Phone	1 025	17%
Mail	452	8%
Internet	189	3%
In person	75	1%
Text message	66	1%
Fax	36	1%
Social networking / online forums	27	0%
Mobile apps	14	0%
N/A	50	1%
Grand total	**5 953**	**100%**

The 2016 data demonstrates that businesses should be particularly wary of email and phone based scams. Common scams in 2016 included:

- Business email compromise scams—is a form of hacking and is linked to the significant increase in losses in the hacking category for 2016. These scams operate by the scammer obtaining access to a business' email address and customer lists, either through a virus or successful phishing attack. These scams come in various forms, however typically the scammer pretending to be from the business sends an email (purportedly from upper management) to the business' customers, advising of new payment arrangements and requesting an immediate wire or bank transfer to a new account. In other cases, the scammer will impersonate the chief executive officer of the business and send an internal email to the accounts department redirecting payment of an invoice to a fraudster. These emails look legitimate as they appear to come from the correct email address and closely resemble genuine emails.
- Ransomware—ransomware is a type of virus that infects computer systems and encrypts the device to prevent user access until payment in the form of bitcoins or wire transfer is made to unlock it. In 2016, reports indicated that there was an increase in ransomware emails to businesses, purportedly from legitimate companies such as Australia Post or utility providers. These emails ask the recipient to follow a link or open an attachment causing malicious software to be downloaded.
- False billing scams—false billing scams generally request businesses to pay fake invoices for advertising, domain name renewals or office supplies. These scams take advantage of the fact that the person handling the administrative duties for the business may not know whether any promotional advertising or office supplies have been requested.
- Investment scams—these scams come in many guises including sports investment or stock broker scams, superannuation schemes or managed funds. They are often promoted as business opportunities and promise inflated returns.

Often these 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 financial and reputational risks to business.

Victim's story: Sierra is stung by a business email scam

Sierra owns a plumbing supplies business. One day she received an email with an attachment, from what appeared to be a prospective supplier from China. Sierra opened the attachment but nothing happened and the document was blank. Believing it was an error she thought nothing of it.

A week later, Sierra received a call from a customer. He was calling to follow up on an email he had received from Sierra advising him that her payment details had changed and she was seeking payment of his outstanding account. Sierra had never sent this email but after calling around she found that all her regular customers had received one and unfortunately, one customer had paid almost $25 000 to the 'new account'.

Sierra then discovered that she had been scammed, along with her clients.

Note: *The story above is based on one or more real scam reports received by the ACCC. For privacy purposes the names of the victims have been changed.*

Consumers and businesses alike are affected by phishing attacks from scammers. The Verizon 2016 Data Breach Investigations Report below highlights some findings from its examination of data breaches across several countries.

Verizon 2016 Data Breach Investigations Report

Verizon is one of the largest communication technology companies, which amongst other things, helps customers prepare and recognise cyber attack trends and provides tips on how to combat them. Verizon's 2016 Data Breach Investigations Report is its ninth report on cybersecurity. The Report examines over 100 000 incidents, including 2260 confirmed data breaches across 82 countries, with data input from 67 contributors including security providers, law enforcement and government agencies.

Some findings in the Report in relation to 'phishing attacks' include:

- 63 per cent of confirmed data breaches involved leveraging weak, default or stolen passwords.
- The majority of phishing cases feature phishing as a means to install persistent malware.
- 30 per cent of phishing messages were opened by their intended target and about 12 per cent of recipients clicked on the malicious attachment or link.
- The main perpetrators of phishing attacks are organised crime syndicates (89 per cent).
- Of 636 000 phishing emails, approximately three per cent of targeted individuals alerted management to a possible phishing email.
- In 93 per cent of cases data was stolen and systems were compromised in minutes or less. In 83 per cent of cases victims took weeks or more to discover the breach.

The full report and tips on how to stay immune from cyber attacks is available on www.verizonenterprise.com.

The ACCC provides tips on how businesses can protect themselves from scams on its Scamwatch website (www.scamwatch.gov.au) and in its publication, *The little black book of scams* (www.accc.gov.au/publications/the-little-black-book-of-scams). A hard copy of this publication can be ordered from the website.

3. Scams targeting Indigenous consumers

The ACCC has been monitoring data for scams targeting Indigenous peoples in accordance with the enduring priority the ACCC placed on Indigenous consumer protection in 2016.

3.1 Scam reports from Indigenous peoples

In 2016, the ACCC received 1499 reports from people identifying as having an Indigenous background, nearly twice as many as in 2015. Losses in this group totalled $1 471 282 million. This represents just less than one per cent of total reports received by the ACCC in 2016 and nearly two per cent of total losses.

Appendix 4 provides a table of scams reported in 2016 by those identifying as having an Indigenous background. Overall, the scams reported by Indigenous peoples broadly reflected the trends seen across all scam categories in 2016, with some notable differences. Advance fee fraud was the most commonly reported scam by Indigenous peoples as compared to phishing, which was the highest for the total population.

Reported losses by Indigenous peoples were skewed by two large individual losses in the dating and romance ($800 000) and inheritance ($300 000) categories. This has contributed to an increase in the average loss from $7142 in 2015 to $8174 in 2016.

Table 11: Scam reports by contact method

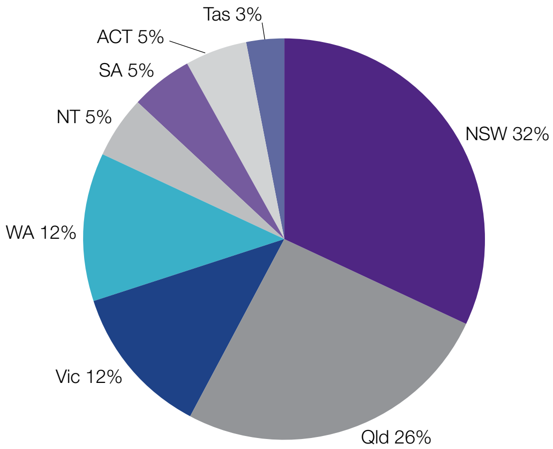
Contact method	Reports	Percentage
Email	542	36%
Phone	342	23%
Internet	204	14%
Social networking / online forums	136	9%
Text message	107	7%
In person	72	5%
Mail	51	3%
Mobile apps	33	2%
Fax	9	1%
Not provided	3	0%
Grand total	**1 499**	**100%**

Similar to the national statistics, scammers largely made online contact (internet, social networking, email and mobile apps) with Indigenous peoples, with emails being the most dominant contact method.

Table 12: Scam reports by gender

Gender	Reported loss	Percentage of loss	Reports	Percentage of reports	Reports with loss
Female	$994 093	67.6%	759	50.6%	93
Male	$451 265	30.7%	648	43.2%	78
Not specified	$25 924	1.8%	92	6.1%	9
Grand total	$1 471 282	100%	1 499	100%	180

Figure 5: Scam report location by state and territory 2016



Victim's story: Francis has faith his money will return

Francis, who lives in a remote area in the Northern Territory, received a phone call from James who claimed to be a banker at The Bank of Ghana. James told Francis that he worked closely with the President of Ghana and that due to some lucrative business deals he was going to be rich soon. James said that he needed an investor, so that he could finalise his deal and told Francis that he could also be very rich if he invested with him. Francis thought this was a really good deal and directly transferred $3500 to the scammer. Francis didn't hear anything from James and after a couple of weeks he contacted James, who told him that he would receive his investment any day now and that he needed to have faith. Each week James would tell Francis that he just needed to have faith and wait a little longer.

A year later, Francis' daughter found out what had happened and had to tell her father that James was not who he said he was and he had been the victim of a scam.

Note: The story above is based on one or more real scam reports received by the ACCC. For privacy purposes the names of the victims have been changed.

Northern Territory Indigenous scam project

As part of its broader Indigenous outreach activities, the ACCC has conducted extensive work on scams awareness in regional and remote parts of Australia.

Scam workshops for the Indigenous community

In 2016 the ACCC developed a pilot project aimed at reducing scams impacting Indigenous consumers. The project analysed international financial transactions being sent from remote Indigenous communities in the Northern Territory to overseas countries. This helped to identify whether people living in remote Indigenous communities were potentially being targeted by scammers, and were sending money to countries of concern where no genuine relationship existed.

Several areas in the Northern Territory were identified as potential targets for scammers. These areas will be the focus of targeted scams awareness workshops in 2017.

Sizzle to raise awareness on scams in the Indigenous community

In 2016, the ACCC hosted a community barbecue in Katherine, Northern Territory, after becoming aware of a number of people being affected by scams in the area. The purpose of the barbecue was to build networks within the community and raise awareness of common techniques used by scammers to lure victims.

The ACCC showcased the different types of scams people could be exposed to through emails or other contacts. The ACCC also provided copies of what appeared to be 'legitimate' correspondence from business such as Apple iTunes, Telstra, the Australian Taxation Office, and the Department of Human Services. This led to informative discussions on what to look out for and, importantly, who to talk to if something seems suspicious.

The ACCC has also used social media to promote scams awareness in Indigenous communities. The 'ACCC—Your Rights Mob' page on Facebook was originally designed for the Tiwi Islands however, has been expanded to be an avenue for all Australians and regular posts are made on being aware of the different types of scams.

The Indigenous consumers Facebook page has been very popular since it was launched and has proven to be an effective method to communicate directly with remote Indigenous consumers and provide consumer advice—Deputy Chair, Delia Rickard

In 2016 the ACCC launched two short films at an event hosted by the Central Aboriginal Media Association in Alice Springs. One of the films, titled 'Too Good To Be True', features a young Indigenous man getting advice from his Aunty on how to avoid being scammed.

Too many Indigenous consumers lose significant amounts of money to scams. These films try to inform, entertain and empower Indigenous consumers about their rights—Delia Rickard

The video can be accessed at http://www.accc.gov.au/about-us/information-for/indigenous-consumers.

4. Disruption & enforcement

Disruption is a key strategy used by the ACCC to tackle scams. In this context, disruption focuses on activities designed to interrupt and impede scams before victims are harmed or to prevent further harm.

Most scams tend to operate from foreign jurisdictions using sophisticated technology, making it difficult for law enforcement agencies to identify scammers and prosecute them. To combat this, the ACCC and other agencies use disruption methods to minimise and prevent harm to victims.

This chapter outlines efforts undertaken by the ACCC and other government agencies to deter scam activities.

4.1 Scam disruption activities

In addition to education, disruption activities provide cost effective alternatives for law enforcement agencies to prevent or restrict scam operations, without having to locate or identify the scammer. Instead, the focus is on collaborative efforts between government agencies and industry to identify intervention opportunities and policies. This includes:

- working with intermediaries such as telecommunication providers and social media platforms that enable scammers to connect with their victims and working with financial institutions, such as banks, to stop the flow of funds to scammers
- providing timely warnings to better educate consumers that utilise legitimate services
- interrupting the sending of funds.

In 2016, the ACCC's key disruption activities focused on relationship scams and working with intermediaries to bolster their scam prevention efforts.

Disrupting relationship scams

The ACCC continued to disrupt relationship scams in 2016. The Scam Disruption Project, which commenced in August 2014 targets scam victims in NSW, Tasmania, ACT, VIC and NT (scam disruption in WA, SA and QLD are undertaken by other agencies). The project uses financial intelligence to identify potential victims sending funds to high risk destinations and advises them via letter that they may be the target of a scam.

The ACCC has sent more than 9066 letters since the project began in August 2014, with over 2834 of these sent to potential scam victims in 2016. Of those that were sent a letter, 74 per cent stopped sending money within six weeks. In 2016, the project detected that fund transfers to high-risk jurisdictions were down by almost 15 per cent from $8.7 million in 2015 to $7.5 million in 2016.

Since 2013, Western Australia Department of Commerce (WA OFT) and South Australia Police (SA Police) have undertaken similar projects to tackle relationship scams. The following figures highlight the success of both disruption projects:

- Project Disrepair (SA Police)—in 2016 fund transfers to known high-risk jurisdictions were down by $586 070 on the previous year, with approximately $900 000 sent in 2016. SA Police also noted a 14 per cent decrease in the number of people sending money to West African countries.
- Project Sunbird (WA OFT)—since 2013 WA has sent over 6100 letters. Of those who received a first letter, 75 per cent stopped sending money within three months. Those who continued sending money received a second personalised letter after which about 58 per cent stopped sending funds. In 2016 WA identified over 1100 potential victims who sent just over $3 million to West Africa.

Disrupting scams on social media platforms and through intermediaries

Most scam activities cannot occur without using the services that people use to connect, communicate and transact. Money transmitters, banks, social networking platforms, email providers and telecommunications services are all integral to the scammer's ability to connect with their victims.

The ACCC recognises the important role intermediaries and platform providers have to protect their customers from fraudsters. Accordingly, in 2016 the ACCC began work on a pilot program with scam intermediaries to disrupt scams and reduce money lost by consumers.

The ACCC collaborates with banks and social media platforms

In 2016, the ACCC met with nine major social media and financial companies to promote better approaches to scam prevention. The participants in this pilot project were the Commonwealth Bank of Australia, Westpac, National Australia Bank, Australia and New Zealand Banking Group, Paypal, MoneyGram, Western Union, Apple and Facebook. The ACCC is also starting to work with telecommunication providers, including Telstra.

In May 2017, the ACCC intends to update its Scamwatch reporting webform so that consumers who report scams can elect for their report to be shared directly with an identified intermediary company. In upcoming meetings with intermediaries the ACCC intends to facilitate the direct provision of these reports (where permission is provided), to allow them to continuously inform and refine their scam prevention systems.

By sharing insights drawn from reports to Scamwatch and other intermediaries the ACCC has provided these companies with information and initiatives that allow them to strengthen their scam prevention approaches.

The ACCC will also highlight good practices with intermediaries by focusing on the best aspects of each of the intermediary companies' approaches to scam prevention. The ACCC will provide advice to businesses on how to identify scams, and how best to intervene where they are identified.

Given that social media platforms are fast becoming the preferred contact method for scammers, the ACCC is also actively engaged with Facebook in relation to disrupting scams. In particular, the ACCC has provided and will continue to provide Notifications of Scam Activity to Facebook when high-priority scams are detected on their platform.

4.2 Enforcement activities

The vast majority of scammers operate from overseas, making it difficult to take enforcement action against them. However, where appropriate the ACCC will undertake enforcement action against the perpetrators of scams, particularly where the trader has a close link to Australia and it is likely to have the potential to deter others who may be considering engaging in unscrupulous conduct.

In 2016, the ACCC initiated proceedings against ABG Pages Pty Ltd and an individual, allegedly involved in misleading and deceptive or scam-like conduct.

ABG Pages Pty Ltd (ABG Pages)

Since 2009, ABG Pages has offered an online business directory service to a range of customers, including small businesses. In December 2016, the ACCC instituted proceedings in the Federal Court against ABG Pages and an individual, alleging misleading or deceptive conduct, false or misleading representations, undue harassment and systemic unconscionable conduct in its dealings with small businesses.

ABG Pages had been cold calling businesses and offering to sell one or more of their available listings on their online business directory. The ACCC alleges that the conduct of ABG resulted in a number of small businesses paying significant amounts of money to ABG Pages for advertising they did not want.

The ACCC alleges that ABG Pages breached the Australian Consumer Law by:

- using high pressure sales tactics to sell listings in its online business directory
- misleading businesses into entering one or more contracts
- refusing to cancel contracts which customers did not want and did not intend to enter into
- refusing to accept customers' attempts to cancel contracts
- misleading businesses about the total duration and the total price of contracts
- misleading businesses into entering into second or subsequent contracts for additional listings
- unduly harassing three customers by repeatedly contacting them for payments.

The ACCC alleges that this conduct was part of a system of unconscionable conduct by ABG Pages.

The ACCC is seeking penalties, declarations, injunctions, a disqualification order against the individual, findings of fact, corrective notices and costs.

5. Education and engagement

Education and awareness raising is a key tool in the ACCC's efforts to minimise the impact of scams on the community. The online, technological and global nature of scams presents significant challenges in prosecuting scammers. Therefore, empowering individuals with knowledge about scams and coordinating awareness raising activities with domestic and overseas entities is essential in combating scams.

This chapter outlines the ACCC's education initiatives and efforts to collaborate with various agencies and industry stakeholders to raise awareness of scams.

5.1 Education

Scamwatch

The ACCC's Scamwatch website (www.scamwatch.gov.au) educates the public on how to recognise, avoid and report scams.

Scamwatch has significant brand awareness amongst Australians, with government departments, media, police forces and consumer groups directing people to the website for information on scams.

In 2016, the Scamwatch website received 1 837 458 unique users—an increase of 18 per cent from 2015. Although the majority of users were located in Australia, Scamwatch also had users from international locations.

Scamwatch radar alert service

Scamwatch runs a free subscription service providing information on emerging scams through email alerts. In 2016, the subscriber network reached 47 965 subscribers, an increase of 9724 from 2015.

The ACCC issued 13 Scamwatch radars in 2016 to warn Australians about the imminent risk of scams, including those relating to current events and trends, such as census scams; government impersonation scams; scams at tax time; Christmas and Valentine's Day. A full list of the Scamwatch radar alerts issued in 2016 can be found on the Scamwatch website. Eleven of these radars were also issued as media releases on the ACCC's mainstream website and received wider media coverage.

Scamwatch Twitter (@Scamwatch_gov)

Twitter allows Scamwatch to reach consumers, businesses and the media in real time as scams emerge. In 2016, Scamwatch Twitter posted 243 tweets and retweets to its 12 500 followers.

Revised edition of *The little black book of scams*

The little black book of scams is one of the ACCC's most popular educational resources and is often adapted by agencies overseas. In 2016, 133 234 copies of the book were distributed, with 13 624 downloads and 32 590 web page visits.

The publication highlights the most common scams that target Australians, explains tools used by scammers to trick people, and offers tips on how individuals can protect themselves.

In 2016 *The little black book of scams* was revised to provide new information about trending scams such as threat and penalty scams and new techniques used by scammers to defraud victims.

scamwatch.gov.au
1 837 458 users
47 965 subscribers
13 radars

twitter
243 tweets
12 500 followers

Little Black Book of Scams
13 624 downloads
32 509 visits
133 234 copies

Media and communications activity

The ACCC proactively engaged in regular media and communications activity throughout 2016 to generate community awareness of scams targeting Australians. The main media event for 2016 was the Fraud Week campaign—'Wise up to scams'—which included multiple television and radio interviews and release of the 2015 *Targeting scams* report.

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.

5.2 Engagement

The Australasian Consumer Fraud Taskforce

The Australasian Consumer Fraud Taskforce (ACFT), established in 2005, comprises over 20 government member agencies across Australia that share responsibility for consumer protection in relation to fraud and scams activity in their jurisdictions.

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

The ACFT's main functions are to:

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

National Consumer Fraud Week

A key Taskforce initiative is National Consumer Fraud Week (Fraud Week). Fraud Week is a coordinated effort by the Taskforce to raise community awareness about scams.

2016 campaign—'Wise up to scams'

The 2016 campaign ran from 16–22 May 2016. The campaign focused on raising awareness of scams targeting older Australians (55+). Awareness raising activities highlighted ways to identify and avoid techniques used by scammers to entice older people to part with their retirement savings, particularly through dating and romance and investment scams.

Campaign highlights included:

- extensive media coverage of the 2015 *Targeting scams* activity report
- interviews and promotion through mainstream media (TV, radio and social media)
- newspaper articles and a feature in the Seniors magazine which has 300 000 subscribers Australia wide
- distribution of 10 000 magnetic cards to consumers.

2017 campaign—'Spot social media scams'

The Taskforce's 2017 Fraud Week campaign, 'Spot social media scams', will run from 15–19 May 2017. Due to the recent increase in scam reports and losses about the use of social media to target and contact prospective victims, the 2017 campaign will focus on scams targeting Australians through social media platforms. In particular, the campaign will focus on dating and romance and fake trader scams and will also provide general tips on how consumers can stay safe on social media.

To support the campaign, the ACFT will use Fraud Week to generate mainstream and social media interest to raise awareness of social media scams.

Other partnerships

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* (Cth).

AUSTRAC is Australia's anti-money laundering and counter-terrorism financing regulator and specialist financial intelligence unit. 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.

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

Australian Cybercrime Online Reporting Network

The ACCC also collaborates with ACORN, a cybercrime initiative of the Australian Government launched in 2014. ACORN is a national online system that allows the public to report instances of cybercrime.

The ACCC is working to ensure that reports about online scams received through ACORN and Scamwatch form part of the national data set of cybercrime (see section 1.2).

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

Cyber Security Strategy—National Awareness Program

In 2016, the ACCC became a member of the recently launched Cyber Security National Awareness Program (CSNAP). Led by the Attorney General's Department, CSNAP brings together a number of government agencies to strengthen Australia's cyber security and raise public awareness of cyber security risks.

Further information about CSNAP is available at www.ag.gov.au.

The International Consumer Protection and Enforcement Network

The ACCC is also a member of the International Consumer Protection and Enforcement Network (ICPEN), a network comprised of 58 governmental consumer protection authorities around the globe. The network enables authorities to share information and combat emerging consumer problems with cross-border transactions in goods and services, such as e-commerce fraud and international scams. Fraud Week is conducted as part of ICPEN's Global Fraud Prevention initiatives.

Another important ICPEN initiative is econsumer.gov, a website portal featuring a global online complaints mechanism in multiple languages, which consumers can use to report complaints about online and related transactions with foreign companies.

Further information about ICPEN is available at www.icpen.org.

Appendix 1: Glossary of scam terms

Classified scams

Scammers use online and paper based 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.

Computing prediction software and sports investment schemes

Sports investment schemes can include computer prediction (betting software) or betting syndicates. These scams try to convince people to invest in 'fool proof' systems and software that can guarantee a profit on sporting events like football or horse racing.

Hacking

Hacking occurs when a scammer gains access to someone's personal information by using technology to break into their computer, mobile device or network.

Hitman scams

Hitman scams involve a scammer threatening someone's life unless they give in to their demands (often paying thousands of dollars).

Identity theft

Identity theft is a type of fraud that involves using someone else's identity to steal money or gain other benefits.

Mobile premium services

These scams try to attract people with offers for 'free' goods. Scammers will often create SMS competitions or trivia scam to trick people into paying extremely high call or text rates when replying to unsolicited text message on mobiles or smart phones.

419 Scams

419 scams are a form of upfront payment or money transfer scam. These scams generally offer the victim a share in a large sum of money on the condition that the victim helps the scammer transfer the money out of the country. The '419' part of the name comes from the section of Nigeria's Criminal Code which outlaws the practice. These scams now come from anywhere in the world.

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, other financial institutions or telecommunications providers. The scammers try to obtain valuable personal information like passwords, bank account or credit card numbers.

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.

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 (ransonware). These scams can target both individuals and businesses.

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.

Remote access scams

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

Sextortion scams

Sexortion scams are a form of blackmail in which the scammer uses compromising images and recordings of the victim to extort money. These scams often start on social media platforms.

Threat-based and impersonation scams

Threat-based and impersonation scams often involve the impersonation of a government agency and the use of threats (fines, arrests, deportation) to coerce the victim into paying money.

Upfront payment and advance fee frauds

Up-front payments and advance fee frauds ask the victim to send money up-front in order to later receive some sort of 'reward', such as a prize, discounted holiday, or pre-approved loan.

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 2016 scam categories by state and territory.

Australian Capital Territory

Scam category	Reported loss	Reports	Reports with loss	Less than $10k lost	Greater than $10k lost	Reports with no loss	Conversion rate
Dating & romance	$886 292	89	30	19	11	59	33.7%
Investment schemes	$501 690	43	8	4	4	35	18.6%
Hacking	$304 893	95	6	3	3	89	6.3%
Other buying & selling scams	$179 656	261	45	43	2	216	17.2%
Classified scams	$61 905	99	19	18	1	80	19.2%
Unexpected prize & lottery scams	$36 360	226	6	5	1	220	2.7%
Nigerian scams	$33 210	34	6	5	1	28	17.6%
Scratchie scams	$29 305	98	3	2	1	95	3.1%
Fake trader websites	$28 205	145	60	60	0	85	41.4%
Other upfront payment & advanced fee frauds	$25 473	448	17	17	0	431	3.8%
Inheritance scams	$20 000	58	1	0	1	57	1.7%
Remote access scams	$17 214	140	12	11	1	128	8.6%
Ransomware & malware	$13 039	195	7	6	1	188	3.6%
Overpayment scams	$12 178	66	6	6	0	60	9.1%
False billing	$9 639	435	16	16	0	419	3.7%
Job & employment	$6 451	56	5	5	0	51	8.9%
Reclaim scams	$5 000	306	1	1	0	305	0.3%
Travel prize scams	$4 087	53	4	4	0	49	7.5%
ID theft involving spam or phishing	$3 851	389	4	4	0	385	1.0%
Computer prediction software & sports investment schemes	$3 000	6	1	1	0	5	16.7%
Other business, employment & investment scams	$2 650	209	5	5	0	204	2.4%
Mobile premium services	$872	57	21	21	0	36	36.8%
Phishing	$628	873	3	3	0	870	0.3%
Fake charity scams	$395	44	1	1	0	43	2.3%
Pyramid Schemes	$333	17	1	1	0	16	5.9%
Health & medical products	$6	26	1	1	0	25	3.8%
Hitman scams	$0	57	0	0	0	57	0.0%
Psychic & clairvoyant	$0	4	0	0	0	4	0.0%
Insufficient data provided	$0	9	0	0	0	9	0.0%
Grand Total	**$2 186 332**	**4 538**	**289**	**262**	**27**	**4 249**	**6.4%**

New South Wales

Scam category	Reported loss	Reports	Reports with loss	Less than $10k lost	Greater than $10k lost	Reports with no loss	Conversion rate
Dating & romance	$9 382 177	865	234	144	90	631	27.1%
Investment schemes	$7 153 584	479	122	55	67	357	25.5%
Other buying & selling scams	$1 242 119	2 901	544	514	30	2 357	18.8%
Other upfront payment & advanced fee frauds	$1 114 239	4 936	264	233	31	4 672	5.3%
Hacking	$827 489	1 178	62	46	16	1 116	5.3%
Computer prediction software & sports investment schemes	$790 774	72	27	14	13	45	37.5%
Inheritance scams	$687 620	789	16	7	9	773	2.0%
Remote access scams	$609 039	2 110	176	161	15	1 934	8.3%
Other business, employment & investment scams	$546 965	1 734	89	71	18	1 645	5.1%
Unexpected prize & lottery scams	$415 646	1 860	70	62	8	1 790	3.8%
Nigerian scams	$413 320	293	37	28	9	256	12.6%
Fake trader websites	$321 389	1 335	579	574	5	756	43.4%
Reclaim scams	$292 473	4 327	73	67	6	4 254	1.7%
ID theft involving spam or phishing	$288 975	4 051	65	58	7	3 986	1.6%
Classified scams	$267 770	920	139	134	5	781	15.1%
Scratchie scams	$167 959	277	11	7	4	266	4.0%
Job & employment	$166 572	628	36	34	2	592	5.7%
False billing	$149 549	4 372	161	158	3	4 211	3.7%
Phishing	$103 679	8 063	65	65	0	7 998	0.8%
Pyramid Schemes	$97 150	94	10	8	2	84	10.6%
Ransomware & malware	$82 218	1 885	74	73	1	1 811	3.9%
Overpayment scams	$68 158	742	53	52	1	689	7.1%
Hitman scams	$60 000	299	4	2	2	295	1.3%
Fake charity scams	$30 177	307	25	23	2	282	8.1%
Health & medical products	$19 805	225	36	36	0	189	16.0%
Travel prize scams	$17 462	264	23	23	0	241	8.7%
Mobile premium services	$14 137	586	202	202	0	384	34.5%
Psychic & clairvoyant	$13 614	41	5	4	1	36	12.2%
Insufficient data provided	$0	109	0	0	0	109	0.0%
Grand Total	**$25 344 059**	**45 742**	**3 202**	**2 855**	**347**	**42 540**	**7.0%**

Northern Territory

Scam category	Reported loss	Reports	Reports with loss	Less than $10k lost	Greater than $10k lost	Reports with no loss	Conversion rate
Dating & romance	$357 825	112	33	26	7	79	29.5%
Investment schemes	$215 017	18	7	5	2	11	38.9%
Other business, employment & investment scams	$66 897	71	5	3	2	66	7.0%
Other upfront payment & advanced fee frauds	$55 048	128	25	23	2	103	19.5%
Other buying & selling scams	$52 672	112	35	34	1	77	31.3%
Fake trader websites	$50 046	48	22	21	1	26	45.8%
Classified scams	$40 825	29	10	9	1	19	34.5%
Hacking	$34 344	51	3	2	1	48	5.9%
Nigerian scams	$19 512	40	9	9	0	31	22.5%
ID theft involving spam or phishing	$13 737	117	4	4	0	113	3.4%
Inheritance scams	$10 400	42	4	4	0	38	9.5%
Scratchie scams	$5 090	34	1	1	0	33	2.9%
Unexpected prize & lottery scams	$4 335	83	7	7	0	76	8.4%
Computer prediction software & sports investment schemes	$4 250	5	3	3	0	2	60.0%
False billing	$3 104	146	7	7	0	139	4.8%
Job & employment	$1 825	24	2	2	0	22	8.3%
Remote access scams	$1 700	42	2	2	0	40	4.8%
Psychic & clairvoyant	$1 050	12	4	4	0	8	33.3%
Reclaim scams	$1 042	92	3	3	0	89	3.3%
Phishing	$735	198	1	1	0	197	0.5%
Travel prize scams	$684	22	2	2	0	20	9.1%
Health & medical products	$611	4	2	2	0	2	50.0%
Mobile premium services	$525	33	12	12	0	21	36.4%
Overpayment scams	$381	31	2	2	0	29	6.5%
Ransomware & malware	$130	48	1	1	0	47	2.1%
Fake charity scams	$25	13	2	2	0	11	15.4%
Hitman scams	$0	17	0	0	0	17	0.0%
Pyramid Schemes	$0	4	0	0	0	4	0.0%
Insufficient data provided	$0	4	0	0	0	4	0.0%
Grand Total	**$941 810**	**1 580**	**208**	**191**	**17**	**1 372**	**13.2%**

Queensland

Scam category	Reported loss	Reports	Reports with loss	Less than $10k lost	Greater than $10k lost	Reports with no loss	Conversion rate
Investment schemes	$5 699 315	352	94	43	51	258	26.7%
Dating & romance	$4 402 317	729	177	120	57	552	24.3%
Inheritance scams	$1 687 830	690	16	7	9	674	2.3%
Other buying & selling scams	$862 778	2 147	347	333	14	1 800	16.2%
Hacking	$765 307	858	49	37	12	809	5.7%
Other business, employment & investment scams	$740 281	1 412	70	55	15	1 342	5.0%
Other upfront payment & advanced fee frauds	$630 031	3 423	163	152	11	3 260	4.8%
Unexpected prize & lottery scams	$422 233	1 628	57	49	8	1 571	3.5%
Remote access scams	$278 757	1 242	101	94	7	1 141	8.1%
Reclaim scams	$254 969	2 774	40	36	4	2 734	1.4%
Fake trader websites	$234 020	902	375	372	3	527	41.6%
False billing	$213 246	3 474	122	120	2	3 352	3.5%
Nigerian scams	$206 556	256	26	21	5	230	10.2%
Scratchie scams	$195 317	268	14	7	7	254	5.2%
Computer prediction software & sports investment schemes	$191 573	93	29	22	7	64	31.2%
Classified scams	$163 043	729	87	82	5	642	11.9%
Job & employment	$132 833	526	32	29	3	494	6.1%
Phishing	$108 294	5 385	36	34	2	5 349	0.7%
Pyramid Schemes	$100 304	89	9	8	1	80	10.1%
ID theft involving spam or phishing	$79 135	2 712	40	38	2	2 672	1.5%
Ransomware & malware	$51 844	1 297	53	52	1	1 244	4.1%
Health & medical products	$29 128	144	34	34	0	110	23.6%
Travel prize scams	$25 436	222	12	12	0	210	5.4%
Overpayment scams	$22 264	732	20	20	0	712	2.7%
Hitman scams	$20 339	300	6	5	1	294	2.0%
Fake charity scams	$9 486	296	16	16	0	280	5.4%
Mobile premium services	$8 271	447	165	165	0	282	36.9%
Psychic & clairvoyant	$1 186	30	4	4	0	26	13.3%
Insufficient data provided	$0	86	0	0	0	86	0.0%
Grand Total	**$17 536 093**	**33 243**	**2 194**	**1 967**	**227**	**31 049**	**6.6%**

South Australia

Scam category	Reported loss	Reports	Reports with loss	Less than $10k lost	Greater than $10k lost	Reports with no loss	Conversion rate
Investment schemes	$1 500 096	112	31	10	21	81	27.7%
Dating & romance	$793 783	241	68	46	22	173	28.2%
Other upfront payment & advanced fee frauds	$213 213	1 502	67	61	6	1 435	4.5%
Computer prediction software & sports investment schemes	$184 943	19	9	6	3	10	47.4%
Other buying & selling scams	$172 029	666	122	119	3	544	18.3%
Other business, employment & investment scams	$136 425	539	22	20	2	517	4.1%
Unexpected prize & lottery scams	$102 015	640	17	14	3	623	2.7%
ID theft involving spam or phishing	$96 678	1 035	17	14	3	1 018	1.6%
Scratchie scams	$81 326	279	7	4	3	272	2.5%
Inheritance scams	$80 000	246	5	3	2	241	2.0%
Hacking	$66 088	308	11	8	3	297	3.6%
Remote access scams	$63 456	496	36	35	1	460	7.3%
Fake trader websites	$60 193	293	111	110	1	182	37.9%
Job & employment	$50 256	228	10	9	1	218	4.4%
Classified scams	$45 785	246	28	27	1	218	11.4%
Overpayment scams	$41 206	252	14	13	1	238	5.6%
Phishing	$39 919	2 320	17	15	2	2 303	0.7%
Travel prize scams	$33 811	131	13	12	1	118	9.9%
Reclaim scams	$30 633	1 908	25	25	0	1 883	1.3%
Fake charity scams	$30 523	83	9	8	1	74	10.8%
Pyramid Schemes	$29 195	44	7	6	1	37	15.9%
Nigerian scams	$28 967	96	11	11	0	85	11.5%
False billing	$18 672	1 157	40	40	0	1 117	3.5%
Ransomware & malware	$13 958	485	22	22	0	463	4.5%
Health & medical products	$4 243	57	8	8	0	49	14.0%
Psychic & clairvoyant	$4 000	10	1	1	0	9	10.0%
Mobile premium services	$1 072	138	43	43	0	95	31.2%
Hitman scams	$0	107	0	0	0	107	0.0%
Insufficient data provided	$0	24	0	0	0	24	0.0%
Grand Total	**$3 922 485**	**13 662**	**771**	**690**	**81**	**12 891**	**5.6%**

Tasmania

Scam category	Reported loss	Reports	Reports with loss	Less than $10k lost	Greater than $10k lost	Reports with no loss	Conversion rate
Investment schemes	$656 217	45	18	9	9	27	40.0%
Dating & romance	$424 102	98	15	8	7	83	15.3%
Hacking	$223 600	93	3	2	1	90	3.2%
Unexpected prize & lottery scams	$57 589	229	9	7	2	220	3.9%
Computer prediction software & sports investment schemes	$51 950	13	8	7	1	5	61.5%
Other buying & selling scams	$39 499	212	36	36	0	176	17.0%
Other upfront payment & advanced fee frauds	$39 404	331	14	13	1	317	4.2%
Other business, employment & investment scams	$38 620	149	8	6	2	141	5.4%
Scratchie scams	$34 000	135	3	2	1	132	2.2%
Remote access scams	$15 261	157	14	14	0	143	8.9%
Fake trader websites	$14 463	81	32	32	0	49	39.5%
Classified scams	$12 463	79	12	12	0	67	15.2%
Fake charity scams	$6 000	30	1	1	0	29	3.3%
Reclaim scams	$4 700	234	1	1	0	233	0.4%
Inheritance scams	$4 000	86	1	1	0	85	1.2%
ID theft involving spam or phishing	$1 675	263	3	3	0	260	1.1%
Phishing	$1 156	496	6	6	0	490	1.2%
Ransomware & malware	$1 066	133	3	3	0	130	2.3%
Mobile premium services	$606	48	20	20	0	28	41.7%
Job & employment	$500	47	1	1	0	46	2.1%
Overpayment scams	$450	66	2	2	0	64	3.0%
False billing	$415	332	6	6	0	326	1.8%
Health & medical products	$67	14	1	1	0	13	7.1%
Travel prize scams	$0	47	0	0	0	47	0.0%
Hitman scams	$0	33	0	0	0	33	0.0%
Nigerian scams	$0	31	0	0	0	31	0.0%
Pyramid Schemes	$0	6	0	0	0	6	0.0%
Psychic & clairvoyant	$0	3	0	0	0	3	0.0%
Insufficient data provided	$0	11	0	0	0	11	0.0%
Grand Total	**$1 627 803**	**3 502**	**217**	**193**	**24**	**3 285**	**6.2%**

Victoria

Scam category	Reported loss	Reports	Reports with loss	Less than $10k lost	Greater than $10k lost	Reports with no loss	Conversion rate
Investment schemes	$5 290 665	384	88	38	50	296	22.9%
Dating & romance	$4 543 037	659	187	128	59	472	28.4%
Other upfront payment & advanced fee frauds	$3 734 310	3 800	197	179	18	3 603	5.2%
Other buying & selling scams	$852 492	2 058	375	355	20	1 683	18.2%
Other business, employment & investment scams	$727 658	1 386	85	72	13	1 301	6.1%
Inheritance scams	$683 174	535	19	14	5	516	3.6%
Reclaim scams	$443 960	2 651	50	40	10	2 601	1.9%
Hacking	$425 286	904	45	35	10	859	5.0%
Scratchie scams	$251 838	228	10	4	6	218	4.4%
Remote access scams	$246 903	1 278	78	73	5	1 200	6.1%
Computer prediction software & sports investment schemes	$235 937	54	18	10	8	36	33.3%
Fake trader websites	$231 550	981	435	432	3	546	44.3%
Classified scams	$184 820	617	82	79	3	535	13.3%
Job & employment	$144 796	566	50	48	2	516	8.8%
False billing	$137 867	2 974	125	122	3	2 849	4.2%
ID theft involving spam or phishing	$121 064	2 633	48	45	3	2 585	1.8%
Nigerian scams	$107 686	243	26	24	2	217	10.7%
Unexpected prize & lottery scams	$103 696	1 368	57	55	2	1 311	4.2%
Overpayment scams	$75 608	623	34	32	2	589	5.5%
Phishing	$68 001	4 916	44	42	2	4 872	0.9%
Psychic & clairvoyant	$65 070	37	4	2	2	33	10.8%
Ransomware & malware	$56 623	1 339	39	39	0	1 300	2.9%
Travel prize scams	$50 350	193	15	14	1	178	7.8%
Pyramid Schemes	$16 584	67	5	4	1	62	7.5%
Hitman scams	$16 199	264	6	6	0	258	2.3%
Health & medical products	$9 193	124	27	27	0	97	21.8%
Mobile premium services	$8 687	476	190	190	0	286	39.9%
Fake charity scams	$5 001	248	18	18	0	230	7.3%
Insufficient data provided	$0	61	0	0	0	61	0.0%
Grand Total	**$18 838 055**	**31 667**	**2 357**	**2 127**	**230**	**29 310**	**7.4%**

Western Australia

Scam category	Reported loss	Reports	Reports with loss	Less than $10k lost	Greater than $10k lost	Reports with no loss	Conversion rate
Dating & romance	$1 710 643	284	73	47	26	211	25.7%
Investment schemes	$1 565 603	180	62	30	32	118	34.4%
Other upfront payment & advanced fee frauds	$328 813	1 807	104	96	8	1 703	5.8%
Other buying & selling scams	$284 403	997	172	165	7	825	17.3%
Inheritance scams	$258 354	358	8	5	3	350	2.2%
Unexpected prize & lottery scams	$251 121	625	20	17	3	605	3.2%
Other business, employment & investment scams	$242 629	806	42	34	8	764	5.2%
Remote access scams	$185 349	801	49	46	3	752	6.1%
Computer prediction software & sports investment schemes	$174 986	36	13	7	6	23	36.1%
Job & employment	$161 989	456	23	19	4	433	5.0%
Reclaim scams	$129 585	977	24	21	3	953	2.5%
Fake trader websites	$110 157	417	173	172	1	244	41.5%
Hacking	$107 520	460	32	30	2	428	7.0%
False billing	$89 891	1 604	65	62	3	1 539	4.1%
Nigerian scams	$87 035	112	15	14	1	97	13.4%
Classified scams	$76 564	306	45	43	2	261	14.7%
ID theft involving spam or phishing	$49 062	1 341	13	11	2	1 328	1.0%
Phishing	$32 218	2 221	13	13	0	2 208	0.6%
Hitman scams	$20 892	168	3	2	1	165	1.8%
Fake charity scams	$17 336	90	5	4	1	85	5.6%
Ransomware & malware	$17 323	662	19	19	0	643	2.9%
Travel prize scams	$14 641	68	10	9	1	58	14.7%
Overpayment scams	$13 938	237	14	14	0	223	5.9%
Health & medical products	$9 768	83	18	18	0	65	21.7%
Mobile premium services	$6 172	225	87	87	0	138	38.7%
Scratchie scams	$5 000	10	1	1	0	9	10.0%
Pyramid Schemes	$4 210	39	4	4	0	35	10.3%
Psychic & clairvoyant	$0	4	0	0	0	4	0.0%
Insufficient data provided	$0	25	0	0	0	25	0.0%
Grand Total	**$5 955 202**	**15 399**	**1 107**	**990**	**117**	**14 292**	**7.2%**

Appendix 3: Scams reports from businesses

Scam category	Reported loss	Reports	Reports with loss	Conversion rate
Hacking	$1 718 836	144	21	14.6%
Investment schemes	$980 626	19	5	26.3%
Other buying & selling scams	$532 509	721	75	10.4%
False billing	$201 277	1 926	89	4.6%
Other upfront payment & advanced fee frauds	$102 530	447	31	6.9%
Other business, employment & investment scams	$66 172	554	33	6.0%
Fake trader websites	$62 066	93	22	23.7%
Classified scams	$39 288	158	32	20.3%
Job & employment	$38 920	67	4	6.0%
Overpayment scams	$13 503	136	3	2.2%
Ransomware & malware	$10 359	237	7	3.0%
Fake charity scams	$7 572	97	11	11.3%
Remote access scams	$4 096	43	2	4.7%
Reclaim scams	$3 060	128	2	1.6%
Health & medical products	$1 743	24	1	4.2%
Mobile premium services	$1 371	22	13	59.1%
Nigerian scams	$320	40	1	2.5%
Phishing	$300	592	1	0.2%
Travel prize scams	$151	5	1	20.0%
ID theft involving spam or phishing	$74	343	1	0.3%
Computer prediction software & sports investment schemes	$6	6	1	16.7%
Unexpected prize & lottery scams	$0	60	0	0.0%
Inheritance scams	$0	40	0	0.0%
Hitman scams	$0	18	0	0.0%
Dating & romance	$0	8	0	0.0%
Scratchie scams	$0	4	0	0.0%
Pyramid Schemes	$0	2	0	0.0%
Psychic & clairvoyant	$0	1	0	0.0%
Not provided	$0	18	0	0.0%
Grand Total	**$3 784 779**	**5 953**	**356**	**6.0%**

Appendix 4: Scam reports from Indigenous peoples

Scam category	Reported loss	Reports	Reports with loss	Conversion rate
Dating & romance	$852 182	101	19	18.8%
Inheritance scams	$320 400	39	6	15.4%
Investment schemes	$70 157	19	6	31.6%
Other upfront payment & advanced fee frauds	$51 684	145	29	20.0%
Other buying & selling scams	$43 875	124	30	24.2%
Nigerian scams	$33 344	72	13	18.1%
Job & employment	$20 720	43	5	11.6%
Unexpected prize & lottery scams	$16 172	93	7	7.5%
Fake trader websites	$12 639	44	17	38.6%
Classified scams	$9 430	35	4	11.4%
ID theft involving spam or phishing	$8 458	112	5	4.5%
Fake charity scams	$8 242	51	5	9.8%
Other business, employment & investment scams	$7 230	73	4	5.5%
Overpayment scams	$6 083	22	2	9.1%
Ransomware & malware	$3 522	38	3	7.9%
False billing	$3 194	129	6	4.7%
Hacking	$2 223	49	2	4.1%
Phishing	$725	132	4	3.0%
Health & medical products	$336	13	3	23.1%
Mobile premium services	$299	17	4	23.5%
Remote access scams	$246	22	3	13.6%
Computer prediction software & sports investment schemes	$100	7	1	14.3%
Reclaim scams	$20	65	1	1.5%
Hitman scams	$1	23	1	4.3%
Pyramid Schemes	$0	10	0	0.0%
Scratchie scams	$0	8	0	0.0%
Travel prize scams	$0	7	0	0.0%
Psychic & clairvoyant	$0	5	0	0.0%
Insufficient detail provided to classify	$0	1	0	0.0%
Grand Total	**$1 471 282**	**1 499**	**180**	**12.0%**

SCAMWATCH

www.scamwatch.gov.au