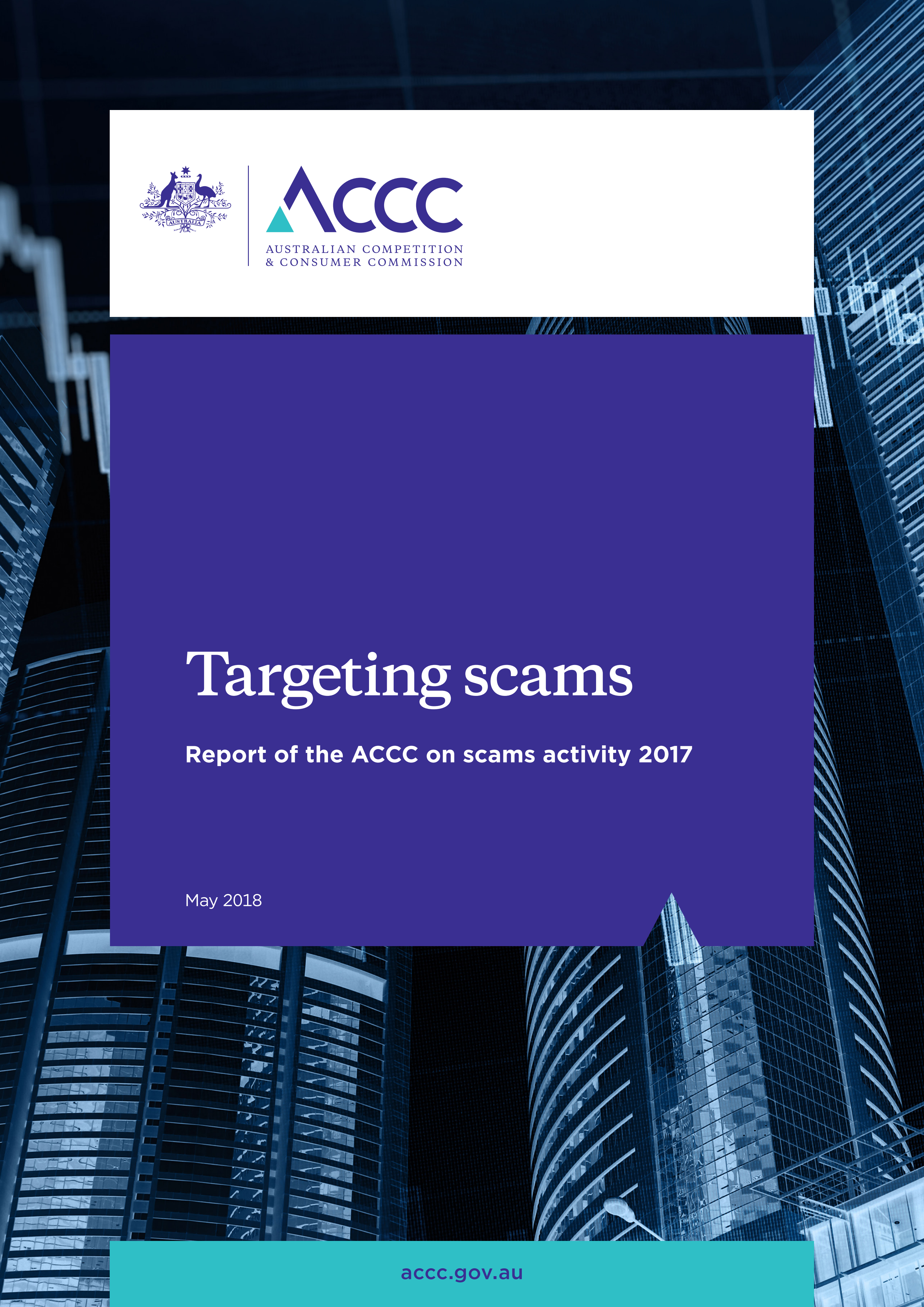


ACCC
AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

Targeting scams

Report of the ACCC on scams activity 2017

May 2018

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, Content and Digital Services, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 05/18_1240

www.accc.gov.au

Foreword

The Australian Competition and Consumer Commission's (ACCC) ninth annual report on scams activity in Australia highlights the continuing financial and emotional harm caused by scams on Australian consumers and businesses. This report seeks to inform the public on scam losses in 2017 and identify emerging trends and techniques employed by scammers to extract money and personal information from their victims.

In 2017, the ACCC, Australian Cybercrime Online Reporting Network (ACORN) and other government organisations such as the Australian Taxation Office received over 200 000 scam reports with reported losses exceeding $340 million, an increase of $40 million over 2016 losses. The ACCC received over 161 500 scam reports with $90.9 million in financial losses which represents an eight per cent increase in reported losses over 2016. These increasing losses unfortunately demonstrate the continuing harm caused by scams on the Australian public.

One of the most concerning trends of 2017 was the significant money Australians reported lost to investment scams. Losses to investment scams reported to ACORN and the ACCC exceeded $64 million in 2017. Investment scam losses reported to the ACCC increased from $23.6 million in 2016 to $31.3 in 2017, a 33 per cent increase. Analysis of investment scam reports did not reveal any particularly new techniques used by investment scammers suggesting the same tricks used in previous years remain effective. More high-value losses to investment scams were also reported to the ACCC in 2017. In 2016, there were seven reports with losses of $400 000 or more whereas in 2017, there were 20 such reports. This pushed up the average reported loss for investment scams in 2017 to $53 827 from $46 980 in 2016.

Combined losses reported to the ACCC and ACORN for dating and romance scams were over $42 million. Losses reported to the ACCC for these scams actually decreased by 19 per cent to $20.5 million from $25.5 million in 2016. However, the combined loss figure of $42 million is the same amount that was reported in 2016. This is significant for a scam which has seen continual increases in reported losses year after year. While stagnation is preferable to an increase, dating and romance scams still caused a concerning degree of financial and emotional damage to many Australians seeking a romantic relationship.

The most commonly reported scams to the ACCC in 2017 were phishing, identity theft and false billing scams. Reports to the ACCC indicated these scam types all increased in reported losses which surpassed $4.6 million in 2017. However, the true cost of these kinds of scams are often not felt right away as the scammer's primary aim is to obtain personal and banking information for future use. The ACCC received over 55 000 reports of these kinds of scams in 2017 and there is little doubt that many more were encountered but not reported. The ACCC received reports of scammers creating convincing copies of the websites and account log-in pages of many major retailers and service providers hoping to trick consumers into entering their account or banking information. From here, scammers hacked bank accounts, email addresses and even engaged in mobile number porting to get around two-step authentication processes. These reports serve as a reminder that personal and business information is a target for scammers and a gateway to our money and should be defended with robust and vigilant information security practices.

In 2017, Australian businesses were targeted by business email compromise scams and reports to the ACCC and ACORN about this scam exposed over $22.1 million transferred from businesses to scammer's accounts in 2017. Scammers infiltrate email accounts and IT systems and observe communications between clients and customers and associated financial transactions. Choosing the right target and time to act, the scammer then sends an email on behalf of the company, stating their banking details have changed and to pay future scheduled payments to a new account. From the perspective of the recipient of these emails, everything looks legitimate and they pay funds to the new account.

Scams continued to evolve with technology and social and market trends and scammers proved they are keen observers of these trends. With the increased popularity of cryptocurrency speculation in the last quarter of 2017, fake initial coin offerings and other cryptocurrency-related scams were reported to the ACCC. Scammers also capitalised on the fidget spinner craze with reports of fake offers for the must-have toy of the year. Social networking continues to increase as a means of accessing scam victims, and this year losses increased to $15.7 million. For the first time this year, more people lost money from dating and romance scams when contacted via social networking than any other contact method.

To minimise the harm caused by scams to the community, the ACCC continued its education and awareness efforts in 2017 through our social media accounts, online and printed publications and engagement with the media. *The little black book of scams* remains our most popular publication and was downloaded in electronic form 13 348 times and 162 095 physical copies were requested and distributed through government organisations, community groups and financial institutions.

We also continued our approach to combat scams with the cooperation of other government agencies through the Scams Awareness Network (SAN). The SAN, formerly the Australasian Consumer Fraud Taskforce (ACFT) is made up of 36 government regulatory agencies and departments in Australia and New Zealand and works alongside private sector, community and non-government partners to raise awareness about scams. In 2017, this group collaborated on National Consumer Fraud Week which was successful in raising awareness about scams on social media.

The international nature of scams presents a considerable challenge for law enforcement agencies but where appropriate the ACCC will take enforcement action, particularly where it is likely to have a deterrent effect on others who may be considering engaging in scam-like, unscrupulous conduct. In 2017, the ACCC instituted proceedings against Domain Name Corp Pty Ltd and Domain Name Agency Pty Ltd alleging that they engaged in misleading or deceptive conduct and made false or misleading representations to Australian businesses about the domain name services they offered.

We also issued public warning notices against the overseas-based online retailer Digital Sourcing ApS (Digital Sourcing) formerly Lux International Sales ApS (Luxstyle), which advertise beauty products on social media sites such as Facebook and Instagram. The warnings were issued after consumer complaints about the retailer sending unsolicited goods and demanding payment.

The ACCC also continued its disruption efforts by engaging with financial institutions, online classifieds sites and social media platforms to help identify scams and where possible to stop victims at the point of transferring money to scammers. These businesses were identified as key intermediaries between scammers and their victims and our engagement with them aimed to help them disrupt the ability of scammers to use their platforms. As a result of this engagement and intelligence sharing, some intermediaries were able to take additional action to return money to customers, block fraudulent transfers and remove fake advertisements from online platforms.

Scams are a complex and evolving problem affecting every demographic of Australians and continue to cause substantial financial and emotional damage. Through education, awareness raising, enforcement and disruption the ACCC and its partners hope to reduce the harm caused by scammers and equip Australians with the knowledge to identify and avoid scams.

Delia Rickard

Deputy Chair, Australian Competition and Consumer Commission
Chair, Scams Awareness Network

Contents

Glossary of scam terms

Betting and sports investment scams

Betting and sports investment scams can include computer prediction (betting software) or betting syndicates. These scams try to convince people to invest in 'foolproof' systems and software that can guarantee a profit by betting strategically on sporting events like football or horse racing.

Binary options

Binary options are a type of investment in which the buyer attempts to predict the value of a share price, currency, index or commodity at a fixed time in the future, usually in a very short period. They are very high risk because these values can move up or down unpredictably in short periods. For more information on binary options, visit ASIC's MoneySmart website at: www.moneysmart.gov.au.

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 their victim's trust with false but convincing documents and elaborate stories.

Cryptocurrency

Cryptocurrencies, also known as virtual currencies or digital currencies, are a form of electronic money. They do not physically exist as coins or notes. A cryptocurrency unit, such as a bitcoin or ether, is a digital token created from code using an encrypted string of data blocks, known as a blockchain. There are usually only a fixed number of digital currency tokens available.

Cryptocurrencies are not only used as payment systems but can also be used to execute contracts and run programs. Anyone can create a digital currency, so at any given time there can be hundreds, or even thousands, of cryptocurrencies in circulation.

Virtual currencies can be bought or sold on an exchange platform using conventional money.[1]

Dating and romance scams

Scammers take advantage of people looking for romantic partners, often via dating websites, apps or social media by pretending to be prospective companions. They play on emotional triggers to get their victims to provide money, gifts or personal details. Dating and romance scams can continue for years and cause both emotional and financial damage.

Fake charities

Scammers impersonate genuine charities and ask for donations or contact people claiming to collect money after natural disasters or major events.

False billing

False billing scams involve sending invoices to individuals or businesses demanding payment for directory listings, advertising, domain name renewals or office supplies that were not ordered. These scams often take advantage of the fact the person handling the administrative duties for a business may not know whether any advertising or promotional activities have actually been requested.

Hacking

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

[1] Cryptocurrency definition from ASIC's Moneysmart website www.moneysmart.gov.au

Health and medical products

Health and medical product scams involve scammers selling healthcare products at low prices that don't actually exist, or they make false promises about their 'cure-all' products, medicines and treatments.

Hitman scams / Threats to life, arrest or other

Hitman scams involve a scammer threatening someone's life unless they give in to their demands.

In 2017, the ACCC changed the 'Hitman' scam category to 'Threats to life, arrest or other'. The new 'Threats to life, arrest or other' captures a broader range of scams which employ the use of threats to scare victims into parting with their money.

Identity theft

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

Inheritance scams

These scams offer you the false promise of an inheritance to trick you into parting with your money or sharing your bank or credit card details.

Investment scams

Investment scams involve scammers offering a range of fake financial opportunities and the promise of quick returns. These offerings may include fake initial stock or coin offerings, brokerage services or an investment in expensive software or online trading platforms. Investment scammers often use smooth talking, glossy brochures and professional-looking websites to lure in victims.

Jobs and employment scams

Jobs and employment scams trick victims into handing over money to scammers who offer 'guaranteed' ways to make fast money or a high-paying job for little effort.

Malware and ransomware

Ransomware and malware involves a scammer placing harmful software onto a victim's computer. Malware can allow scammers access to computers, 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 (ransomware). These scams can target both individuals and businesses.

Mobile number porting

Mobile number porting occurs when a mobile phone number is transferred from one telecommunications provider to another. This happens legitimately whenever a consumer changes their provider to seek a better deal. However, scammers do this without the knowledge of the number's owner and set up their own mobile phone to receive messages to the ported number. This is usually done in order to intercept two-step authentication messages from banks or other service providers.

Mobile premium services

Scammers create SMS competitions or trivia scams to trick people into paying extremely high call or text rates when replying to an unsolicited text messages on mobile or smart phones.

'Nigerian' scams

'Nigerian' 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. These scams are also known as '419 scams' which refers to the section of Nigeria's Criminal Code which outlaws the practice. These scams now come from anywhere in the world.

Online shopping scams

Online shopping scams involve scammers pretending to be legitimate online sellers, either with a fake website or a fake ad on a genuine retailer site or social media platform.

Other business, employment and investment scams

This is a scam category in Scamwatch data designed to capture business employment and investment related scams which do not fit neatly into the description of several other scam categories. In 2017, this category contained a range of scams including scammers offering services commonly used by businesses such as web page development, search engine optimisation, small business loans and business directory listings. A revision of scam categories on the Scamwatch website in 2018 means this category will no longer appear on the Scamwatch website or future *Targeting scams* reports.

Other buying and selling scams

This is a scam category in Scamwatch data designed to capture buying and selling scams which do not fit neatly into the description of several other scam categories. A revision of scam categories on the Scamwatch website in 2018 means this category will no longer appear on the Scamwatch website or future *Targeting scams* reports.

Overpayment scams

Overpayment scams work by convincing someone to 'refund' a scammer who has sent too much money for an item the person is trying to sell. The reason for 'overpaying' often has to do with shipping the item to a remote location. Scammers often target those trying to sell something through classified websites.

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. Another form of phishing, which is performed over telephone is called 'vishing' (voice phishing) and is employed when scammers impersonate a telecommunications or utility provider to obtain personal information.

Psychic and clairvoyant

Psychic and clairvoyant scammers approach their victims by post, email, telephone or even face-to-face and make claims they see a positive event or some sort of trouble in their future. They then ask for money to remove curses or provide ongoing protection.

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.

Rebate scams / Reclaim scams

Scammers contact a victim pretending to be from the government, utility company, bank or other well-known entity and convince their victims they are entitled to a rebate or reimbursement but must pay a fee to access it.

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.

Spear phishing

Spear phishing is a more precise version of ‘phishing’ and describes a range of techniques to elicit information from a specific person or organisation. While ‘phishing’ casts a wide net and hopes to gather data from a wide set of people, spear phishing is an attempt to gather data from an identified target.

Scratchie scams

Scratchie scams take the form of fake scratchie cards that promise some sort of prize, on the condition that the ‘winner’ pays a collection fee.

Threat-based impersonation scams

Threat-based impersonation scams often involve the impersonation of a government agency or well-known company and the use of threats (for example, of fines, arrests, deportation) to coerce the victim into paying money or providing personal information. Threat-based impersonation scams are not a specific category in Scamwatch data but is a description of a technique employed by scammers.

Travel prize scams

Travel prize scams involve attempts to trick people into parting with their money to claim a ‘reward’ such as a free or discounted holiday.

Upfront payment and advanced fee frauds

Upfront payment and advanced fee frauds ask the victim to send money upfront in order to later receive some sort of ‘reward’, such as a prize, discounted holiday, or pre-approved loan. A revision of scam categories on the Scamwatch website in 2018 means this category will no longer appear on the Scamwatch website or future *Targeting scams* reports.

Unexpected prize and lottery scams

Unexpected prize and lottery scams involve scammers tricking people into paying some sort of fee in order to claim a prize or winnings from a competition or lottery they never entered.

Targeting Scams 2017

Losses

$340 million

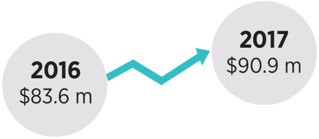
2017 combined financial losses to scams
as reported to Scamwatch, ACORN and other government agencies

$90.9 million

Amount reported lost to Scamwatch

161 528

reports to Scamwatch



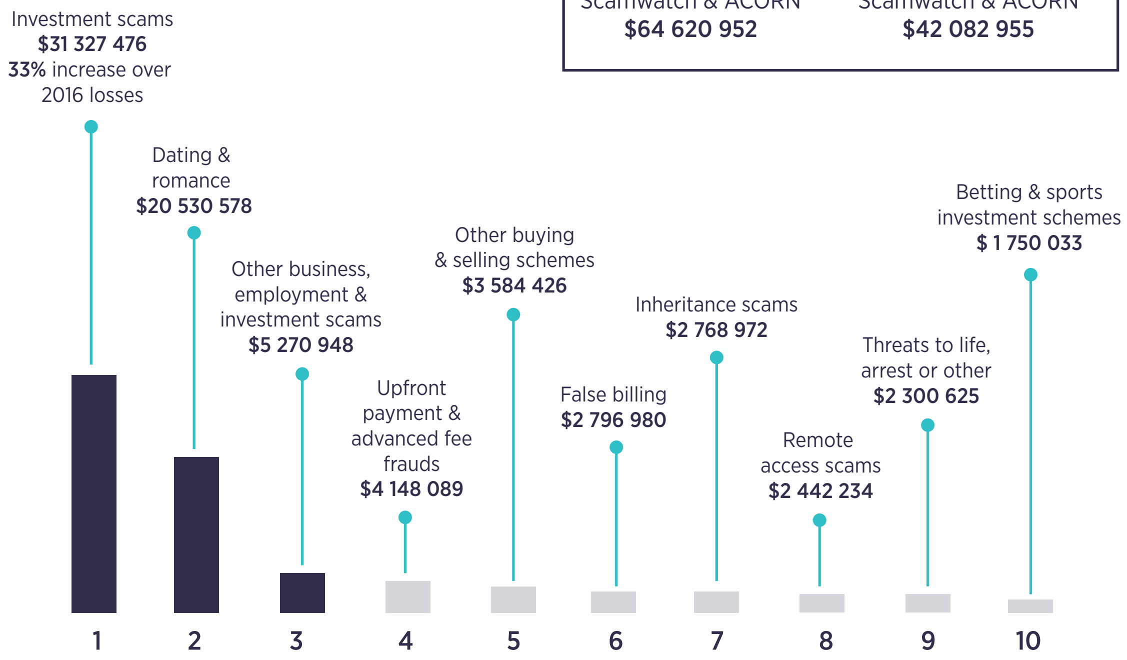
▲ **8.8%** since 2016

Average loss: **$6471**

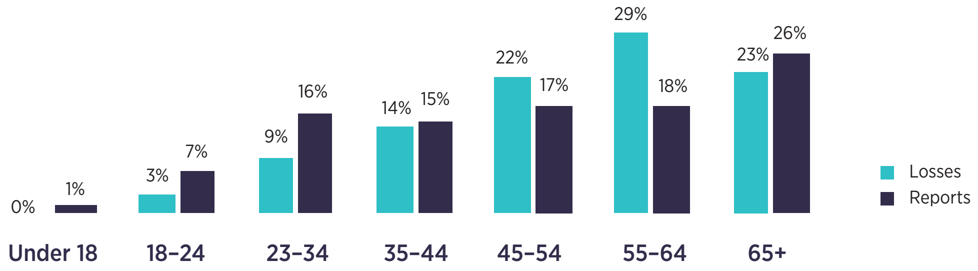
Top scams by loss

As reported to Scamwatch

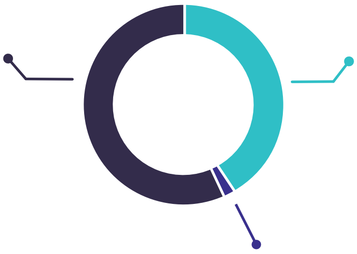
Investment scams Scamwatch & ACORN **$64 620 952**	Dating & romance scams Scamwatch & ACORN **$42 082 955**



Age



Gender



Men

$51 371 588

72 282 reports

Males were more affected by investment scams, reporting losses of **$22.8 million**.

Women

$37 908 289

85 495 reports

Females reported losing more to dating and romance scams with **$12.7 million** in losses.

Non-specified

$1 648 745

3751 reports

Top contact methods by reports

40%
Phone
65 097 reports
$29.1 million
reported lost

31%
Email
50 635 reports
$17.4 million
reported lost

12%
Text message
18 597 reports
$1.7 million
reported lost

Online-based contact methods

Scams via email, social media,
mobile apps and internet
68 351 reports (42% of all reports)
$49.9 million in reported losses

1. Snapshot of 2017

Losses and reports

- In 2017, Scamwatch, the Australian Cybercrime Online Reporting Network (ACORN) and other federal and state-based government agencies received over 200 000 reports about scams. The combined losses reported to Scamwatch and these other agencies exceeded $340 million.
- Investment scams had the highest losses reported in 2017 with reports to Scamwatch and ACORN exceeding $64.6 million.
- 'Dating and romance scams' had the next highest reported losses with over $42 million in combined reports to Scamwatch and ACORN.
- In 2017, Scamwatch received 161 528 scam reports. This represents a four per cent increase over 2016 reports which numbered 155 034. Losses reported to Scamwatch increased in 2017 to $90.9 million which is an 8.8 per cent increase over 2016 losses which totalled $83.6 million.
- Losses to investment scams reported to Scamwatch increased by 33 per cent in 2017 to $31.3 million. Losses to dating and romance scams reported to Scamwatch decreased in 2017 in comparison to 2016 from $25.5 million to $20.5 million.
- When combined with losses reported to ACORN, dating and romance losses were the same as reported in 2016 at $42 million.
- The percentage of Scamwatch reports which included a financial loss increased from 7.5 per cent in 2016 to 8.7 per cent in 2017. This means more reports included a loss.
- The average amount reported to Scamwatch from those who lost money was $6471. This is a 10 per cent decrease from the average loss in 2016 which was $7226. The lower average loss in the Scamwatch data can be attributed to a greater number of reports with lower loss amounts and these were mostly found in 'Online shopping' scams.

Demographics in Scamwatch reports

- The age range with the highest reported losses was the 55–64 range which reported losses of $21.6 million.
- Where gender was provided, women reported more scams but lost less money than men. Women reported 85 495 scams and reported losses of $37.9 million. Men reported 72 282 scams and reported losses of $51.3 million.
- Women reported losing most to dating and romance scams with $12.7 million in losses, while men were most affected by investment scams, reporting losses of $22.8 million.
- In 2017, Indigenous consumers reported $1.6 million in losses (across 1810 reports). This represents a 12 per cent increase over the $1.4 million reported losses (across 1499 reports) in 2016.

Scam contact methods in Scamwatch reports

- The top two contact methods used by scammers in 2017 were phone (40 per cent) and emails (31 per cent). Phone-based scam reports numbered 65 097 with $29.1 million in reported losses. Email-based scam reports numbered 50 635 with $17.4 million in reported losses.
- Phone call and text message-based scams increased in 2017 by 14 227 reports, but email-based scams decreased by 3433 reports.
- Phishing and identity theft scams were the most prevalent of phone-based scams with 20 220 reports but investment scams conducted over the phone resulted in the highest reported losses of $17 million.
- When combined, online-based contact methods (those delivered via email, social media, mobile apps and the internet) amounted to 68 351 reports (representing 42 per cent of all reports) and $49.9 million in reported losses.

- Reports about scams where contact was made via 'social networking/online forums' numbered 4711 in 2017 with $15.7 million in reported losses.
- Fax-based scams still occurred even in 2017 but only represented 0.1 per cent of reported scams. These scams are usually targeted at businesses.

Other scam trends

Business email compromise scams

- The ACCC received reports of over $2.1 million lost to this scam in 2017 and ACORN data indicated further losses of over $20 million resulting in combined losses of over $22.1 million. These scams involve targeted phishing and hacking of a business in order to send emails to that business's clients informing them that banking details have been changed. When the client attempts to pay the business, the money goes to the scammer's account. Another version of this scam impersonates the CEO of the company requesting money be transferred for some supposedly legitimate business purpose.

Threat-based impersonation scams

- Scamwatch data shows there were almost 33 000 reports of these scams in 2017 with over $4.7 million of reported losses. When combined with ATO data, losses exceed $7 million. Threat-based impersonation scams involve scammers pretending to represent government departments, the police or trusted companies and use threats to pressure or scare victims into giving them money or personal information.

Cryptocurrencies in scams

- The use of cryptocurrencies as a payment method in scams and scams capitalising on the popularity of investments in cryptocurrencies peaked in the last quarter of 2017. Approximately $2.1 million in losses where cryptocurrencies were a factor in the scam were reported to Scamwatch in 2017.

iTunes cards in scams

- Scammers requesting payment through iTunes cards continued in 2017 with $1.2 million in reported losses. However, this is a reduction from the 2016 reported losses of $1.6 million. In 2017, warnings were added to iTunes cards to minimise their use in scams and major retailers also displayed warnings at the point of sale to help alert potential victims before parting with their money.

Scams targeting businesses

- Scamwatch received 5432 scam reports submitted by businesses in 2017 with losses of $4.6 million.
- 60 per cent of business scams were delivered via email and money was sent to scammers via bank transfers 85 per cent of the time.
- Business email compromise scams continued to infiltrate and redirect money from Australian businesses with over $22.1 million in combined losses reported to the ACCC and ACORN.

ACCC enforcement

- In August 2017 the ACCC instituted proceedings against Domain Name Corp Pty Ltd and Domain Name Agency Pty Ltd alleging that they engaged in misleading or deceptive conduct and made false or misleading representations to Australian businesses about the domain name services they offered.
- In March and December 2017, the ACCC issued public warning notices against Digital Sourcing ApS (Digital Sourcing) formerly Lux International Sales ApS (Luxstyle) for potential breaches of the Australian Consumer Law by misleading consumers and asserting a right to payment for unsolicited goods.

Education and engagement

- In 2017, ACCC and Scamwatch media releases generated hundreds of media requests which resulted in hundreds of radio, newspaper and television interviews. These interviews were broadcast both locally and nationally and reached millions of Australians.
- The Scamwatch radar email subscription service sent 14 scam alerts to its almost 60 000 (as at 31 December 2017) subscribers in 2017.
- The Scamwatch Twitter account sent 306 tweets and retweets and grew in followers by 20 per cent to 15 744.
- The ACCC's *The little black book of scams*, which provides guidance and protection advice on scams was downloaded 13 348 times and 162 095 hard copies were distributed to a range of government organisations, community groups, financial services and individual Australians.
- The ACCC engaged in targeted scams awareness outreach to a number of Indigenous communities identified as sending money to foreign scammers. This engagement succeeded in reducing these scam based transactions by 42 per cent.
- In 2017, the ACCC engaged with a range of intermediaries whose systems and platforms are used in the course of scams. These include financial institutions, technology companies and popular online classifieds and social media platforms. As a result of this engagement and intelligence sharing, some intermediaries were able to take additional action to return money to customers, block fraudulent transfers and remove fake advertisements from online platforms.

2. 2017 scam trends[2]

2.1 Scam reports

In 2017, combined reports to the ACCC and ACORN exceeded 200 000 in number. The ACCC received 161 528 reports. This represents a four per cent increase over 2016. The majority of reports are made by the public to the scamwatch.gov.au website but the ACCC also received reports via phone and letter.

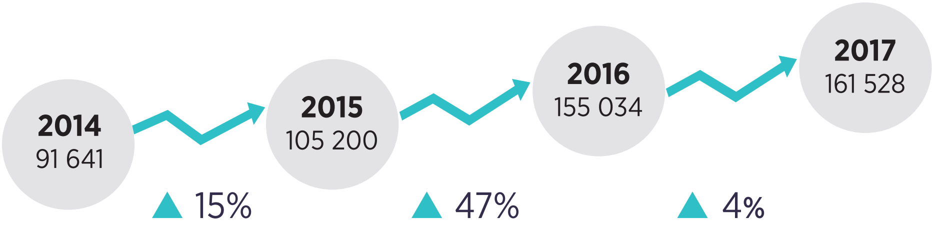
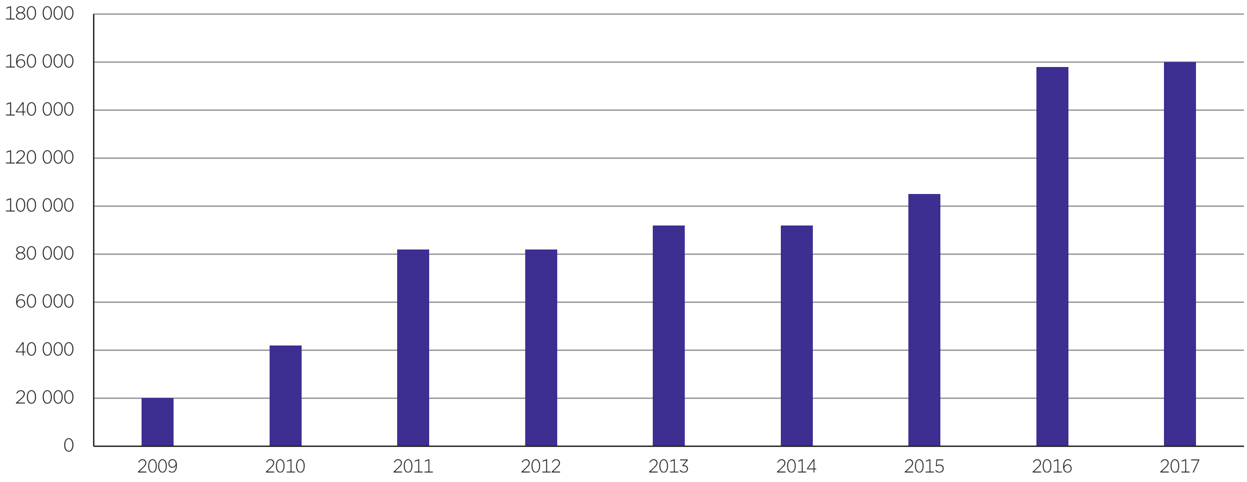


Figure 1 shows the increase over time of scams reported to Scamwatch between 2009 and 2017. 2009 was the first year reported on in the ACCC's first *Targeting scams* report released in 2010. The large increase in reports between 2015 and 2016 is attributed to a large number of bulk email-based scams.

Figure 1. Number of Scamwatch reports 2009–17



The top three most reported scam categories of 2017 were phishing, identity theft and false billing scams.[3] The 'Reports with loss' column in table 1 illustrates that these top scams are very common but were not accompanied by large financial losses. These scams are focused on gathering personal information in order to steal money from victims later through hacking for example. Combined reports to ACORN and the ACCC showed that the resulting monetary losses from the theft of personal information exceeded $45 million.

The volume of these information theft-based scams is concerning because they represent tens of thousands of attempts to obtain personal and banking details from a broad range of people. Many people do not realise they have provided their information to scammers because they do not always suffer the consequences immediately.

[2] Unless otherwise indicated, all data is based on reports provided to the ACCC by web form 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. When ACORN data is referenced, reasonable efforts have been undertaken to remove data also reported to Scamwatch.

[3] A glossary of scam terms is found at the start of this report. Alternatively, definitions of all scam categories can be found on the Scamwatch website (www.scamwatch.gov.au).

Reports to Scamwatch also showed that scammers created convincing fake websites and social media pages for most household-name businesses that Australians deal with on a daily basis like banks, supermarkets, energy companies, telecommunications companies and other popular retailers. As with other types of scams, the true numbers of phishing and identity theft scams are likely to be far greater in number than those reported to us.

In the following victim story, the hacking aspect is very possibly a result of successful phishing performed at some point in the past.

Victim story: Identity theft resulting in mobile number porting and access to bank accounts[4]

Scam category: Identity theft

Loss: $10 000

The scammer hacked into my personal email account which had soft copies of my wife's and my personal documents like driver's licence, passport, Medicare card, credit card, banking details, salary slips, contracts, academic documents etc.

The hacker stole my identity and ported my mobile number as well as my wife's and accessed our bank accounts. We managed to lock our bank account but the hacker used our identification documents to unlock them but we again managed to lock the bank accounts until we could physically visit the branch.

The hacker also performed cardless cash transactions. As per my credit rating report, the hacker has used my identity documents to access credit which I have reported as fraudulent to the credit rating agencies.

Top 10 Scamwatch categories by reports

Table 1 provides an overview of the top 10 scams by number of reports submitted to the ACCC in 2017. The 'Reports with loss' column includes the number of reports with a loss as well as what those reports represent as a percentage of the total reports for that category.

For example, in 2017, there were 26 386 reports of phishing scams but only 221, or 0.8 per cent, with a financial loss reported. This percentage is known as the 'conversion rate' and indicates how effective the scam is at extracting money from victims.

A low conversion rate suggests that either the scam is not good at extracting money from victims or its true purpose, as in the case of phishing scams, is not to get money but information. Some scams have a primary goal of obtaining money but also attempt to gather personal information in the course of the scam.

[4] All victim stories in this report are based on real reports submitted to www.scamwatch.gov.au in which the reporter provided express consent to share their story. The reports have been altered only for clarity and to protect the identity of the reporter and other parties.

Table 1: Top 10 scam categories reported to the ACCC in 2017 by number of reports[5]

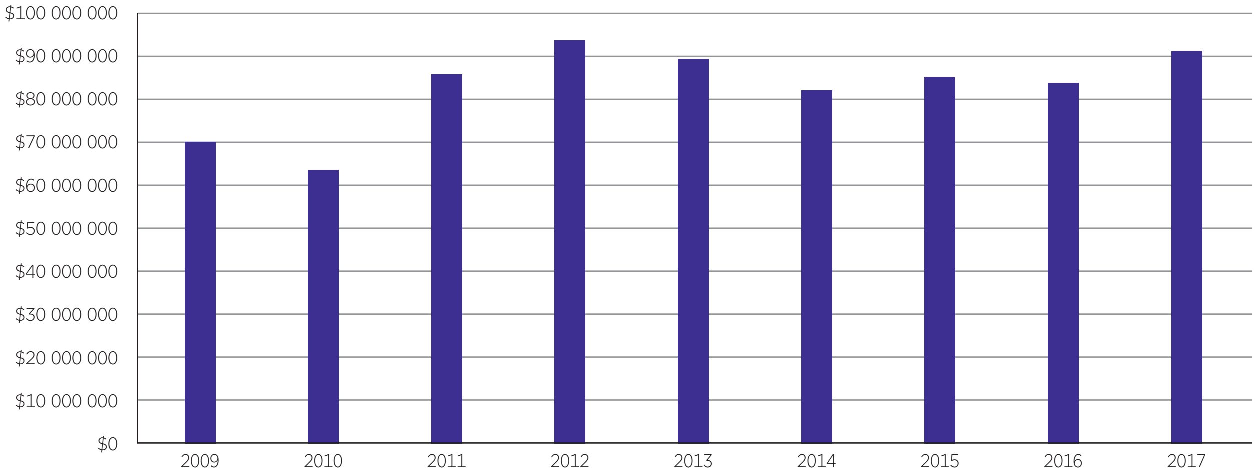
Scam category	Reports	Reported loss	Reports with loss	Change in reports since 2016
Phishing	26 386	$810 224	221 (0.8%)	▲ 5.9%
Identity theft	15 703	$1 018 543	281 (1.8%)	▲ 23.3%
False billing	13 455	$2 796 980	737 (5.5%)	▼ -8.1%
Unexpected prize and lottery scams	12 726	$1 645 380	266 (2.1%)	▲ 83.1%
Other buying and selling scams	10 279	$3 584 426	2 279 (22.2%)	▲ 4.6%
Reclaim scams	9 329	$696 836	200 (2.1%)	▼ -30.2%
Remote access scams	8 685	$2 442 234	707 (8.1%)	▲ 36.4%
Upfront payment and advanced fee frauds	8 588	$4 148 089	1 004 (11.7%)	▼ -49.0%
Threats to life, arrest or other	8 297	$2 300 625	133 (1.6%)	▲ 546.7%
Online shopping scams	6 803	$1 380 563	3 320 (48.8%)	▲ 47.8%

2.2 Financial losses to scams

In 2017, financial losses reported to the ACCC, ACORN and other state and territory government organisations exceeded $340 million. Losses reported to the ACCC totalled $90 928 622.

Figure 2 shows a comparison of losses reported to Scamwatch over the last nine years. It shows that losses in 2017 have increased and are approaching the level of losses reported in 2012.

Figure 2. Reported financial losses to Scamwatch 2009–17



According to Scamwatch reports, there were a number of scams in 2017 that increased and decreased significantly in terms of reported losses in comparison to 2016 numbers.

- Losses to investment scams reported to Scamwatch increased by 33 per cent which translates to an increase in losses of $7.6 million. Combined losses with ACORN reports brings investment scam losses to $64.6 million in 2017, an increase over the $59 million in combined losses reported in 2016.
- False billing scams reported to Scamwatch increased by 324 per cent, from $659 835 in 2016 to $2.7 million in 2017.
- Remote access scams reported to Scamwatch increased by 72 per cent representing an increase in losses of $1 million.
- On the other hand, dating and romance scams, the scam with the highest reported losses in 2016, decreased by 19 per cent. This drop in losses translates to $4.9 million less in reported losses. However, combined losses with ACORN reports for dating and romance scams in 2017 were over $42 million which is on par with combined losses reported in 2016.
- Other scam categories with a decrease in the 2017 Scamwatch reports include hacking by 40 per cent and inheritance scams by 21 per cent.

[5] Appendix 1 provides a full breakdown of Scamwatch reports for 2017.

Top 10 Scamwatch categories by losses

Table 2 provides an overview of the top 10 Scamwatch scam categories by losses in 2017.

Table 2: Overview of scams reported to the ACCC in order of reported losses

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Investment scams	$31 327 476	1 997	582 (29.1%)	▲ 32.6%
Dating and romance	$20 530 578	3 763	886 (23.5%)	▼ –19.4%
Other business, employment and investment scams	$5 270 948	6 131	376 (6.1%)	▲ 92.2%
Upfront payment and advanced fee frauds	$4 148 089	8 588	1 004 (11.7%)	▼ –36.2%
Other buying and selling scams	$3 584 426	10 279	2 279 (22.2%)	▼ –13.2%
False billing	$2 796 980	13 455	737 (5.5%)	▲ 323.9%
Inheritance scams	$2 768 972	2 874	42 (1.5%)	▼ –21.2%
Remote access scams	$2 442 234	8 685	707 (8.1%)	▲ 71.6%
Threats to life, arrest or other[6]	$2 300 625	8 297	133 (1.6%)	▲ 1 743.7%
Betting and sports investment scams	$1 750 033	247	111 (44.9%)	▼ –1.9%

The third most common category by loss in the Scamwatch data, ‘Other business, employment and investment scams’ was a category which allowed the public to report scams which don’t quite fit into the ‘investment scams’ category or ‘false billing scams’ which affect businesses. The kinds of scams described in these reports include scammers offering services commonly used by businesses such as web page development, search engine optimisation, small business loans and business directory listings.

Losses reported to other agencies

There are a number of government agencies in Australia which receive reports from the public about scams. While the Scamwatch website offers the public a central point to report scams, organisations like the Australian Taxation Office receive a large number of public enquiries because of scams which impersonate them. State and territory based offices of fair trading also receive reports and enquiries from the public about scams.

The ACORN offers a reporting channel for cybercrime including many crimes that are not considered ‘scams’ like cyber bullying and online offences against children. These reports are directed to Australian law enforcement agencies to investigate potential crimes committed in Australia. ACORN also receives a large number of scam reports similar to those reported to Scamwatch that are generally perpetrated by scammers outside of Australia which complicates the ability of law enforcement to pursue them.

This report attempts to collate as many of the reports received by other agencies as possible in order to demonstrate the extent of the losses suffered by Australians in 2017.

Where the ACCC was able to obtain scam report data, when combined, the losses reported to these various agencies exceeded $340 million for 2017. However, even an amalgamation of the reported losses does not reflect the total losses actually suffered by Australians in 2017.

This is because many scam victims do not report their experience for a variety of reasons including embarrassment of being fooled by a scammer, not realising they have been scammed or not knowing how or where to report their experience to the government. Some people may not realise the value of reporting scams when a loss has not been suffered or when they are convinced there is no chance of recovering their losses. However, every scam report is valuable because it directs the education and awareness efforts of government agencies to help the public recognise and avoid scams.

[6] The scam category ‘Hitman scams’ changed to ‘Threats to life, arrest or other’ in 2017. This new category captures more types of scams than the old category. For this reason, ‘Threats to life, arrest or other’ will appear to have a disproportionately high increase when compared to 2016 data.

ACORN statistics

The ACORN's online system is a facility for reporting a broad range of online-based crimes including a number of scams which to some degree overlap with those reported to Scamwatch. The ACCC analysed the ACORN data from 2017 and identified those reports which best match 'scams' as defined by the ACCC. These reports to ACORN amounted to over $230 million in reported losses from 43 000 reports. To a greater degree than Scamwatch, scam reports to ACORN are those in which the reporter has lost money. This is demonstrated in the conversion rates in table 3 which are significantly higher than those in the equivalent Scamwatch scam categories. A review of both sets of data provides a more accurate perspective on the genuine scope and impact of scams.

Table 3: Top five ACORN scam categories by loss

Scam category	Reported loss	Reports	Reports with loss	Conversion rate
Online identity theft	$43 769 762	7 645	3 927	51.4%
Offered an investment opportunity	$33 293 476	479	396	82.7%
Asked to pay money upfront or transfer money ('Nigerian' scam)	$26 406 640	2 390	1 412	59.1%
Dating or romance scam	$21 552 377	770	563	73.1%
An online account has been hacked into	$17 504 259	1 923	1 579	82.1%
Total	**$142 526 514**	**13 207**	**7 877**	**59.6%**

Australian Taxation Office (ATO) statistics

In 2017, scammers impersonated the ATO and contacted Australians attempting to gather personal information or threaten them with fines or jail time for tax evasion. The ATO received 81 250 scam reports with $2 396 178 of reported losses. Of these, 58 054 reports were for threat-based impersonation scams for which $2.3 million was reported lost. When combined with the $4.7 million reported to Scamwatch, threat-based impersonation scams cost Australians over $7 million in 2017.

A trend that peaked in 2016 with ATO impersonation scams was scammers requesting payment via iTunes cards. This continued in 2017 with 55 per cent of victims paying this way. In November 2017, ATO collaboration with Apple resulted in a warning being placed on the back of iTunes cards in an effort to minimise losses.

2.3 Contact methods in Scamwatch reports

40%
Phone
65 097 reports
$29.1 million
reported lost

31%
Email
50 635 reports
$17.4 million
reported lost

12%
Text message
18 597 reports
$1.7 million
reported lost

Scams via email, social media, mobile apps and internet
68 351 reports (42% of all reports)
$49.9 million in reported losses

Telephone calls were the most common single contact method employed by scammers reported to Scamwatch in 2017 at 40 per cent or 65 097 reports. High numbers of phishing and remote access scams delivered via phone explain this. Reported losses in which the scammer used phone as the contact method amount to $29 160 342 or 18 per cent of total losses. The majority of phone-based scams involve scammers calling ranges of landline numbers one after another or using phone number directories, which include an initial and surname, to personalise the call.

The most common phone-based scam of 2017 was phishing scams with 11 404 reports. The scam delivered by phone with the highest reported losses was 'Investment scams' with $17 029 522 reported lost. The phone-based scam with the highest conversion rate was remote access scams with 21 per cent of scam reports indicating a loss was suffered.

Email-based scams were the second most common contact method and accounted for 31 per cent of total scam reports. False billing, phishing and unexpected prize and lottery scams were the top three scams which utilised email as a contact method. In terms of financial impact, investment scams were the top scam delivered via email with $4 084 395 in reported losses.

Text message-based scams increased from 6 per cent to 12 per cent in 2017. These scams are mostly unexpected prize and lottery scams, phishing and identity theft scams. Scams delivered via text message accounted for $1 706 895 in reported losses.

Online-based scams

When put together, online-based contact methods (including email, internet, social networking/online forums and mobile apps) equated to 68 351 reports which is close to the number of phone-based contacts. These reports represent 42 per cent of total reports but 55 per cent of total reported losses ($49 901 030). This means that while Scamwatch received more reports of phone-based scams, online-based scams resulted in higher reported losses.

Scams through social media

Only three per cent of reports with a contact method provided listed 'social networking' as the contact channel used by the scammer. This represents 4711 reports. However, social networking accounted for 12.5 per cent of the total losses reported in 2017 ($15 750 763). The majority of these reported losses, 62 per cent or $9 520 498, were from dating and romance scam reports. Social networking was also the most commonly reported contact method for dating and romance scams in 2017 (35 per cent of all dating and romance scams).

Investment scams were the second most reported scam type which used social networking as a contact method with 143 reports resulting in $3 080 004 in reported losses.

Women lost significantly more money through social networking-based scams than men. Women reported losses of $9 050 283 (59 per cent) while men reported losses of $6 372 403 (41 per cent). This difference is largely because women fall victim to dating and romance scams more than men with 65 per cent of the losses for dating and romance scams through social networking ($6 221 492) being reported by women (where gender is provided). On the other hand, men reported 74 per cent of the losses ($2 209 969) for investment scams on social networking.

Table 4 provides a breakdown of scam reports and losses by contact method in 2017.

Table 4: Breakdown of reports and losses by contact method

Contact method	Reports 2017	Percentage of total reports 2017	Reported losses	Percentage of total reported losses
Phone	65 097	40.3%	$29 160 342	32.1%
Email	50 635	31.3%	$17 470 299	19.2%
Text message	18 597	11.5%	$1 706 895	17.3%
Internet	11 559	7.2%	$14 761 762	16.2%
Mail	6 288	3.9%	$1 819 475	8.6%
Social networking/online forums	4 711	2.9%	$15 750 763	2.1%
In person	1 705	1.1%	$7 789 671	2.0%
Mobile apps	1 446	0.9%	$1 918 206	1.9%
Not provided	1 309	0.8%	$517 619	0.6%
Fax	181	0.1%	$33 590	0.04%
Total	**161 528**	**100%**	**$90 928 622**	**100%**

Victim story: Extortion via social media

Scam category: Threats to life, arrest or other

Loss: $400

I accepted a friend request on Facebook from some strange user. She only had two photos in her profile but I accepted the request anyway. She messaged me not long afterwards and introduced herself. We sent messages back and forth and after some time she invited me to a Skype video chat.

During the chat, things became sexual and she exposed herself to me and invited me to do the same. She eventually persuaded me to expose myself but she was secretly recording the whole thing. She then threatened to release the video to all my Facebook friends if I didn't pay her $400 via Western Union. She told me that if I paid she would delete the video.

I was terrified of what might happen if she posted the video so I paid the $400. After I paid however she went back on her promise to delete the video and demanded more money. I have now blocked her on Facebook and deactivated my Facebook account to avoid her threats.

2.4 Demographics in Scamwatch reports

Not every scam report to the ACCC includes age, gender and geographic data but those that do, provide us with valuable insights about which scams affect different groups in society. Analysis of this information helps us better understand how certain scams work. Age, gender and geographic data can inform us about who a scam is targeting and also helps us direct our education and awareness raising efforts to the right audiences.

Age

A trend that continues in 2017 from previous years is higher losses suffered by older Australians but higher conversion rates reported by younger Australians.

Older Australians hold far more accumulated wealth and have more to risk when presented with a convincing scam. Older Australians are also more exposed to high loss scams like investment and dating and romance scams with many attempting to shore up retirement funds or find love online in later life.

The corollary holds true in that younger Australians have less accumulated wealth and less money to lose on scams. Their higher conversion rate, as shown in table 5, perhaps suggests that younger people are more likely to report scams only when they suffer a loss whereas older people report scams even if they do not suffer a loss. Older Australians also report far more phone-based scams because of their continued use of landlines which have a low conversion rate.

Table 5: Breakdown of reports and losses by age demographics

Age	Reports	Reported loss	Reports with loss	Percentage of all reports
Under 18	1 004	$115 074	232 (23.1%)	0.6%
18–24	6 717	$2 428 101	1 351 (20.1%)	4.2%
25–34	14 978	$6 439 528	2 225 (14.9%)	9.3%
35–44	14 594	$10 188 915	2 054 (14.1%)	9.0%
45–54	16 483	$16 191 489	1 828 (11.1%)	10.2%
55–64	17 866	$21 632 704	1 546 (8.7%)	11.1%
65 and over	25 262	$17 547 713	1 598 (6.3%)	15.6%
Not provided	64 624	$16 385 098	3 217 (5.0%)	40.0%
Total	**161 528**	**$90 928 622**	**14 051 (8.7%)**	**100%**

A comparison of four common scams by age group

To illustrate how scams can impact different age groups we have grouped the Scamwatch age categories into three broad groups of younger, middle-aged and older Australians and then compared the differences in statistics of four of the top scam categories of 2017. The scams included are ‘investment scams’, ‘Threats to life, arrest or other’, ‘Other buying and selling scams’ and ‘Dating and romance’ scams.

With the 33 per cent increase in reported losses to ‘Investment scams’ in 2017, every group was hit hard by this type of scam. Losses to this scam increased with age as discussed previously. The average loss for these scams also increased significantly as age increased.

‘Dating and romance scams’ ranked lowest for younger Australians but second for middle-aged and older Australians and losses also increased with age.

‘Threats to life, arrest or other’ ranked second for younger Australians who suffered the most substantial losses to this scam of the three age groups. There was an average loss of $29 891 in these scam reports from younger Australians where a loss was included. A number of young Australians lost large amounts to this scam including younger immigrants who were told by scammers they would be deported because of issues with their visa paperwork. Those less knowledgeable about law enforcement agencies in Australia may be more easily scared by these scams.

Older Australians reported ‘Other buying and selling scams’ about as much as middle-aged and younger Australians but lost the least amount of money. However, the average loss for middle-aged and older Australians was about $2000 which suggests that when they did lose money to these scams, both age groups lost more than younger Australians.

Table 6: The impact of four different scams on different age groups

Category	Reported loss	Reports	Reports with loss	Average loss
Younger Australians (under 18–34)				
Investment scams	$1 629 838	348	119	$13 696
Threats to life, arrest or other	$1 225 536	850	41	$29 891
Other buying and selling scams	$942 762	2 356	820	$1 149
Dating and romance	$511 017	622	139	$3 676
Total	**$4 309 153**	**4 176**	**1 119**	**$3 850**
Middle-aged Australians (35–54)				
Investment scams	$9 980 248	557	200	$49 901
Dating and romance	$7 601 176	1 129	323	$23 533
Other buying and selling scams	$1 338 730	2 458	656	$2 040
Threats to life, arrest or other	$464 008	1 519	27	$17 185
Total	**$19 384 162**	**5 663**	**1 206**	**$16 073**
Older Australians (55+)				
Investment scams	$13 591 265	506	162	$83 896
Dating and romance	$9 683 475	1 063	270	$35 864
Other buying and selling scams	$708 556	2 360	374	$1 894
Threats to life, arrest or other	$201 916	2 417	20	$10 095
Total	**$24 185 212**	**6 346**	**826**	**$29 279**

Gender

Where gender information is provided, women reported more scams than men but suffered lower and fewer losses. Women reported 42 per cent of the total losses in 2017 and men reported 56 per cent.

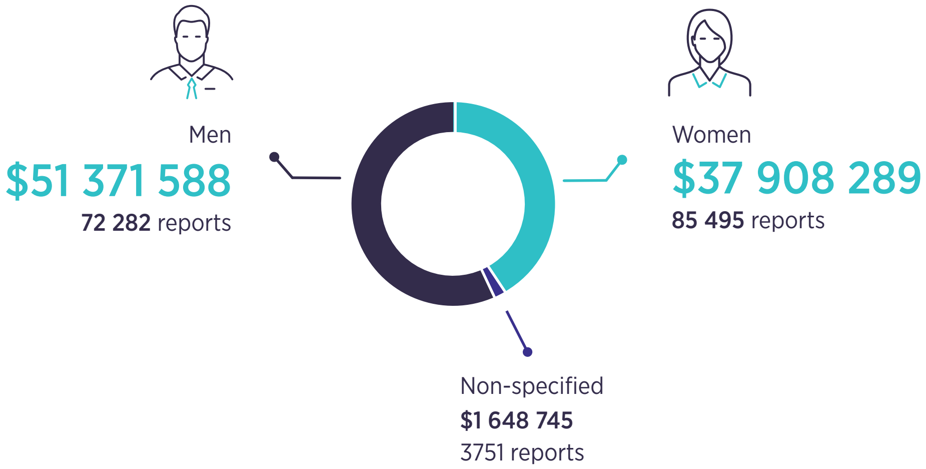


Table 7: Scams reported by gender

Gender	Reports	Percentage of reports	Reports with loss	Reported loss
Female	85 495	53.0%	7 015 (8.2%)	$37 908 289
Male	72 282	44.7%	6 838 (9.5%)	$51 371 588
Not specified	3 751	2.3%	198 (5.3%)	$1 648 745
Total	**161 528**	**100%**	**14 051 (8.7%)**	**$90 928 622**

The disparity in losses between men and women is explained by significant losses by men to investment scams. Men reported a $22.8 million loss to investment scams whereas women reported $8.0 million. Women on the other hand lost more than men to dating and romance scams with $12.7 million lost versus $7.1 million.

Table 8: Top five scam categories by loss by gender

Scam category	Male reported loss	Female reported loss	Total
Investment scams	$22 800 385	$8 039 714	**$30 840 099**
Dating and romance	$7 100 730	$12 746 253	**$19 846 983**
Other business, employment and investment scams	$3 825 106	$1 440 527	**$5 265 633**
Upfront payment and advanced fee frauds	$1 313 919	$2 830 422	**$4 144 341**
Other buying and selling scams	$1 845 282	$1 682 311	**$3 527 593**

Different approaches based on the gender of the target

Scammers deliberately target and employ different techniques depending on the gender of their intended victim. This is most apparent in dating and romance scams where scammers will create generic profiles of a love interest which are very different depending on whether the scam is targeted at men or women. No matter if the victim is a man or woman, the scammer will quickly profess their love but the supporting story of who they are and why they need money is often different. While not true of every dating and romance scam, there are common themes in what is reported by victims to the ACCC. Scammers seem to use these character themes because it is what they believe will be appealing to men and women and since we receive reports from victims about them, to some degree they seem to work.

For women, scammers will often present themselves as a middle-aged gentlemen with a profession such as an engineer, rare stone trader or military officer currently working in an exotic location. The scammer will sometimes claim that they were married once before but their wife died in tragic circumstances such as a car crash or from a terminal illness. Often the scammer will claim to have a child they are raising on their own and the reason for them working overseas is to earn a large sum of money or they are finishing their final military mission in order to take care of them and set up their future. All of this plays into the reasons why the scammer claims to need money: the project they are working on has hit a snag and they cannot access funds, they have been detained by authorities for errors in paperwork and must pay a fine or they were mugged in the street and have lost their passport. The overall impression the scammer is hoping to create is of a strong, capable, responsible, worldly character who is on the brink of significant wealth and success but keeps running into bad luck.

For dating and romance scams targeting men, scammers often create a character who is young and energetic and perhaps working in a profession such as nursing or will claim they are studying or about to launch a small business. Often there is a significant age difference which many victims raise early in the scam as a major issue but the scammer brushes this off by stating ‘love is ageless’ or ‘love doesn’t care about numbers’. The scammer will quickly determine if the victim is looking for a short or long-term relationship and will adapt their language and approach accordingly. The scammer will often claim to have a close family member who is suffering a painful illness requiring expensive medication which creates an excuse for needing money early in the scam. The scammer will claim to suffer a string of tragedies, missed flights and visa issues which requires more money to resolve. This character is presented as nurturing, caring, energetic, and loyal but also vulnerable, perhaps hoping the male victim will feel they are acting as a saviour of some kind.

No matter the target, dating and romance scammers will often twist the story toward whatever path they think will net them the most money. Another common story arc they employ is an investment opportunity as a reason for needing money and this trick is pulled on both men and women.

Victim story: Romance scam with an investment angle

Scam category: Dating and romance

Loss: $223 000

I met this guy on a dating site claiming to be a businessman from Western Australia, who deals in mining diamonds and mineral stones. He flew to Malaysia to seek chemicals and equipment to use for processing raw and rough diamonds. He lost his wallet at the airport. He was feeling distraught and alone without cash and a credit card and he begged me to send him some cash. This was for accommodation, food, and transport.

He finally found a supplier for his equipment, and sent me an official receipt of purchase worth $478 000 from the supplier and documents showing the bank loaned him the money for the purchase of supplies and equipment. He told me that shipment of goods would not happen unless a 15 per cent custom duty was paid. I transferred money via a remittance service, $71 700 for custom duties, another $20 000 for GST, $40 000 for clearance, legal, and shipping costs, and airline ticket to return to Australia.

He had an accident on the way to the airport, I paid for his hospital bills. He asked me to help him with this project by helping to fund the operation supposedly running back in Australia. I supported the ongoing process of cutting and polishing diamonds, hiring three technicians, a factory lease, and payment for utilities.

Believing that we were partners in this business and his limited access to cash, I ended up borrowing money from the bank to support the ongoing process of the business.

Geography

Loss reports to Scamwatch by Australian states and territories largely rank in line with the population of those states and territories with a few exceptions.

- When comparing states, losses by Queenslanders correlate with population size but there are more scams reported by Queenslanders than Victorians.
- Australian Capital Territory residents both reported and lost more than Tasmanians despite having a lower population.
- South Australians reported just 1220 fewer reports than Western Australians but reported $2.6 million less in losses.

Table 9 provides a breakdown of reports and losses by state and territory.

Table 9: Breakdown of reports and losses by state and territory[7]

State	Reports	Reported loss
New South Wales	47 669	$28 011 041
Queensland	36 290	$14 176 788
Victoria	33 705	$22 974 264
Western Australia	14 962	$6 309 834
South Australia	13 742	$3 669 854
Australian Capital Territory	4 477	$1 674 002
Tasmania	3 762	$1 435 968
Northern Territory	1 527	$962 208
Not provided	332	$2 512 070
Overseas[7]	5 062	$9 202 593
Total	**161 528**	**$90 928 622**

[7] A significant number of reports are submitted with ‘overseas’ as the location and while many of these are reported from overseas both by Australians and citizens of other countries, many are actually in Australia. It is not clear if these Australia-based reporters chose the incorrect location, thought they were reporting on the location of the scammer or did not want to reveal their location in their report.

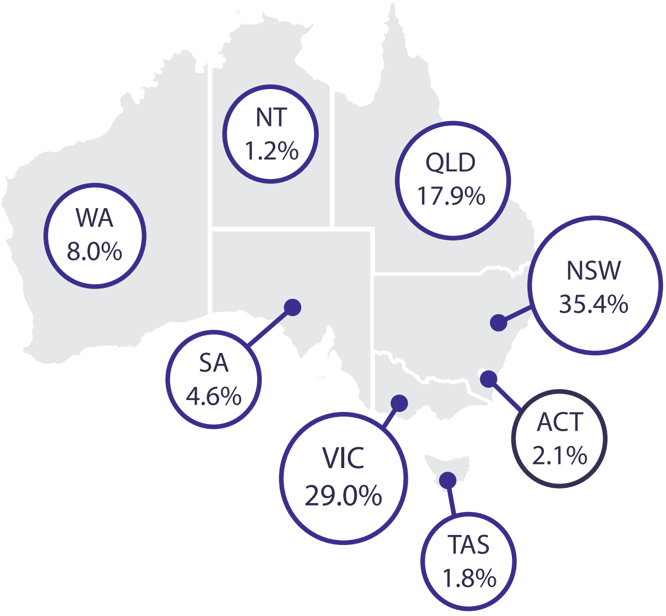
Top scams by geographic location by Scamwatch scam category

Investment scams and dating and romance scams cost Australians the most in 2017 and this is reflected in the top scams for each state. 'Investment scams' was the scam type with the highest reported losses in the Australian Capital Territory, New South Wales, Queensland, South Australia, Victoria and Western Australia. In the Northern Territory and Tasmania, dating and romance scams extracted more money from victims.

For almost all states and territories, investment scams and dating and romance scams were the first or second highest reported losses.

As the same scams affect Australians no matter where they live, this suggests that scammers are not targeting different scams at different states. Instead they cast a wide net by sending bulk emails, approaching anyone they can online and calling a range of Australian phone numbers one after the other.

Percentage of total scam losses by state



3. Other trends of 2017

3.1 Increase in Scamwatch investment scam losses

'Investment scams' was the scam type with the highest losses reported in 2017 with reports to Scamwatch and ACORN exceeding $64.6 million. Losses to investment scams reported to Scamwatch increased by 33 per cent in 2017 to $31.3 million.

An analysis of Scamwatch data did not reveal any particular scam which can be directly attributed to this increase nor did there seem to be a range of new techniques employed by investment scammers that made their scams more effective. They simply continued using techniques, such as cold calling, that are known to work and more Australians reported their experience to us in 2017. In terms of who was most affected by investment scams, all age groups reported losses, but men reported more losses to investment scams than women.

The increase in losses in 2017 is mostly found in higher-loss reports and not in an increase of low-value losses. In 2016, there were seven reports with losses of $400 000 or more whereas in 2017, there were 20 such reports. This pushed up the average loss in 2017 to $53 827 from $46 980 in 2016.

Almost half (46 per cent) of the investment scams reported started with a phone call from a well-spoken representative of a fake investment firm. Sometimes these are cold calls, sometimes they are following leads based on enquiries the victim made online on seemingly unrelated sites in prior weeks or months. The victim is promised large returns with a very high chance of success and is told in the first weeks after the investment that everything is travelling well and that their money is growing steadily. The victim is then encouraged to invest more and more to maximise their returns. Eventually, the fake firm disappears with all the money. Any attempts to track down the fake investment firm are futile, their phone number is disconnected, their website is not updated and they don't respond to emails.

Binary options

Binary options scams, which are a type of investment scam, appear to have peaked in 2016 and reduced in number of reports and in reported losses in 2017. Despite this, the average loss reported is binary options scams increased by 24 per cent from $32 744 to $43 085 which suggests that while there were fewer of them, these scams became more effective at extracting large sums of money from victims. While binary options are not illegal in Australia, there are a number of very professional looking websites usually operated from overseas offering binary options investments that are outright scams.

Victim story: Fake stock offer

Scam category: Investment scams

Loss: $250 000

I received a call offering an investment opportunity. The caller offered a discounted share price for Tesla and Space X shares. Once I paid the money, they said I could resell the shares with a healthy profit but told me that I did not have enough shares to quality for this special deal. So I paid more money. Then it was a 'security deposit' to get the funds from the sale cleared and paid to me. I said there was no more money so they offered to decrease the deposit amount. I still said I did not have any more money. I emailed them to say I was going to personally visit them in Hong Kong.

I sent a colleague of mine to the address they provided but the company at that address was a different company who told him they had never heard of the investment company I thought I was dealing with. I called the same day but could not get a connection. I called their USA office, again no connection.

Another company has called me offering to buy my shares but I suspect this is a scam as well.

3.2 Threat-based impersonation scams

Threat-based impersonation scams involve scammers pretending to be from law enforcement, government agencies or well-known service providers such as Telstra and threatening people with fines, jail time or loss of benefits because of an imaginary violation of some kind. The scammers will claim that the victim hasn't paid their taxes, has committed some crime, has failed to fill out paperwork correctly on immigration forms or has technical issues with their home internet connection which will incur charges unless they provide remote access to their computer. Also common is a version of the scam in which the scammer impersonates Centrelink and tells victims that they have been overpaid and unless they pay this money back they will have their benefits cut. Fear and intimidation are used to frighten the victim into doing what the scammer asks and victims are led to believe that unless they pay the non-existent fine or provide remote access, they could face harsh consequences.

An analysis of Scamwatch data for 2017 revealed almost 33 000 reports and over $4.7 million in reported losses. Also, 2800 people reported losing their personal information to scammers which could then be used in future scam attempts. When combined with losses reported to the ATO for this kind of scam, total reported losses were over $7 million.

Over 85 per cent of those who submitted a report were contacted by phone. This allows scammers to use a threatening tone and pressure the victim to act quickly and without having time to think the situation over.

The ATO also collected data on reports and enquiries from concerned members of the public who were told they did not correctly pay their taxes. The ATO received 58 054 reports about such scams with over $2.3 million in reported losses.

'Hitman scams' and 'Threats to life, arrest or other'

In 2017, the ACCC changed the 'Hitman scams' category to 'Threats to life, arrest or other'.

Reports of 'Hitman scams' (described in the glossary of scam terms at the start of this report) were becoming less and less common while reports of scammers impersonating government and private organisations and using threats to scare consumers into paying fake fines and fees were on the increase.

These impersonation scams were submitted by the public on the Scamwatch website across a range of categories such as 'Reclaim scams' and 'Upfront payment and advanced fee frauds'. As a result it was difficult to isolate them and clearly identify how many of these scams were being reported.

The solution was to change the 'Hitman scams' category to 'Threats to life, arrest or other'. This category captures both the classic 'Hitman scams' and any other threat-based scams which has the effect of concentrating reports of these scams into one category, instead of being spread across a number of categories.

As a result, apparent excessively large increases in 'Threats to life, arrest or other' in tables in this report are not indicative of a true increase versus the previous year's 'Hitman scams' numbers.

3.3 Scams and cryptocurrencies

In the fourth quarter of 2017, the value and popularity of cryptocurrencies increased worldwide. Scammers adapt each year and find ways to exploit popular trends, new platforms, new ways of communicating, fad products, changes to legislation or new investment opportunities. Between January and September 2017, about $100 000 was reported lost per month to scams which had a cryptocurrency angle. However, in the month of December 2017, reported losses to Scamwatch exceeded $700 000 and the average reported loss had jumped from $1885 in January to $13 205.

As the value of actual cryptocurrencies increased, so too did the scam losses in what people thought were real investments. By the end of the year, reports of losses related to cryptocurrencies exceeded $2.1 million but as with other scams, this is likely the very tip of the iceberg.

Examples of cryptocurrency scams in 2017 include fake 'initial coin offerings' which, like initial stock offerings, purport to be the launch of a new cryptocurrency. Others capitalised on the general confusion about how cryptocurrency works and instead of people discovering how to directly buy cryptocurrencies, many found themselves caught up in what were essentially pyramid schemes. A number of reports showed that victims entered into cryptocurrency-based scams through friends and family who convinced them they were onto a good thing, a classic element of pyramid schemes.

Not all cryptocurrency-related scams involved victims attempting to invest in stocks or initial coin offerings. Many scammers also ask for payment through cryptocurrencies for a variety of scams because it is easier to remain anonymous while receiving payment. Ransomware scammers for example, commonly ask for payment through Bitcoin.

3.4 iTunes gift cards

In 2016, the use of iTunes cards as a payment method emerged in a number of scams, but most commonly in threat-based impersonation scams in which the scammer impersonates the Australian Tax Office or Centrelink. This involves the scammer asking the victim to visit a local shop to buy a large number of iTunes cards. Once purchased, the victim then reads out the serial numbers on the cards to the scammer over the phone. The scammer can then sell these unused serial numbers online, often on the dark web.

This trend continued in 2017 with 490 scam reports indicating payment to a scammer via iTunes cards with a loss of $1 231 553. Upon a closer examination of the data, iTunes cards were mentioned in many more scam reports and many consumers paid the scammer with iTunes cards but recorded their payment method as 'credit card' because that was how they paid for the iTunes cards. A number of other scams involved the scammer asking for payment via iTunes cards but ultimately ended up hacking the victim's bank account and transferring money from it.

When these factors are taken into consideration, iTunes cards were reported as an element in 2164 reports with $1.9 million in losses in 2017.

3.5 The reduction of average loss

In 2017, the average loss suffered by scam victims dropped by 10 per cent from $7226 in 2016 to $6471. However, at the same time, the reported losses for 2017 increased by eight per cent over 2016 losses and the number of reports indicating a loss increased by 17.7 per cent.

The reason for lower average losses despite greater overall losses is because of a higher number of reports with small dollar value losses. These low-value losses are almost entirely because of online shopping scams.

In 2017, more Australians reported being scammed thinking they had found a bargain online. An analysis of the 2017 Scamwatch data revealed that shoes and the must-have toy of 2017, the fidget spinner, were the two most commonly reported items victims were trying to buy from online shopping scams.

Table 10 shows that 56 per cent of scam losses were under $500 in 2017 but there were also six reported losses of $1 million or more.

Of the six reported losses over $1 million, five were investment scams and one was a form of unexpected money scam. Scams with such high losses generally involve longer-term grooming of the victim to build trust with multiple transactions sent over a long period.

Table 10: Losses by loss value range

Loss ranges	Reports	Percentage of total loss
$1–$99	3 267	0.1%
$100–$499	4 632	1.3%
$500–$999	1 876	1.4%
$1 000–$9 999	3 108	10.6%
$10 000–$49 999	809	18.6%
$50 000–$499 999	333	48.1%
$500 000–$999 999	20	12.1%
$1 million–$10 million	6	7.9%
Total	**14 051**	**100%**

4. Scams targeting businesses

Scamwatch received 5432 reports from businesses in 2017 with $4 669 409 in reported losses. The average loss for businesses was $10 935 which is a three per cent increase over 2016.

The typical business scam in 2017 was delivered via email (60 per cent) and money was sent via bank transfers (85 per cent) rather than through remittance services or cryptocurrencies which are common in other scams. This indicates that typical business scams presented in writing are relatively convincing and seek payment via trusted financial channels.

The scam category with the highest losses reported by businesses in 2017 was 'Other business, employment and investment scams'. A closer look at the reports in this category involved scammers offering services commonly used by businesses such as web page development, search engine optimisation, small business loans and business directory listings. Busy businesses sign up to what seem like good deals at the time but find out when no service is delivered that the offer was not legitimate.

Where appropriate, the ACCC will undertake enforcement action against perpetrators of scams. In August 2017, the ACCC instituted proceedings against Domain Name Corp Pty Ltd and Domain Name Agency Pty Ltd (also trading as Domain Name Register) (the Domain companies). The ACCC alleged that they engaged in misleading or deceptive conduct and made false or misleading representations to Australian businesses about the domain name services they offered. More information about this can be found in section 6.3.

More complex scams targeting businesses involve the use of a range of targeted techniques like phishing and the use of malware such as trojans and keyloggers to get a specific person in an organisation to give up key information like passwords to email accounts or IT systems. This information is then used to hack a business's IT systems and misdirect funds to their own accounts.

Table 11 provides an overview of the top scams which targeted businesses in 2017.

Table 11: Overview of top scams targeted at businesses

Scam category	Reported loss	Reports	Reports with loss
Other business, employment and investment scams	$1 659 465	658	46
False billing	$1 470 148	1 323	106
Hacking	$581 537	177	22
Other buying and selling scams	$407 381	592	89

Since nine in 10 businesses in Australia are small businesses, the bulk of our scam reports which targeted businesses were from this cohort as shown in table 12.

Table 12: Breakdown of scams by business size

Employees	Reported loss	Reports	Percentage of reports
Micro (0–4 staff)	$740 132	1 505	27.8%
Small (5–19 staff)	$2 249 836	1 430	26.4%
Medium (20–199 staff)	$812 040	797	14.7%
Large (over 200 staff)	$503 138	350	6.5%
Blank	$308 508	1 334	24.6%
Total	**$4 613 654**	**5 416**	**100%**

The impact of scams on businesses

The true impact of scams on Australian businesses is greater than what is reported to Scamwatch. In 2017, the New South Wales Small Business Commissioner commissioned research and released a report on cybercrime affecting small to medium enterprises (SMEs) in New South Wales.[8] The cybercrime discussed in the report has direct overlap with many of the scams reported by businesses to the ACCC. The report illustrates the extent of the threat of scams and cybercrime faced by SMEs.

According to report:

- The cost of cybercrime to business in Australia costs an estimated $1 billion each year and $3 trillion globally.
- Cybercrime is rated as the fifth biggest risk to their business.
- SMEs are most concerned about fraudulent emails or phone calls, social media hacking, online banking fraud and ransomware and malware.

4.1 Business email compromise scams

Most scams work on the basic principle of making the victim believe something that is not true. This is the case across very different types of scams. Dating and romance scammers convince their victims they are communicating with a legitimate romantic interest. Threat-based impersonation scammers convince their victims they must pay a supposed fine or tax debt immediately or face legal consequences. In most cases, these scams involve a single, out of the blue communication from a scammer to a victim and possibly follow up communications with the victim if they engage with the scammer. Such scams can be conducted with tools like a laptop, a social media account or a telephone. There is little to no set up required to perform these scams, and if unsuccessful, it is easy to move on to the next victim by calling another number or sending scam emails to more email addresses.

Business email compromise scams are significantly more complex. This scam includes the core principle of convincing the victim of a lie but the set-up requires very specific technical skills and a more significant time investment. If the scam fails, finding the next target and setting up another scam is difficult. This scam requires a patient and strategic approach and can result in significant losses for the victim.

Steps of an email compromise scam:

1. A hacker obtains login details which have been obtained through a separate phishing scam, targeted 'spear phishing' against a specific target or hacks into an email account belonging to a business. From there they may be able to gain access to the business's entire IT systems.
2. The hacker trawls though the email account or IT systems for information such as account numbers, names, supplier details and schedules for regular deliveries and payments. The hacker carefully identifies a relationship between the business and a supplier/buyer/customer to exploit.
3. The hacker, with access to the business's systems, is able to send an email to a customer alerting them that their banking details have changed and that future invoices should be paid to a new account. From the receiver's point of view, the email appears legitimate and so they update the invoice account details.
4. Payments start to flow into the hacker's account, who quickly moves them out as soon as they land to avoid losing them if the scam is discovered.
5. If the conditions are correct, the hacker may also try to scam the same business they have hacked into by sending emails purporting to come from one business area to another, asking for funds to be transferred for various reasons. For example, the scammer may send an email asking for emergency funds to be transferred to an executive's account who has run into trouble on an overseas trip.
6. The hacker may be successful in diverting a single money transfer, or may linger in the business's system for months sending carefully crafted emails which result in substantial losses.

[8] NSW Small Business Commissioner, *Cyber Scare*, 2017.

An analysis of ACCC and ACORN data revealed losses of over $22.1 million from businesses across a range of industries. Reports indicated that scammers attempted to send emails to redirect funds wherever funds were transferred between parties including between businesses and their suppliers and businesses and their customers. In some scenarios, consumers who were trying to buy or build houses were emailed by scammers to pay their agents or builders into the wrong account so that they not only lost substantial sums of money, they may have also missed out on the purchase of a property or the completion of a build.

Victim story: Small business email compromise scam

Scam category: Hacking

Loss: $67 000

A scammer hacked into our boss's email account in May 2017. The scammer studied how he communicated to me because I am in charge of the accounts mailbox which is used for money transfer requests.

In July, when our boss was overseas, the scammer sent an email from my boss's email address to our accounts mailbox asking for a transfer of $67 000 to an external account. I thought it was a legitimate instruction from the boss so I made the transfer. When the boss returned later in the month, it was only then that we realised that it was a fraud and that our boss had not made that request.

We could not find the email I received in our boss's email account. The scammer must have deleted it to cover his tracks. We have reported the incident to the bank and police and we are awaiting their investigation but we fear it is too late to get the money back.

5. Scams reported by Indigenous consumers

5.1 Scam trends

In 2017, Scamwatch received 1810 scam reports from those identifying as Indigenous consumers. Losses from these reports total $1 680 367 which is an increase of 14 per cent over reported losses of $1 471 282 in 2016. Appendix 4 provides a breakdown of reports and losses from those identifying as Indigenous.

From these reports, dating and romance scams had the highest reported financial losses of $746 790. Investment scams ranked third with $164 904 reported lost. A look through the reports does not suggest any specific targeting by scammers of Indigenous consumers.

Table 13 lists the top five scams suffered by those identifying as Indigenous. The 2000 per cent increase in 'job and employment' scams is due to two very large losses reported in 2017 and does not reflect a broader trend.

Table 13: Top five scams by loss reported by indigenous consumers

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Dating and romance	$746 790	101	22 (21.8%)	▼ –12.4%
Job and employment	$435 150	49	3 (6.1%)	▲ 2 000.1%
Investment scams	$164 904	28	13 (46.4%)	▲ 135.0%
Online shopping scams	$60 249	97	47 (48.5%)	▲ 377.7%
Unexpected prize and lottery scams	$56 948	194	9 (4.6%)	▲ 252.1%

The age demographics for reports from Indigenous consumers differ from the wider population in that the 65 and over cohort reported a significantly lower percentage of scams (6 per cent versus 15 per cent). However, the conversion rate of scams, meaning the percentage of reported scams which include a loss, generally follows that of the larger population.

Table 14: Breakdown of scam reports by indigenous consumers by age

Age	Reported loss	Reports	Reports with loss	Percentage of reports
Under 18	$11 198	32	8 (25.0%)	1.8%
18–24	$102 750	172	40 (23.3%)	9.5%
25–34	$79 897	342	62 (18.1%)	18.9%
35–44	$72 587	295	46 (15.6%)	16.3%
45–54	$179 576	264	30 (11.4%)	14.6%
55–64	$684 441	201	24 (11.9%)	11.1%
65 and over	$458 477	108	10 (9.3%)	6.0%
Not provided	$91 441	396	42 (10.6%)	21.9%
Total	**$1 680 367**	**1 810**	**262 (14.5%)**	**100%**

Contact methods reported by this cohort also follow the trends of the larger population. The greatest exception is reports of scams delivered via social media. In the greater population, three per cent of reports indicated social media as the contact method used by the scammer but for reports by Indigenous consumers, social media accounts for eight per cent. This may be explained by the fact that many Indigenous communities have taken up social media as a method of staying in touch across geographic distance. It also matches the trend of social media being a very common contact method for dating and romance scams, which is the most frequently reported scam by Indigenous consumers.

Table 15: Contact methods

Contact method	Reports 2017	Percentage of total reports in 2017
Email	557	30.8%
Phone	518	28.6%
Text message	248	13.7%
Internet	169	9.3%
Social networking/online forums	145	8.0%
Mail	64	3.6%
In person	53	2.9%
Mobile apps	40	2.2%
Fax	10	0.6%
Not provided	6	0.3%
Total	**1810**	**100%**

5.2 Northern Territory Indigenous scam project

In 2017, the ACCC's Darwin office engaged in targeted scams awareness outreach in a number of Indigenous communities and succeeded in reducing scam-related losses.

In order to engage effectively, nine Indigenous communities were identified as scam hotspots by analysing international financial transactions being sent from these communities to countries of concern overseas. These are countries which do not seem to present any familial or other link to members of those communities.

Once identified, tailored workshops were held in these communities to raise awareness of scams to help reduce their impact. Eleven workshops were held in these communities across the Northern Territory with four separate engagement visits. Members of two of these communities created a series of posters which helped spread scam warnings to others in the community including using language from one of the communities.

This approach seems to have met with success as a comparison of 2016 and 2017 international transactions data for the targeted communities shows there was a reduction of approximately 42 per cent.

Victim story: Indigenous consumer

Scam category: Classified scams

Loss: $2585

I purchased a kitten for $310 from Tasmania from a classifieds site and paid online.

The seller said for shipping I needed to hire a heated crate for $550. Then I was told I needed to pay pet insurance of $1300. I was told the kitten arrived at Melbourne airport but needed a 'cities permit' for $425. The scammer said all of this was to be refunded at delivery.

Then the kitten was never put on the flight to Sydney and the scammer rang and told me the cat was sick and not able to fly. I was asked to cover the vet bills. I refused to pay. The next day I was told the cat was still sick but getting delivered. Then they told me the cat had died as it needed some surgery.

What makes this worse is I am a single mum. I borrowed the money for the kitten. It was my daughter's birthday present and I cannot get the money back. I had never shipped an animal before so I had no idea.

6. Disruption and enforcement

6.1 Scams disruption project

In August 2017 the ACCC concluded its 'scams disruption' project which used financial intelligence to identify Australians sending funds to high-risk jurisdictions in West Africa and advising them that they may have been targeted by a scam. Many of the scams originating from these jurisdictions were dating and romance scams which are often both financially and emotionally damaging for victims.

The project commenced in August 2014 and over the next three years the ACCC sent more than 10 000 letters to potential scam victims. About 70 per cent of those who received our warning letters stopped sending money overseas within six weeks of receiving the letter.

ACCC staff spoke with many of the victims who received letters and helped them understand the reality of the deception the scammers had subjected them to, sometimes over the space of several years. The information provided by victims also helped the ACCC keep track of emerging techniques and methods used by scammers to get money from their victims.

While this project wound up in 2017, the ACCC continued to seek opportunities to disrupt the activities of scammers targeting Australians on a broader scale through other projects and initiatives.

6.2 Scam intermediaries project

In 2017 the ACCC continued engaging with a range of private sector 'intermediaries' whose businesses are commonly used to facilitate scams either through connecting scammers to victims or by facilitating the transfer of funds to scammers. These include financial institutions, online payment platforms, online classified sites and social media platforms.

The ACCC recognised that these intermediaries are in a unique position to identify and intervene in scams that rely on their facilities. The ACCC expects these businesses to actively take steps to reduce the ability of scammers and fraudsters to use their systems. The point of money transfer for example from a victim to a scammer is a key point at which intervention is important. In the same sense, systems to detect scam advertisements on classified sites and fake accounts on social media platforms could have a significant impact on the ability of scammers to operate.

The ACCC has been working with these intermediaries to reduce the impact of scams on Australians. The ACCC has provided information to intermediaries to assist them to identify scam trends and inform their scam prevention activities.

As a result of this engagement, some intermediaries were able to recover additional funds and block scam transfers for customers in some circumstances. One of the intermediaries, an online classifieds platform was able to identify and delete fake advertisements based on shared intelligence. Some intermediaries increased the resources they dedicate to scam prevention efforts and all participants continue to optimise their efforts to detect and prevent scam conduct on their systems.

The ACCC has provided guidance to assist financial institutions to implement good practices to reduce scams operating through their platforms.

6.3 Enforcement

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

Where appropriate the ACCC will undertake enforcement action against the perpetrators of scams, particularly where it is likely to have the potential to deter others who may be considering engaging in unscrupulous conduct.[9]

In 2017, the ACCC instituted proceedings or continued previously instituted proceedings against a number of entities operating in Australia.

Domain Name Corp Pty Ltd

In August 2017, the ACCC instituted proceedings against Domain Name Corp Pty Ltd and Domain Name Agency Pty Ltd (also trading as Domain Name Register) (the Domain Companies) alleging that they engaged in misleading or deceptive conduct and made false or misleading representations to Australian businesses about the domain name services they offered.

From November 2015 to at least April 2017, the Domain Companies sent out approximately 300 000 unsolicited notices to businesses, which the ACCC alleges looked like a renewal invoice for the business's existing domain name. Instead, these notices were for the registration of a new domain name, at a cost ranging from $249 to $275.

The ACCC alleges that because these notices looked like they were renewal invoices, many businesses paid them thinking they were simply renewing the domain name for their business. The ACCC is alleging that the businesses were instead unwittingly signing up for a new domain name ending in either a .net.au or .com suffix that the business might not have needed or wanted.

The ACCC alleges that the notices sent out by the Domain Companies offered domain names that looked very similar to the business's current domain name. This detail and the fine print disclaimer were easily missed.

The ACCC believes that Australian businesses and organisations paid approximately $2.3 million to the Domain Companies as a result of receiving the notices.

The ACCC is seeking declarations, injunctions, pecuniary penalties, corrective advertising, disqualifying orders against the director and costs.

Luxstyle / Digital Sourcing

In 2017, the ACCC received over 1600 complaints about overseas based online retailer Digital Sourcing ApS (Digital Sourcing) formerly Lux International Sales ApS (Luxstyle), which advertise beauty products on social media sites such as Facebook and Instagram.

In December 2017, after the name change, the ACCC issued another public warning notice about the conduct of Digital Sourcing.

The ACCC issued this notice based on a reasonable suspicion that the conduct of Digital Sourcing may have breached the Australian Consumer Law by misleading consumers and asserting a right to payment for unsolicited goods, and considers that it is in the public interest to inform consumers about this conduct.

These ads directed people to a website that does not display prices unless the customer enters mailing and email addresses. Many people complained that they are then sent a goods package by this company despite not making an order or entering payment information. The package contains an invoice with the products demanding payment. If not paid, people then receive letters of demand threatening legal action.

In March 2017, the ACCC issued a public warning notice about the conduct of Luxstyle. This company changed its name to Digital Sourcing on 1 October.

Digital Sourcing claims that customers order the products based on its 'deliver now, pay later' system, and points to fine print displayed during the ordering process and links to its terms and conditions.

[9] For more information on the ACCC's compliance and enforcement policy, please visit the ACCC website at www.accc.gov.au.

7. Education and engagement

7.1 Education

Due to the international nature of scams and the jurisdictional and enforcement realities of bringing scammers to justice, the main tool to reduce scams impacting Australians is education, awareness raising and engagement with the public. The ACCC's main method of achieving this is our online activity through the Scamwatch website and its resources, such as *The little black book of scams*, as well as our social media presence and getting the message out in the news media. The ACCC monitors scam reports for trends and to ensure the most salient information is presented to the public.

Web users

Users: 1 842 745
Page views: 4 790 701

Radar subscribers

Subscribers: 59 957
▲ 24%

The Little black book of scams

Downloads: 13 348
Page views: 48 815
Hard copies: 162 095

Twitter

Tweets: 306
New followers: 3177
Total followers: 15 744
▲ 20%

In 2017, the Scamwatch website received 4 790 701 page views. *The little black book of scams*, a simple guide that helps Australians understand how scams work and how to avoid them was downloaded 13 348 times. It is also highly sought after in physical form for distribution by community groups, financial institutions and government organisations with 162 095 copies sent around the country.

The Scamwatch radar email subscription service grew in subscribers by 24 per cent to 59 957 by the end of 2017. Fourteen radar alerts were sent to these subscribers informing them of trending scams and how to avoid them throughout the year.

ACCC and Scamwatch media releases throughout 2017 generated hundreds of media requests which resulted in hundreds of radio, newspaper and television interviews. These interviews were broadcast both locally and nationally and reached millions of Australians.

The Scamwatch Twitter account also grew in subscribers by 20 per cent to 15 744 followers. The account posted 306 tweets and retweets alerting Australians to current scams and other scam-related information.

To ensure Australia's linguistically diverse population has greater access information on how to recognise, avoid and report scams, the ACCC made scams information available on the Scamwatch website in 12 languages other than English in 2017. These languages are:

- Arabic
- Chinese simplified
- Chinese traditional
- Dari
- Farsi
- Hindi
- Indonesian
- Korean
- Spanish
- Tagalog
- Turkish
- Vietnamese.

7.2 Engagement

In order to increase our ability to inform the public about scams and disrupt the activities of scammers, the ACCC engages with a range of government and private sector organisations. This engagement is driven through specific projects, such as the aforementioned scams intermediaries project, through more formal partnerships such as the Scams Awareness Network and at other times with a variety of organisations to deal with emerging scam issues.

Scams Awareness Network (SAN)

The SAN, formerly the Australasian Consumer Fraud Taskforce (ACFT), is made up of government regulatory agencies and departments in Australia and New Zealand that work alongside private sector, community and non-government partners to raise awareness about scams and disrupt them.

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

The core purpose of the SAN is for members to share information about scams regularly and to deliver a coordinated awareness campaign for consumers, the Scams Awareness Week in May each year, which also involves private sector and community partners. The major annual public engagement work of SAN is the Scam Awareness Week, formerly known as the National Consumer Fraud Week.

National Consumer Fraud Week 2017

The 2017 National Consumer Fraud Week campaign 'Spot social media scams' warned Australians to tread carefully when using social media platforms. In particular, Australians were advised to be on the lookout for dating and romance scams and online shopping scams.

The campaign attracted significant media attention and resulted in dozens of interviews which helped spread the message across newspapers, radio and television.

7.3 Other partnerships

Australian Transaction Reports and Analysis Centre

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 used by the ACCC to identify and track scam trends which inform our education and awareness-raising efforts.

Further information about AUSTRAC is available at www.austrac.gov.au.

Australian Cybercrime Online Reporting Network

The ACCC 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. ACORN is managed by the Australian Criminal Intelligence Commission.

The ACCC draws on ACORN data to help inform its understanding of scam and cybercrime trends.

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

The International Consumer Protection and Enforcement Network

The ACCC is a member of the International Consumer Protection and Enforcement Network (ICPEN), a network comprised of over 60 government 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.

Computer Emergency Response Team (CERT) Australia

CERT is the primary point of contact for cyber security issues affecting major Australian businesses and is a trusted source of information and advice on cyber security issues.

CERT provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest. These businesses and industries underpin essential service delivery across Australia, including banking and finance, communications, energy, resources, transport and water.

CERT manages the Joint Cyber Security Centre program which is a key initiative of the Australian Government's Cyber Security Strategy and brings together business, academia and government agencies to enhance collaboration on cyber security.

In 2017, the ACCC worked actively with CERT on cyber security and scam-related matters.

Appendix 1: Breakdown of scam categories by reports and reported losses

Overview of scam categories reported to the ACCC in 2017 by reports

Scam category	Reports	Reported loss	Reports with loss	Change in reports since 2016
Phishing	26 386	$810 224	221 (0.8%)	▲ 5.9%
Identity theft	15 703	$1 018 543	281 (1.8%)	▲ 23.3%
False billing	13 455	$2 796 980	737 (5.5%)	▼ –8.1%
Unexpected prize and lottery scams	12 726	$1 645 380	266 (2.1%)	▲ 83.1%
Other buying and selling scams	10 279	$3 584 426	2 279 (22.2%)	▲ 4.6%
Reclaim scams	9 329	$696 836	200 (2.1%)	▼ –30.2%
Remote access scams	8 685	$2 442 234	707 (8.1%)	▲ 36.4%
Upfront payment and advanced fee frauds	8 588	$4 148 089	1 004 (11.7%)	▼ –49.0%
Threats to life, arrest or other	8 297	$2 300 625	133 (1.6%)	▲ 546.7%
Online shopping scams	6 803	$1 380 563	3 320 (48.8%)	▲ 47.8%
Other business, employment and investment scams	6 131	$5 270 948	376 (6.1%)	▼ –5.7%
Hacking	5 757	$1 706 876	327 (5.7%)	▲ 42.1%
Malware and ransomware	4 412	$239 287	224 (5.1%)	▼ –29.0%
Dating and romance	3 763	$20 530 578	886 (23.5%)	▼ –8.4%
Inheritance scams	2 874	$2 768 972	42 (1.5%)	▼ –6.2%
Classified scams	2 729	$1 088 648	504 (18.5%)	▼ –12.7%
Job and employment	2 567	$1 428 942	188 (7.3%)	▼ –10.1%
Investment scams	1 997	$31 327 476	582 (29.1%)	▲ 13.1%
Mobile premium services	1 847	$48 843	712 (38.5%)	▼ –9.0%
Overpayment scams	1 815	$359 627	237 (13.1%)	▼ –35.3%
Travel prize scams	1 738	$83 403	71 (4.1%)	▲ 71.1%
Scratchie scams	1 330	$448 155	34 (2.6%)	▼ –0.7%
Nigerian scams	1 287	$1 665 373	163 (12.7%)	▼ –14.1%
Fake charities	1 146	$313 563	122 (10.6%)	▼–2.2%
Health and medical products	1 067	$523 241	231 (21.6%)	▲ 45.4%
Pyramid schemes	325	$363 238	46 (14.2%)	▼ –17.3%
Betting and sports investment scams	247	$1 750 033	111 (44.9%)	▼ –22.6%
Psychic and clairvoyant	237	$177 519	46 (19.4%)	▲ 37.0%
Not provided	8	$10 000	1 (12.5%)	▼ –98.0%
Total	**161 528**	**$90 928 622**	**14 051 (8.7%)**	**▲ 4.2%**

Overview of scam categories reported to the ACCC in 2017 by reported losses

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Investment scams	$31 327 476	1 997	582 (29.1%)	▲ 32.6%
Dating and romance	$20 530 578	3 763	886 (23.5%)	▼ -19.4%
Other business, employment and investment scams	$5 270 948	6 131	376 (6.1%)	▲ 92.2%
Upfront payment and advanced fee frauds	$4 148 089	8 588	1 004 (11.7%)	▼ -36.2%
Other buying and selling scams	$3 584 426	10 279	2 279 (22.2%)	▼ -13.2%
False billing	$2 796 980	13 455	737 (5.5%)	▲ 323.9%
Inheritance scams	$2 768 972	2 874	42 (1.5%)	▼ -21.2%
Remote access scams	$2 442 234	8 685	707 (8.1%)	▲ 71.6%
Threats to life, arrest or other	$2 300 625	8 297	133 (1.6%)	▲ 1 743.7%
Betting and sports investment scams	$1 750 033	247	111 (44.9%)	▼ -1.9%
Hacking	$1 706 876	5 757	327 (5.7%)	▼ -40.1%
Nigerian scams	$1 665 373	1 287	163 (12.7%)	▲ 18.6%
Unexpected prize and lottery scams	$1 645 380	12 726	266 (2.1%)	▲ 13.4%
Job and employment	$1 428 942	2 567	188 (7.3%)	▲ 26.8%
Online shopping scams	$1 380 563	6 803	3 320 (48.8%)	▲ 8.0%
Classified scams	$1 088 648	2 729	504 (18.5%)	▲ 17.8%
Identity theft	$1 018 543	15 703	281 (1.8%)	▲ 42.3%
Phishing	$810 224	26 386	221 (0.8%)	▲ 116.7%
Reclaim scams	$696 836	9 329	200 (2.1%)	▼ -40.4%
Health and medical products	$523 241	1 067	231 (21.6%)	▲ 540.5%
Scratchie scams	$448 155	1 330	34 (2.6%)	▼ -41.8%
Pyramid schemes	$363 238	325	46 (14.2%)	▲ 45.0%
Overpayment scams	$359 627	1 815	237 (13.1%)	▲ 40.2%
Fake charities	$313 563	1 146	122 (10.6%)	▲ 185.0%
Malware and ransomware	$239 287	4 412	224 (5.1%)	▼ -1.1%
Psychic and clairvoyant	$177 519	237	46 (19.4%)	▼ -53.6%
Travel prize scams	$83 403	1 738	71 (4.1%)	▼ -44.7%
Mobile premium services	$48 843	1 847	712 (38.5%)	▲ 21.0%
Not provided	$10 000	8	1 (12.5%)	No loss reported in 2016
Total	**$90 928 622**	**161 528**	**14 051 (8.7%)**	**▲8.8%**

Appendix 2: Scam tables by state and territory

Australian Capital Territory

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Investment scams	$574 943	56	21 (37.5%)	▲ 14.6%
Threats to life, arrest or other	$187 348	238	3 (1.3%)	No loss reported in 2016
Dating and romance	$103 830	72	18 (25.0%)	▼ -88.3%
Upfront payment and advanced fee frauds	$93 122	197	25 (12.7%)	▲ 265.6%
Pyramid schemes	$92 000	11	2 (18.2%)	▲ Very low loss in 2016
Hacking	$83 806	123	5 (4.1%)	▼ -72.5%
Other buying and selling scams	$82 089	341	75 (22.0%)	▼ -54.3%
Unexpected prize and lottery scams	$72 349	415	9 (2.2%)	▲ 99.0%
Nigerian scams	$67 251	40	8 (20.0%)	▲ 102.5%
Remote access scams	$64 229	136	17 (12.5%)	▲ 273.1%
Scratchie scams	$45 331	162	3 (1.9%)	▲ 54.7%
Other business, employment and investment scams	$42 167	168	12 (7.1%)	▲ 1 491.2%
Online shopping scams	$41 515	194	100 (51.5%)	▲ 47.2%
Betting and sports investment scams	$25 950	8	5 (62.5%)	▲ 765.0%
Identity theft	$23 126	444	8 (1.8%)	▲ 500.5%
Phishing	$20 467	796	8 (1.0%)	▲ Very low loss in 2016
Classified scams	$17 205	81	18 (22.2%)	▼ -72.2%
Job and employment	$15 449	56	7 (12.5%)	▲ 139.5%
False billing	$6 370	329	16 (4.9%)	▼ -33.9%
Overpayment scams	$4 035	42	6 (14.3%)	▼ -66.9%
Fake charities	$3 289	35	4 (11.4%)	▲ 732.7%
Reclaim scams	$2 939	211	6 (2.8%)	▼ -41.2%
Malware and ransomware	$2 599	86	4 (4.7%)	▼ -80.1%
Mobile premium services	$1 261	50	18 (36.0%)	▲ 44.6%
Health and medical products	$832	29	7 (24.1%)	▲ Very low loss in 2016
Travel prize scams	$500	104	1 (1.0%)	▼ -87.8%
Psychic and clairvoyant	$0	2	0 (0%)	No loss reported in 2016
Inheritance scams	$0	51	0 (0%)	▼ -100.0%
Total	**$1 674 002**	**4 477**	**406 (9.1%)**	**▼ -23.4%**

New South Wales

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Investment scams	$10 037 615	568	145 (25.5%)	▲ 40.3%
Dating and romance	$6 223 595	900	185 (20.6%)	▼ -33.7%
False billing	$1 347 799	3 977	214 (5.4%)	▲ 801.2%
Inheritance scams	$1 246 450	769	8 (1.0%)	▲ 81.3%
Other buying and selling scams	$1 168 639	3 145	674 (21.4%)	▼ -5.9%
Other business, employment and investment scams	$1 135 636	1 808	90 (5.0%)	▲ 107.6%
Remote access scams	$910 805	2 774	235 (8.5%)	▲ 49.5%
Upfront payment and advanced fee frauds	$718 096	2 490	271 (10.9%)	▼ -35.6%
Job and employment	$576 227	557	25 (4.5%)	▲ 245.9%
Identity theft	$571 771	4 927	106 (2.2%)	▲ 97.9%
Hacking	$561 664	1 640	98 (6.0%)	▼ -32.1%
Betting and sports investment scams	$555 785	56	22 (39.3%)	▼ -29.7%
Unexpected prize and lottery scams	$458 778	3 508	64 (1.8%)	▲ 10.4%
Online shopping scams	$405 945	2 021	1 046 (51.8%)	▲ 26.3%
Phishing	$353 300	8 321	66 (0.8%)	▲ 240.8%
Classified scams	$343 792	843	140 (16.6%)	▲ 28.4%
Fake charities	$244 714	327	44 (13.5%)	▲ 710.9%
Threats to life, arrest or other	$215 941	2 673	39 (1.5%)	▲ 259.9%
Scratchie scams	$159 950	235	7 (3.0%)	▼ -4.8%
Pyramid schemes	$135 460	77	8 (10.4%)	▲ 39.4%
Reclaim scams	$112 142	2 454	54 (2.2%)	▼ -61.7%
Overpayment scams	$110 549	533	72 (13.5%)	▲ 62.2%
Nigerian scams	$101 246	294	27 (9.2%)	▼ -75.5%
Psychic and clairvoyant	$100 760	40	18 (45.0%)	▲ 640.1%
Health and medical products	$82 075	291	55 (18.9%)	▲ 314.4%
Malware and ransomware	$63 952	1 436	70 (4.9%)	▼ -22.2%
Travel prize scams	$42 652	452	21 (4.6%)	▲ 144.3%
Mobile premium services	$15 703	550	215 (39.1%)	▲ 11.1%
Not provided	$10 000	3	1 (33.3%)	No loss reported in 2016
Total	**$28 011 041**	**47 669**	**4 020 (8.4%)**	**▲ 10.5%**

Northern Territory

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Dating and romance	$335 608	137	35 (25.5%)	▼ -6.2%
Investment scams	$225 456	20	8 (40.0%)	▲ 4.9%
Other business, employment and investment scams	$102 607	76	5 (6.6%)	▲ 53.4%
Health and medical products	$71 064	15	5 (33.3%)	▲ Very low loss in 2016
Upfront payment and advanced fee frauds	$64 201	74	14 (18.9%)	▲ 16.6%
Other buying and selling scams	$41 812	121	22 (18.2%)	▼ -20.6%
Unexpected prize and lottery scams	$31 421	110	6 (5.5%)	▲ 624.8%
Classified scams	$20 113	39	10 (25.6%)	▼ -50.7%
Pyramid schemes	$10 350	5	2 (40.0%)	No loss reported in 2016
Online shopping scams	$9 302	69	31 (44.9%)	▼ -81.4%
Nigerian scams	$7 640	43	9 (20.9%)	▼ -60.8%
False billing	$6 651	119	7 (5.9%)	▲ 114.3%
Inheritance scams	$5 800	44	4 (9.1%)	▼ -44.2%
Identity theft	$4 681	119	4 (3.4%)	▼ -65.9%
Hacking	$4 590	48	2 (4.2%)	▼ -86.6%
Psychic and clairvoyant	$4 400	5	2 (40.0%)	▲ 319.0%
Threats to life, arrest or other	$4 321	76	1 (1.3%)	No loss reported in 2016
Malware and ransomware	$2 635	40	6 (15.0%)	▲ 1 926.9%
Job and employment	$2 399	36	3 (8.3%)	▲ 31.5%
Fake charities	$1 940	12	2 (16.7%)	▲ Very low loss in 2016
Phishing	$1 800	156	2 (1.3%)	▲ 144.9%
Overpayment scams	$1 356	16	2 (12.5%)	▲ 255.9%
Remote access scams	$1 174	38	3 (7.9%)	▼ -30.9%
Travel prize scams	$392	24	1 (4.2%)	▼ -42.7%
Reclaim scams	$250	40	1 (2.5%)	▼ -76.0%
Mobile premium services	$177	30	6 (20.0%)	▼ -66.3%
Betting and sports investment scams	$68	2	1 (50.0%)	▼ -98.4%
Scratchie scams	$0	13	0 (0%)	▼ -100.0%
Total	**$962 208**	**1 527**	**194 (12.7%)**	**▲ 2.2%**

Queensland

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Investment scams	$5 600 713	399	93 (23.3%)	▼ -1.7%
Dating and romance	$3 153 239	652	153 (23.5%)	▼ -28.4%
Other business, employment and investment scams	$556 257	1 276	43 (3.4%)	▼ -24.9%
Other buying and selling scams	$533 286	2 216	438 (19.8%)	▼ -38.2%
Remote access scams	$482 996	2 336	149 (6.4%)	▲ 73.3%
Upfront payment and advanced fee frauds	$427 374	1 986	190 (9.6%)	▼ -32.2%
False billing	$427 195	3 224	165 (5.1%)	▲ 100.3%
Hacking	$414 431	1 481	63 (4.3%)	▼ -45.8%
Unexpected prize and lottery scams	$360 754	2 883	64 (2.2%)	▼ -14.6%
Online shopping scams	$285 948	1 333	596 (44.7%)	▲ 22.2%
Threats to life, arrest or other	$270 688	1 984	16 (0.8%)	▲ 1 230.9%
Betting and sports investment scams	$266 826	57	27 (47.4%)	▲ 39.3%
Classified scams	$236 333	612	99 (16.2%)	▲ 45.0%
Nigerian scams	$225 738	243	21 (8.6%)	▲ 9.3%
Job and employment	$166 221	521	25 (4.8%)	▲ 25.1%
Identity theft	$157 997	3 634	41 (1.1%)	▲ 99.7%
Inheritance scams	$140 250	623	5 (0.8%)	▼ -91.7%
Overpayment scams	$109 843	390	45 (11.5%)	▲393.4%
Phishing	$82 099	5 727	45 (0.8%)	▼ -24.2%
Reclaim scams	$63 606	2 102	29 (1.4%)	▼ -75.1%
Scratchie scams	$53 153	236	7 (3.0%)	▼ -72.8%
Malware and ransomware	$43 880	1 048	52 (5.0%)	▼ -15.4%
Psychic and clairvoyant	$31 334	50	6 (12.0%)	▲2 542.0%
Pyramid schemes	$26 293	60	6 (10.0%)	▼ -73.8%
Health and medical products	$23 198	252	41 (16.3%)	▼ -20.4%
Fake charities	$15 288	254	24 (9.4%)	▲ 61.2%
Travel prize scams	$14 067	327	12 (3.7%)	▼ -44.7%
Mobile premium services	$7 781	382	132 (34.6%)	▼ -5.9%
Not provided	$0	3	0 (0%)	No loss reported in 2016
Total	**$14 176 788**	**36 290**	**2 587 (7.1%)**	**▼ -19.2%**

South Australia

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Investment scams	$1 816 351	101	26 (25.7%)	▲ 21.1%
Dating and romance	$598 157	179	51 (28.5%)	▼ –24.6%
Betting and sports investment scams	$181 715	17	9 (52.9%)	▼ –1.7%
Remote access scams	$169 138	531	47 (8.9%)	▲ 166.5%
Other buying and selling scams	$145 858	685	127 (18.5%)	▼ –15.2%
Upfront payment and advanced fee frauds	$85 736	680	52 (7.6%)	▼ –59.8%
Other business, employment and investment scams	$85 527	518	28 (5.4%)	▼ –37.3%
Classified scams	$84 599	222	36 (16.2%)	▲ 84.8%
Phishing	$84 282	2 389	19 (0.8%)	▲ 111.1%
Online shopping scams	$69 407	424	204 (48.1%)	▲ 15.3%
Reclaim scams	$61 549	1 543	32 (2.1%)	▲100.9%
Job and employment	$57 131	174	11 (6.3%)	▲ 13.7%
Hacking	$37 984	384	20 (5.2%)	▼ –42.5%
Overpayment scams	$32 239	170	21 (12.4%)	▼ –21.8%
False billing	$30 917	1 114	57 (5.1%)	▲65.6%
Threats to life, arrest or other	$25 997	653	11 (1.7%)	No loss reported in 2016
Unexpected prize and lottery scams	$20 290	1 065	16 (1.5%)	▼ –80.1%
Identity theft	$18 882	1 490	17 (1.1%)	▼ –80.5%
Malware and ransomware	$18 193	336	18 (5.4%)	▲ 30.3%
Pyramid schemes	$15 855	17	3 (17.6%)	▼ –45.7%
Scratchie scams	$11 900	237	3 (1.3%)	▼ –85.4%
Health and medical products	$5 965	117	27 (23.1%)	▲ 40.6%
Travel prize scams	$4 671	145	6 (4.1%)	▼ –86.2%
Fake charities	$4 413	85	6 (7.1%)	▼ –85.5%
Mobile premium services	$2 594	145	55 (37.9%)	▲ 142.0%
Nigerian scams	$386	80	4 (5.0%)	▼ –98.7%
Psychic and clairvoyant	$118	13	2 (15.4%)	▼ –97.1%
Inheritance scams	$0	226	0 (0%)	No loss reported in 2016
Not provided	$0	2	0 (0%)	▼ –100.0%
Total	**$3 669 854**	**13 742**	**908 (6.6%)**	**▼ –6.4%**

Tasmania

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Dating and romance	$719 812	63	27 (42.9%)	▲ 69.7%
Investment scams	$130 365	39	8 (20.5%)	▼ -80.1%
Other business, employment and investment scams	$128 866	145	14 (9.7%)	▲233.7%
Hacking	$96 699	123	15 (12.2%)	▼ -56.8%
Unexpected prize and lottery scams	$82 596	325	6 (1.8%)	▲ 43.4%
Other buying and selling scams	$78 436	211	41 (19.4%)	▲ 98.6%
Online shopping scams	$47 703	125	55 (44.0%)	▲ 229.8%
False billing	$36 471	318	16 (5.0%)	▲ Very low loss in 2016
Fake charities	$26 035	30	5 (16.7%)	▲ 333.9%
Upfront payment and advanced fee frauds	$23 185	197	25 (12.7%)	▼ -41.2%
Betting and sports investment scams	$22 170	5	4 (80.0%)	▼ -57.3%
Remote access scams	$13 237	175	16 (9.1%)	▼ -13.3%
Scratchie scams	$7 700	139	2 (1.4%)	▼ -77.4%
Reclaim scams	$4 950	351	8 (2.3%)	▲ 5.3%
Classified scams	$4 725	48	9 (18.8%)	▼ -62.1%
Malware and ransomware	$2 946	102	5 (4.9%)	▲ 176.4%
Health and medical products	$2 289	23	8 (34.8%)	▲ 3 316.4%
Identity theft	$1 742	328	5 (1.5%)	▲ 4.0%
Psychic and clairvoyant	$1 695	7	2 (28.6%)	No loss reported in 2016
Phishing	$1 619	550	6 (1.1%)	▲ 40.1%
Travel prize scams	$1 575	64	3 (4.7%)	No loss reported in 2016
Overpayment scams	$550	56	2 (3.6%)	▲ 22.2%
Mobile premium services	$502	31	11 (35.5%)	▼ -17.2%
Job and employment	$100	43	1 (2.3%)	▼ -80.0%
Threats to life, arrest or other	$0	171	0 (0%)	▼ -100.0%
Inheritance scams	$0	65	0 (0%)	No loss reported in 2016
Pyramid schemes	$0	7	0 (0%)	No loss reported in 2016
Nigerian scams	$0	21	0 (0%)	No loss reported in 2016
Total	**$1 435 968**	**3 762**	**294 (7.8%)**	▼ **-11.8%**

Victoria

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Investment scams	$6 490 247	407	102 (25.1%)	▲ 22.7%
Dating and romance	$4 734 922	649	167 (25.7%)	▲ 4.2%
Other business, employment and investment scams	$2 141 551	1 329	90 (6.8%)	▲ 194.3%
Upfront payment and advanced fee frauds	$1 759 574	1 831	196 (10.7%)	▼ -52.9%
Threats to life, arrest or other	$1 526 948	1 813	42 (2.3%)	▲ 9 326.2%
Inheritance scams	$1 030 372	514	10 (1.9%)	▲ 50.8%
Other buying and selling scams	$802 215	2 051	485 (23.6%)	▼ -5.9%
False billing	$655 995	2 785	154 (5.5%)	▲ 375.8%
Remote access scams	$557 257	1 830	142 (7.8%)	▲ 125.7%
Nigerian scams	$418 034	200	27 (13.5%)	▲ 288.2%
Hacking	$406 998	1 251	77 (6.2%)	▼ -4.3%
Unexpected prize and lottery scams	$375 817	2 917	50 (1.7%)	▲262.4%
Job and employment	$368 524	619	52 (8.4%)	▲ 154.5%
Betting and sports investment scams	$365 940	56	17 (30.4%)	▲ 55.1%
Classified scams	$236 160	521	113 (21.7%)	▲ 27.8%
Online shopping scams	$225 001	1 375	627 (45.6%)	▼ -2.8%
Phishing	$212 104	5 709	52 (0.9%)	▲ 211.9%
Scratchie scams	$162 621	295	10 (3.4%)	▼ -35.4%
Identity theft	$132 155	3 181	65 (2.0%)	▲ 9.2%
Health and medical products	$99 013	162	37 (22.8%)	▲ 977.0%
Malware and ransomware	$72 098	833	37 (4.4%)	▲ 27.3%
Reclaim scams	$65 913	1 757	47 (2.7%)	▼ -85.2%
Overpayment scams	$43 428	391	49 (12.5%)	▼ -42.6%
Pyramid schemes	$35 270	77	11 (14.3%)	▲ 112.7%
Mobile premium services	$17 607	442	193 (43.7%)	▲ 102.7%
Fake charities	$15 504	251	27 (10.8%)	▲ 210.0%
Travel prize scams	$11 882	424	15 (3.5%)	▼ -76.4%
Psychic and clairvoyant	$11 114	35	10 (28.6%)	▼ -82.9%
Total	**$22 974 264**	**33 705**	**2 904 (8.6%)**	**▲ 22.0%**

Western Australia

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Investment scams	$2 779 925	208	58 (27.9%)	▲ 77.6%
Dating and romance	$1 178 472	241	63 (26.1%)	▼ -31.1%
Other business, employment and investment scams	$563 770	602	40 (6.6%)	▲ 132.4%
Betting and sports investment scams	$308 044	23	11 (47.8%)	▲ 76.0%
Upfront payment and advanced fee frauds	$275 793	783	84 (10.7%)	▼ -16.1%
Other buying and selling scams	$221 168	1 042	209 (20.1%)	▼ -22.2%
Remote access scams	$183 445	796	82 (10.3%)	▼ -1.0%
Nigerian scams	$142 812	106	13 (12.3%)	▲ 64.1%
Online shopping scams	$136 561	645	316 (49.0%)	▲ 24.0%
False billing	$77 723	1 370	76 (5.5%)	▼ -13.5%
Hacking	$65 832	627	37 (5.9%)	▼ -38.8%
Unexpected prize and lottery scams	$55 065	1 251	18 (1.4%)	▼ -78.1%
Phishing	$49 945	2 429	18 (0.7%)	▲ 55.0%
Classified scams	$49 665	249	38 (15.3%)	▼ -35.1%
Overpayment scams	$43 751	158	22 (13.9%)	▲ 213.9%
Identity theft	$40 867	1 439	26 (1.8%)	▼ -16.7%
Job and employment	$34 989	248	13 (5.2%)	▼ -78.4%
Threats to life, arrest or other	$33 062	606	12 (2.0%)	▲ 58.3%
Malware and ransomware	$23 094	423	19 (4.5%)	▲ 33.3%
Reclaim scams	$16 904	782	11 (1.4%)	▼ -87.0%
Pyramid Schemes	$8 900	32	4 (12.5%)	▲ 111.4%
Inheritance scams	$8 600	330	2 (0.6%)	▼ -96.7%
Health and medical products	$5 788	116	20 (17.2%)	▼ -40.7%
Mobile premium services	$2 985	197	76 (38.6%)	▼ -51.6%
Travel prize scams	$2 012	149	7 (4.7%)	▼ -86.3%
Fake charities	$662	96	5 (5.2%)	▼ -96.2%
Scratchie scams	$0	3	0 (0%)	No loss reported in 2016
Psychic and clairvoyant	$0	11	0 (0%)	▼ -100.0%
Total	**$6 309 834**	**14 962**	**1 280 (8.6%)**	**▲ 6.0%**

Appendix 3: Scam reports from businesses

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Other business, employment and investment scams	$1 659 465	658	46 (7.0%)	▲ 2 407.8%
False billing	$1 470 148	1 323	106 (7.9%)	▲ 630.4%
Hacking	$581 537	177	22 (11.9%)	▼ –66.2%
Other buying and selling scams	$407 381	592	89 (15.1%)	▼ –23.5%
Identity theft	$137 775	376	6 (1.6%)	▲ Very low loss in 2016
Upfront payment and advanced fee frauds	$118 316	412	25 (6.1%)	▲ 15.4%
Remote access scams	$55 875	73	7 (9.6%)	▲ 1 264.1%
Classified scams	$53 201	102	23 (22.5%)	▲ 35.4%
Malware and ransomware	$38 754	124	7 (5.6%)	▲ 274.1%
Overpayment scams	$35 503	107	7 (6.5%)	▲ 162.9%
Phishing	$29 140	654	4 (0.6%)	▲ 9 613.3%
Online shopping scams	$22 729	149	41 (27.5%)	▼ –63.4%
Fake charities	$21 168	105	23 (21.9%)	▲ 179.6%
Reclaim scams	$10 000	104	1 (1.0%)	▲ 226.8%
Investment scams	$9 600	22	3 (13.6%)	▼ –99.0%
Betting and sports investment scams	$6 050	2	1 (50%)	▲ Very low loss in 2016
Nigerian scams	$4 820	40	1 (2.5%)	▲ 1 406.3%
Health and medical products	$4 119	43	1 (2.3%)	▲ 136.3%
Threats to life, arrest or other	$2 090	135	1 (0.7%)	No loss reported in 2016
Mobile premium services	$1 738	27	13 (48.1%)	▲ 27.0%
Unexpected prize and lottery scams	$0	58	0 (0%)	No loss reported in 2016
Psychic and clairvoyant	$0	1	0 (0%)	No loss reported in 2016
Scratchie scams	$0	1	0 (0%)	No loss reported in 2016
Inheritance scams	$0	55	0 (0%)	No loss reported in 2016
Travel prize scams	$0	34	0 (0%)	▼ –100.0%
Dating and romance	$0	7	0 (0%)	No loss reported in 2016
Pyramid schemes	$0	2	0 (0%)	No loss reported in 2016
Job and employment	$0	49	0 (0%)	▼ –100.0%
Total	**$4 669 409**	**5 432**	**427 (7.9%)**	**▲ 23.4%**

Appendix 4: Scam reports from Indigenous consumers

Scam category	Reported loss	Reports	Reports with loss	Change in losses since 2016
Dating and romance	$746 790	101	22 (21.8%)	▼ –12.4%
Job and employment	$435 150	49	3 (6.1%)	▲ 2 000.1%
Investment scams	$164 904	28	13 (46.4%)	▲ 135.0%
Online shopping scams	$60 249	97	47 (48.5%)	▲ 376.7%
Unexpected prize and lottery scams	$56 948	194	9 (4.6%)	▲ 252.1%
Upfront payment and advanced fee frauds	$52 358	122	31 (25.4%)	▲ 1.3%
Other buying and selling scams	$28 120	142	38 (26.8%)	▼ –35.9%
Fake charities	$25 399	24	5 (20.8%)	▲ 208.2%
Other business, employment and investment scams	$18 291	76	9 (11.8%)	▲ 153.0%
Classified scams	$14 414	35	7 (20.0%)	▲ 52.9%
Scratchie scams	$11 000	8	1 (12.5%)	No loss reported in 2016
Hacking	$10 226	67	4 (6.0%)	▲ 360.0%
Betting and sports investment scams	$10 180	7	5 (71.4%)	▲ Very low loss in 2016
Pyramid schemes	$10 010	6	2 (33.3%)	No loss reported in 2016
Identity theft	$8 553	154	9 (5.8%)	▲ 1.1%
Nigerian scams	$6 914	71	14 (19.7%)	▼ –79.3%
False billing	$3 245	157	7 (4.5%)	▲ 1.6%
Malware and ransomware	$3 244	36	5 (13.9%)	No loss reported in 2016
Psychic and clairvoyant	$3 000	6	2 (33.3%)	No loss reported in 2016
Travel prize scams	$2 976	24	4 (16.7%)	No loss reported in 2016
Overpayment scams	$2 589	26	3 (11.5%)	▼ –57.4%
Threats to life, arrest or other	$2 500	68	1 (1.5%)	No loss reported in 2016
Phishing	$1 820	137	3 (2.2%)	▲ 151.0%
Health and medical products	$959	7	3 (42.9%)	▲ 185.4%
Mobile premium services	$463	36	14 (38.9%)	▲ 54.8%
Remote access scams	$65	31	1 (3.2%)	▼ –73.6%
Inheritance scams	$0	37	0 (0.0%)	▼ –100.0%
Reclaim scams	$0	64	0 (0.0%)	▼ –100.0%
Total	**$1 680 367**	**1 810**	**262 (14.5%)**	**▲ 14.2%**

ACCC

AUSTRALIAN COMPETITION
& CONSUMER COMMISSION