ACCC

AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

Targeting scams

Report of the ACCC on scams activity 2018

May 2019

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

ACCC 05/19_1548

www.accc.gov.au

Foreword

The Australian Competition and Consumer Commission's (ACCC) 10th annual *Targeting scams* report highlights the increasing harm of scams to the Australian community. This report seeks to inform the public about scams and identify emerging trends and techniques used by scammers to extract money and personal information from their victims.

In 2018, almost half a billion dollars ($489 million) in losses from over 378 000 scam reports was reported to the ACCC, the Australian Cybercrime Online Reporting Network (ACORN) and other state and territory government agencies. These losses represent an increase of 44 per cent over the $340 million reported in 2017 and demonstrate that the impact of scams on the Australian public is worsening.

Despite these record loss figures, the true cost of scams is likely much higher as many scams are not reported. The reasons for this vary. Some scam victims are embarrassed, some are unaware of where to report scams and others may fear the consequences of their own behaviour, particularly if they are manipulated into committing crimes such as money laundering or participating in pyramid schemes. Unfortunately, there are also many Australians who are not aware that they are caught up in long-term scams and continue to send money to scammers for years. The losses reported to the government are just the tip of the iceberg.

The ACCC's Scamwatch service received a record 177 516 scam reports with over $107 million in losses, with 'investment scams' and 'dating and romance scams' remaining the most financially harmful. When combined with losses reported to ACORN and other government agencies, losses to 'investment scams' increased 34 per cent to $86 million and losses to 'dating and romance scams' increased 44 per cent to $60.5 million compared with 2017.

In 2018 scammers continued to use technology to increase their reach and efficiency and to develop new techniques to scam more people. More scammers are now using social media and automated scam calls to access potential victims. In late 2018, reports of the Australian Taxation Office impersonation scam rose 900 per cent with tens of thousands of Australians reporting an automated 'robo-call' version of the scam.

To avoid the fraud and scam detection systems employed by banks, scammers are now increasingly asking for payment via unusual payment methods such as gift cards and cryptocurrencies. In 2018 Apple iTunes cards remained the most requested but demands for payment via Google Play cards and other gift cards are increasing rapidly. The shift towards Google Play and other gift cards may be a result of efforts by the ACCC, the Australian Taxation Office and other government and private organisations to display scam warnings about iTunes cards in major Australian retailer outlets.

Australian businesses were also hit hard by scammers in 2018 with sophisticated 'business email compromise' scams costing businesses over $60 million. These scams involve hacking business email systems and carefully impersonating key personnel to trick businesses into sending upcoming payments into a scammer's account. Consumers can also be caught up in these scams, for example when undertaking real estate transactions. Unsuspecting consumers pay their house deposits or legal fees to scammers instead of the agents and solicitors.

To combat these increasingly sophisticated scams and the growing volume of contact with potential victims, the ACCC and other government and private organisations came together to raise awareness and find intelligent solutions. In 2018, the ACCC engaged with a range of private sector 'intermediaries' whose businesses are commonly used in the course of scams. These included Australia's four major banks (ANZ, Commonwealth, NAB and Westpac), money remitters and online classified sites. The ACCC sent thousands of scam reports (where reporters gave their permission) to these intermediaries, resulting in improved scam detection, the blocking of scam transactions, the recovery of funds for victims, training for frontline bank staff and the blacklisting of scammer bank accounts.

We also engaged and cooperated on scam awareness-raising campaigns with state and federal government organisations through the Scams Awareness Network. In 2018 the Scams Awareness Network grew to 40 members who came together for Scams Awareness Week in May 2018 to raise awareness about threat-based impersonation scams. The ACCC and other organisations also assisted the Australian Cyber Security Centre with its 'Stay Smart Online' week, which raised awareness about cybercrime.

These dedicated campaigns were undertaken in addition to our ongoing education and awareness efforts, which included the distribution of 192 000 physical copies of *The Little Black Book of Scams*, 15 scam-related media releases, emails to our 77 000 Scamwatch radar email subscribers, media interviews and hundreds of posts via social media platforms.

In January 2018, the ACCC alerted Australian scam victims who lost money via Western Union to submit refund claims to try to get their money back. Victims who reported scams to the ACCC and indicated they lost money via Western Union were informed of their potential eligibility for reimbursement via email. Western Union agreed to pay a penalty of US$586 million to the United States Department of Justice (DOJ) after admitting to aiding and abetting wire fraud.[1] The DOJ is using this penalty to provide refunds to eligible people worldwide who were tricked into paying scammers via Western Union.

Scams are a complex and evolving problem affecting every demographic in Australia and continue to cause substantial financial and emotional damage. The scams reported to the ACCC are perpetrated overwhelming by criminals overseas, which makes it extremely difficult for law enforcement agencies to track them down and take action against them once the scam has occurred. The ACCC expects private organisations to do more to ensure their services, platforms, technology and systems are not able to be exploited by scammers. By focusing our efforts on education, awareness raising and disruption, the ACCC and its partners hope to reduce the harm caused by scammers and equip Australians with the knowledge to identify, avoid and report scams.

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

1 US FTC action—https://www.ftc.gov/enforcement/cases-proceedings/122-3208/western-union-company.

Contents

Glossary of scam terms

ATO impersonation scams

In recent years, scammers have increasingly impersonated the Australian Taxation Office (ATO) and offered Australians rebates for overpaid taxes or threatened them with legal action for not paying taxes. These scams do not have their own Scamwatch scam category. When reported to Scamwatch, ATO impersonation scams are commonly categorised as either 'rebate scams' for the version of the scam where the victim is offered a rebate or 'threats to life, arrest or other' for the version of the scam involving threats for not paying taxes.

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 claim to guarantee a profit on sporting events such as 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. If the prediction is correct, the investor earns a sizeable return on their investment (up to as much as 50–80 per cent), but if incorrect, they lose the entire invested sum. Binary options are very high risk because these values can move up or down unpredictably in short periods and the investor stands to lose their entire investment. For more information on binary options, visit the Australian Securities and Investment Commission's (ASIC) MoneySmart website at www.moneysmart.gov.au.

Business email compromise scams

These scams involve targeted phishing and hacking of a business 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. Other versions of this scam include impersonation of the chief executive officer of the company requesting money be transferred for some supposedly legitimate business purpose, altering details in real estate contracts, and requests for employees' salaries to be paid to a scammer's account.

Classified scams

Scammers use online and paper-based classifieds and auction sites to advertise (often popular) products or even puppies for sale at cheap prices. They will ask for payment up-front and often claim to be overseas. The scammer may try to gain victims' trust with false but convincing documents and elaborate stories.

Cryptocurrency

Cryptocurrencies, also known as virtual or digital currencies, are a form of electronic money. They do not physically exist as coins or notes. Virtual currencies can be bought or sold on an exchange platform using conventional money, or traded for other virtual currencies.

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 be collecting 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 processes many similar invoices without necessarily being across the details.

Hacking

Hacking occurs when a scammer uses technology to break into someone's computer, mobile device or network.

Health and medical products

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

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 victims the false promise of an inheritance to trick them into parting with their money or sharing their bank or credit card details.

Investment scams

Investment scams involve scammers offering a range of fake financial opportunities and the promise of high returns with low risk. 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 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.

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. Scammers do this without the knowledge of the mobile phone number's owner and set up their own mobile phone to receive messages to the ported number. This is usually done to intercept two-step authentication messages from banks or other service providers.

Mobile premium services

Scammers will often create SMS competitions to trick people into paying extremely high call or text rates when replying to unsolicited text messages on mobiles.

'Nigerian' scams

'Nigerian' scams are a form of up-front 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 that 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.

Phishing

Phishing scams are attempts by scammers to trick victims into giving out personal information such as bank account numbers, passwords and credit card numbers. A common form of phishing involves the impersonation of trusted organisations such as banks, telecommunications providers or government departments. This may be done via emails, text messages, web sites or over the phone.

Pyramid schemes

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

Ransomware and malware

Ransomware and malware involves a scammer placing harmful software onto a victim's computer. Malware can allow scammers to access 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.

Rebate scams

Scammers contact a victim pretending to be from the government or a utility company, bank or other well-known entity and claim the victim is owed money. However, they ask for an up-front fee before the larger rebate can be provided.

Remote access scams

The scammer contacts their victim claiming that the victim's computer is infected and that the scammer needs 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 or they may spin a complex story claiming they are working with authorities and they need to make transactions from the victim's bank account to 'track scammers'.

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.

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.

Unexpected prize and lottery scams

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

The role of Scamwatch

Scamwatch is run by the ACCC. The Scamwatch website provides information to consumers and small businesses about how to recognise, avoid and report scams.

The ACCC outlines its approach to scams each year in its Compliance and Enforcement Policy. In 2018–19, in relation to scam conduct, the ACCC prioritises awareness raising and education, and works with government and the private sector to reduce opportunities for scams to occur. We analyse data collected through our Scamwatch service to identify trends, monitor financial losses and inform our scam prevention strategies. On behalf of the Australian Scams Awareness Network, the ACCC runs Scams Awareness Week—an annual campaign to warn consumers about the ongoing risk of scams.

Education and awareness is used to reduce the harm caused by scams. Many scams, if tested in court, may be breaches of the Australian Consumer Law but because the scammers targeting Australians are overwhelmingly based overseas, it is extremely difficult for regulators such as the ACCC or even law enforcement agencies to track them down and take action against them.

Notes on data in this report

Most of the detail in this report is focused on reports made to Scamwatch by the public in 2018. However, to demonstrate the enormous cost of scams to the Australian public, we also provide high-level financial loss data from several government agencies where it is available. Due to the under-reporting of scams, we believe that the financial losses referred to in this report are only a fraction of the true losses suffered.

We analysed the first six months of 2018 ACORN data and projected losses for the remainder of the year. When ACORN or other external data is referenced, reasonable efforts have been undertaken to remove reports also reported to Scamwatch.

Changes to Scamwatch data in 2018

Scamwatch now receives well over 100 000 scam reports each year, the vast majority of which are submitted by the public through our Scamwatch web form. The web form asks the reporter to choose from 25 different scam categories, or an additional 'other scams' catch-all, to categorise their experience. These categories are referred to throughout this report.[2]

Some scam experiences are easy to categorise, for example 'investment scams' and 'dating and romance scams'. Other scam experiences may fall under several categories or may not fit into any of the 25 categories available on Scamwatch. The ACCC reviews how the public reports scams to Scamwatch and modifies the web form and categories where practical to improve accuracy in reporting.

Unless otherwise indicated, all Scamwatch 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.

In 2017 and 2018 a number of changes were made to improve our categories. One of these changes was to merge two categories[3] into a single 'other' category. An analysis of the reports contained in this new category indicates most could be re-categorised into existing categories. Due to the number of reports the ACCC received in 2018, dedicated re-categorisation of the 'Other scams' category has not been undertaken. To avoid confusion, all tables and charts in this report will omit the 'Other scams' category.

The ACCC publishes scam report data on the Scamwatch website on a monthly basis. Researchers, the media and the public can find the latest report and loss figures for all scam categories, basic demographic information such as location, gender and age as well as the contact method used in the scam.

2 More information about Scamwatch categories is available at https://www.scamwatch.gov.au/types-of-scams.

3 The two 'other' categories were 'other business, employment and investment scams' and 'other buying and selling scams'.

Targeting scams 2018

Losses

$489.7 million

2018 combined financial losses to scams
as reported to Scamwatch, ACORN and other government agencies

$107 million
Amount reported lost to Scamwatch

177 516
reports to Scamwatch

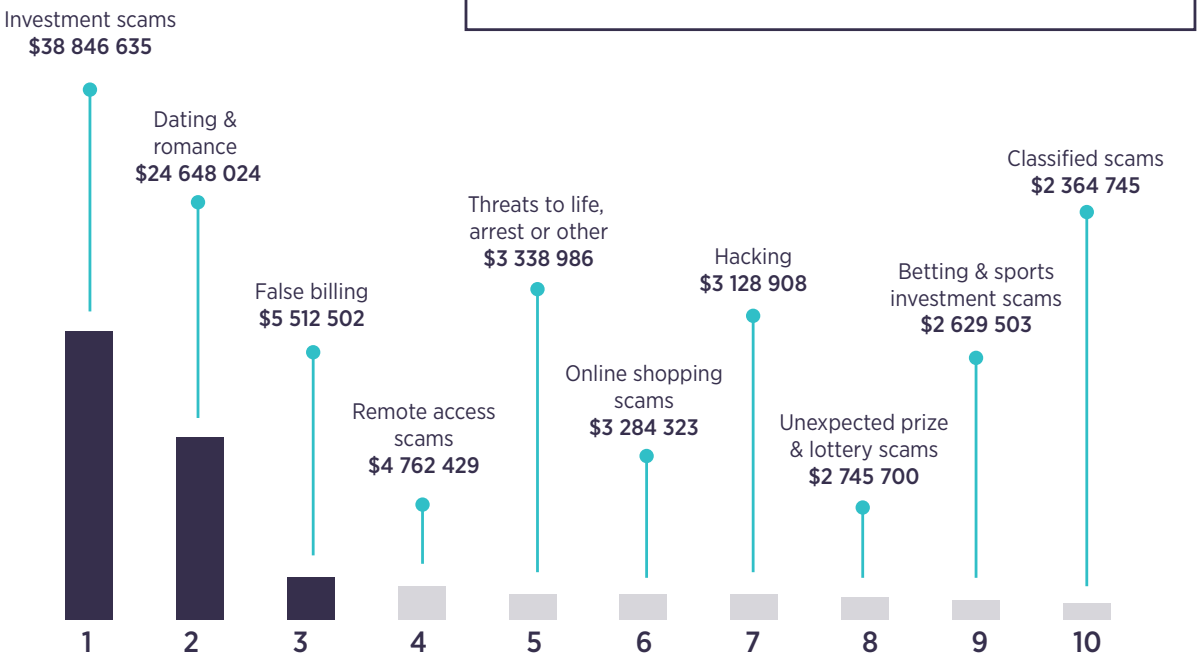
▲ **18%** since 2017
Average loss: **$5997**

Top scams by loss

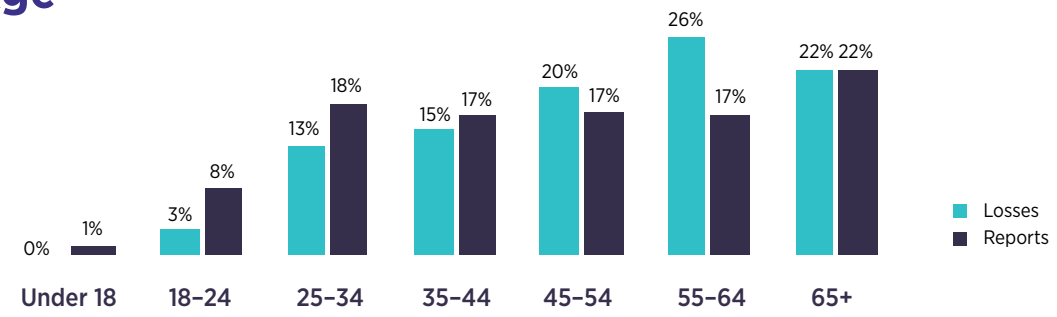
As reported to Scamwatch

Investment scams
Scamwatch & other agencies
$86 000 000

Dating & romance scams
Scamwatch & other agencies
$60 500 000



Age



Gender

Men

$56.9 million

79 600 reports

Males were more affected by investment scams, reporting losses of **$29.1 million**.

Women

$48.8 million

94 200 reports

Females reported losing more to dating and romance scams with **$19.5 million** in losses.

Non-specified

$1.2 million

3600 reports

Top contact methods by reports

46.9%

Phone

83 247 reports

$30.3 million

reported lost

23.2%

Email

41 170 reports

$25.3 million

reported lost

14.4%

Text message

25 595 reports

$2.1 million

reported lost

3.8%

Social media

6828 reports

$15.7 million

reported lost

1. Snapshot of scams in 2018

Key points

- In 2018, Scamwatch received 177 516 scam reports. This represents a 10 per cent increase over the 161 528 reports in 2017.
- The year 2018 had the highest level of financial loss ever reported to Scamwatch with $107 million reported lost. This is an 18 per cent increase over 2017 which totalled $90.9 million.
- Scamwatch, ACORN and other federal and state-based government agencies received over 378 000 reports about scams. The combined losses exceeded $489.7 million.
- The percentage of Scamwatch reports that included a financial loss increased from 8.7 per cent in 2017 to 10.1 per cent in 2018. This means more reports were from victims who actually lost money, as opposed to reports of attempted scams that failed to part a victim from their money.[4]
- The average of losses reported to Scamwatch was $5997. This is a 6.7 per cent decrease from the average loss in 2017.
- 'Investment scams' were the most financially damaging scams reported to Scamwatch in 2018 with $38.8 million reported lost. When combined with reports to other government agencies, 'investment scam' losses exceeded $86 million.
- 'Dating and romance scams' were the second most financially damaging with losses of $24.6 million. When combined with reports to other government agencies, 'dating and romance scam' losses exceeded $60.5 million.

Demographics

- People aged 55–64 reported losing more money than any other age group with losses of $24.8 million.
- Women reported more scams but lost less money than men. Women reported over 94 200 scams and reported losses of $48.8 million. Men reported over 79 600 scams and reported losses of $56.9 million.
- Women reported losing most to 'dating and romance scams' with $19.5 million in losses, while men were most affected by 'investment scams', reporting losses of $29.1 million.
- Australians aged 65 and older submitted over 26 400 reports to Scamwatch in 2018 with losses of over $21.4 million.
- Scamwatch received over 7800 reports from those who identified as suffering a disability or chronic illness with over $8.7 million in losses.
- In 2018 Indigenous consumers reported $3 million in losses (across 2434 reports). This represents a 79 per cent increase over the $1.6 million lost (across 1810 reports) in 2017.

Contact methods

- In 2018, 46.8 per cent of scam reports indicated contact via phone calls and 23.2 per cent by email. There were over 83 200 reports of phone-based scams with $30.3 million lost. There were 41 170 email-based scam reports with $25.3 million lost.
- Reports of phone and text-based scams increased in 2018, but reports of email scams decreased. Reports of phone-based scams increased from 40.3 per cent of contacts in 2017 to 46.8 per cent in 2018. This is partly because of large numbers of automated scam phone calls in 2018.

4 In 2018 the ACCC transitioned to a web-only reporting service. This may mean people are less likely to complete a Scamwatch web form unless they incurred a loss.

- ‘Phishing’ and ‘threats to life, arrest or other’ scams were the most common phone-based scams with 27 318 reports combined. However, ‘investment scams’ conducted over the phone resulted in the highest losses of $19 million.

Scam trends in 2018

ATO impersonation scams

- ATO impersonation scams spiked in November and December 2018 with many thousands of Australians receiving an automated message version of the scam. Scamwatch received 23 000 reports of these scams in 2018 with over $1.4 million in reported losses. The ATO also received over 114 000 reports with $2.8 million in reported losses making a combined total of $4.2 million in reported losses.

‘Threats to life, arrest or other’ scams

- Reports and losses attributed to scammers threatening arrest, loss of benefits and even deportation increased in 2018 with over 19 000 reports and $3.3 million in reported losses. This represents a 45 per cent increase over 2017 reports. The significant increase in ATO impersonation scams in late 2018 is a major contributor to this increase.

False billing scams

- In 2018 losses to ‘false billing’ scams increased by 97 per cent to $5.5 million. A large portion of these losses can be attributed to business email compromise scams in which both consumers and businesses receive emails from compromised businesses asking for payment for goods or services.

Remote access scams

- A more elaborate version of the classic tech support scam in which scammers impersonate the police and ask for access to a victim’s computer to catch scammers, resulted in increased losses for ‘remote access scams’ in 2018. Scamwatch received over 11 300 reports with $4.7 million in reported losses, an increase of 95 per cent over 2017 losses.

Cryptocurrencies in scams

- In 2018, there were 674 reports where cryptocurrency was used to pay the scammer with reported losses of $6.1 million. This is a 190 per cent increase over the $2.1 million reported in 2017.

iTunes and Google Play cards in scams

- Scammers requesting payment through iTunes cards increased in 2018 with $3.1 million in reported losses. Scammers requesting payment through Google Play cards also increased with losses rising from $1250 reported in July to $179 000 in December 2018.

Scams reported by businesses

- In 2018, businesses reported 5846 scams with $7.2 million in losses.
- Business email compromise losses reported to Scamwatch in 2018 exceeded $3.8 million. When combined with reports to ACORN, losses to business email compromise scams exceeded $60 million. This is a 170 per cent increase over the combined losses of $22.1 million reported in 2017.

Education and engagement

- In 2018, the Scamwatch website received over 6.2 million page views, an increase of 29 per cent over 2017’s 4.8 million page views.

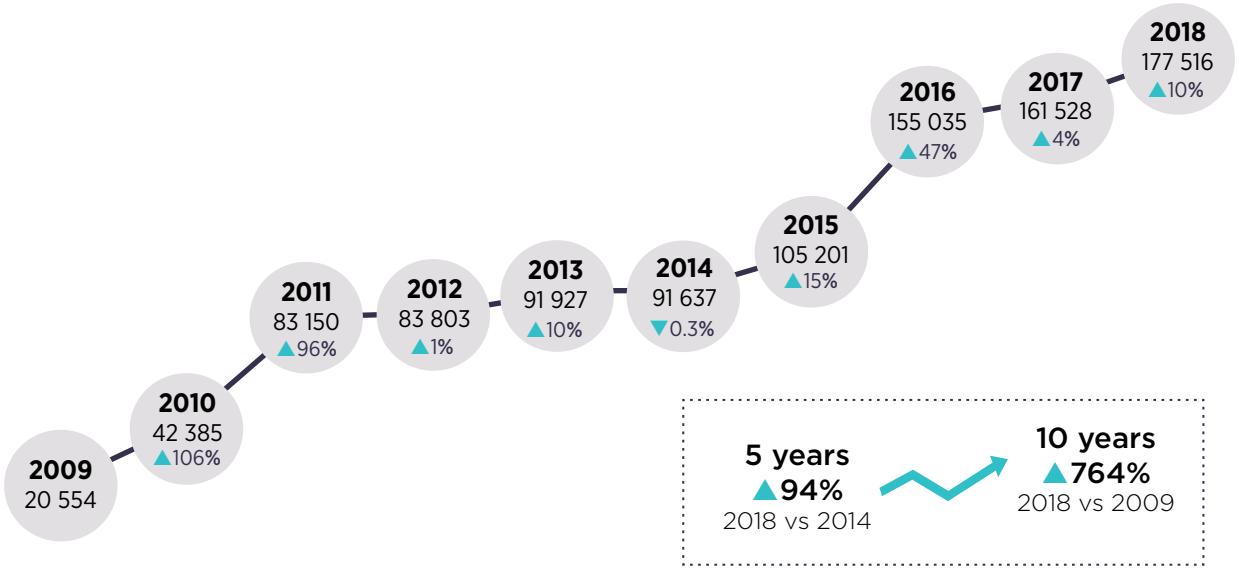
- In 2018 *The Little Black Book of Scams*, a simple guide that helps Australians understand how scams work and how to avoid them, was downloaded almost 23 000 times and over 192 000 copies were distributed.
- The Scamwatch radar email subscription service grew in subscribers from 60 000 at the end of 2017 to over 77 000 at the end of 2018. Fifteen radar alerts were sent throughout the year to subscribers informing them of trending scams and how to avoid them.
- The Scamwatch Twitter account also grew in subscribers by 22 per cent to 19 253 followers. The account posted 402 tweets and retweets alerting Australians to current scams and other scam-related information in 2018.
- ACCC and Scamwatch media releases throughout 2018 generated hundreds of media requests for information and for interviews which resulted in hundreds of radio, newspaper and television appearances. These interviews were broadcast to a national audience of millions.
- In January 2018 the ACCC alerted Australian scam victims who lost money via Western Union to submit refund claims to try to get their money back. Western Union agreed to pay a penalty of US$586 million to the United States Department of Justice (DOJ) after admitting to aiding and abetting wire fraud. The DOJ is using this penalty to provide refunds to eligible people worldwide who were tricked into paying scammers via Western Union.
- The ACCC as Chair of the Scams Awareness Network welcomed several new members to the network, which seeks to coordinate efforts to inform the Australian public about scams. The Scams Awareness Network currently has 40 members from across Australian federal and state government organisations as well as two New Zealand based government agencies.
- The 2018 Scams Awareness Week campaign ran from 21–25 May 2018 and focused on threat-based impersonation scams with the slogan 'Stop and check: is this for real?' The campaign included 47 campaign partners from government, community and private sectors.
- In 2018, the ACCC engaged with a range of private sector 'intermediaries' whose businesses are commonly used in the course of scams. These included Australia's four major banks (ANZ, Commonwealth, NAB and Westpac), money remitters, and online classified sites. The ACCC recognised that these intermediaries are in a unique position to identify and intervene in scams using their facilities.
- The ACCC engaged with a large range of government and private stakeholders to inform them about current scams and to share information. We also agreed to participate in the Australian Communications and Media Authority's Scam Technology Project which aims to explore technological solutions to address the proliferation of scams over the telecommunications network.

2. 2018 scam statistics

2.1 Scam reports in 2018

The ACCC received 177 516 scam reports in 2018. This is an increase of 9.9 per cent over reports in 2017 which totalled 161 528. Over the past five years, the number of reports received has increased by 94 per cent. Compared with the number of reports received 10 years ago in 2009, reports have increased by 764 per cent. This is both a reflection of a growing scam problem and an increased knowledge in the Australian community of where to report scams.

Figure 1: Scamwatch reports 2009–18



The top three scam categories reported in 2018 were 'phishing' scams, 'threats to life, arrest or other' and 'identity theft' scams.[5] In 2018, reports of these scams were boosted partly because of scammers using technology to automate communication via emails, text message and phone calls. Two concerning trends in 2018 were an increase of 'remote access scam' reports by 31 per cent and the 134.5 per cent increase to 'threats to life, arrest or other' scams over 2017 numbers. Both also resulted in more financial loss in 2018. The reason for these increases is explored later in this report.

'Identity theft' remained a problem in 2018, despite reports decreasing by 18 per cent, to 12 800 and $1.4 million in losses. Identity theft is a risk in all scams as scammers often collect a wealth of personal information from victims.

The impact of identity theft is worsened by the time and effort it takes many Australians to recover their identity, rectify credit reports, and update (or get new) bank accounts and personal identification documents when compromised by scammers. For example, victims may be unable to obtain a new driver's licence, which means the cycle of identity theft and recovery continues over many years. Over 9700 scam reports in 2018 indicated a loss of banking details and over 27 400 reports indicated a loss of personal information. Banking information was obtained by scammers most in reports about 'online shopping scams' and 'remote access scams'. 'Identity theft' and 'phishing' scams had the most reports of personal information loss. However, it is likely that many more scam victims have exposed a wealth of their information to scammers without realising it.

5 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).

IDENTITY THEFT

Scammers want to steal your identity for financial gain

SCAMMERS GAIN ACCESS TO YOUR PRIVATE INFORMATION BY:

- Breaking into your mailbox
- Phishing emails and text messages
- Fake online quizzes, surveys and job advertisements
- Fake online stores
- Hacking your email and other online accounts
- Social media requests from people you don't know

SCAMMERS WILL USE YOUR INFORMATION TO:

- Purchase expensive goods in your name
- Drain your bank account
- Open bank accounts and take out loans
- Take out phone and other contracts
- Transfer your superannuation
- Contact your friends on social media to impersonate you

STATISTICS:

Losses: **$1.4 million**

Reports: **12 800**

100% of scams have the potential for identity theft

Reports to Scamwatch in 2018

PROTECT YOURSELF:

- Secure your letterbox and online accounts
- Recognise the value of your personal information

For example, the ATO impersonation scam usually starts with a scammer obtaining a number from a directory or call list and so they may start with only an initial, surname and possibly a street address. By asking just a few questions, the scammer may be able to elicit the victim's first name and tax file number and, later in the scam, driver's licence details, mobile phone number and online banking details. The scammer can then use this information in other scams or sell it online to other scammers.

Victim story: 'Identity theft' scam

Reported loss: $30 000

The scammer impersonated a NAB employee and already had sufficient information to convince anyone that he was legitimate. He explained that he was calling about suspicious transactions on my account and asked me if I had recently made transactions for a certain amount, maybe in another country.

He was very convincing. He said that he will stop the payment and after going away for a while came back and asked me for my ID to make sure he was talking to the account owner. He then gave advice on the process that he will use to stop the fraudulent transactions. He asked me to provide him with the access number appearing on my mobile phone. Once I provided it, he changed my online banking password.

He told me that the bank will stop further transactions but will need to close off all my accounts. At this point I couldn't check my internet bank accounts. He then went away and came back on the phone and convinced me that there was another figure that looked suspicious and repeated the process.

After three times he told me to turn off my mobile phone for 24 hours. This was so the bank could not verify changes happening to my account but I did not realise this at the time. At all times the scammer kept convincing me that he was helping stop the thief while he was the thief.

Table 1: Top 10 scam categories reported to the ACCC in 2018 by number of reports[6]

Scam category	Reports	Reported losses	Reports with loss	Change in reports since 2017
Phishing	24 291	$933 470	357 (1.5%)	▼–7.9%
Threats to life, arrest or other	19 455	$3 338 986	344 (1.8%)	▲134.5%
Identity theft	12 800	$1 472 388	445 (3.5%)	▼–18.5%
Remote access scams	11 344	$4 762 429	881 (7.8%)	▲30.6%
False billing	10 996	$5 512 502	1 241 (11.3%)	▼–18.3%
Unexpected prize & lottery scams	10 049	$2 745 700	338 (3.4%)	▼–21%
Online shopping scams	9 691	$3 278 776	5 567 (57.4%)	▲42.5%
Hacking	8 625	$3 128 908	502 (5.8%)	▲49.8%
Classified scams	4 970	$2 364 745	1 173 (23.6%)	▲82.1%
Ransomware & malware	4 356	$151 195	92 (2.1%)	▼–1.3%

Table 1 provides an overview of the top 10 scams by number of reports. The 'Reports with loss' column provides the number and percentage of reports that include any monetary loss. The most commonly reported scam ('phishing') is high in number of reports but only a small per cent involved any money being sent to scammers. This percentage is known as the 'conversion rate'.

A low conversion rate may suggest that the scam is not effective or its true purpose, as in the case of 'phishing' scams, is not to get money but information. Alternatively, a low conversion rate may indicate the scammers contact a very large number of people, most of whom identify the scam and avoid it, but because of the volume of contacts, the scam may still result in large losses. 'Threats to life, arrest or other' is a good example of such a scam. Only a small percentage of people reporting this type of scam suffered a monetary loss but from that small percentage large losses were suffered.

6 Appendix 2 provides a full breakdown of Scamwatch reports for 2018.

ONLINE SHOPPING SCAMS

Scammers create fake shopping websites and ads for products that don't exist

Scammers set up fake retailer websites that look like genuine sites

They offer products at very low prices

They may sell via fake ads on eBay, classified sites, Instagram and Facebook

Scammers accept payment but don't provide any product

The scammers may also use your payment and shipping details for identity theft

STATISTICS:

Losses: **$3.2 million**

Reports: **9600+**

Average loss: **$588**

Reports to Scamwatch in 2018

PROTECT YOURSELF:

If the price seems too good to be true, it probably is

Do a search to see what others have said about them & check the comments

'Threats to life, arrest or other' scams and 'remote access scams' increased in 2018 and are discussed in greater detail later in this report. Other trends in scam report numbers in 2018 include:

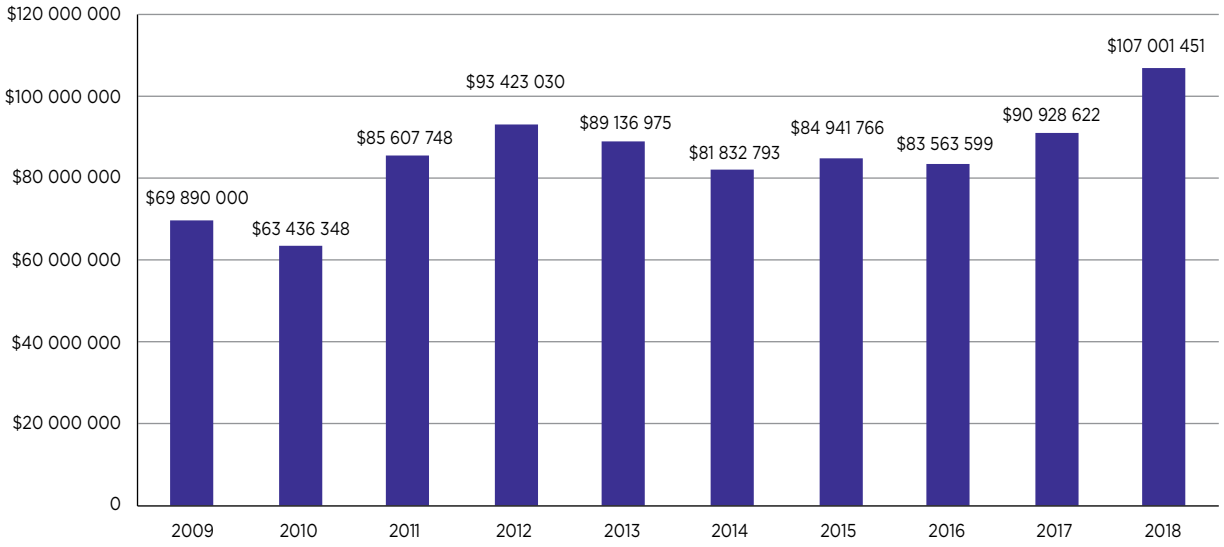
- 'Classified scams', which increased 82.1 per cent over 2017 reports. This is partly attributable to an increase in automobile sale-related scams on classified sites. An analysis of these reports indicate scammers are creating dozens of Gmail, Yahoo and Hotmail email accounts with minor variations between them such as the addition of a number or slightly different spellings of the same name. This indicates that a relatively small group of scammers is targeting classifieds buyers and sellers.
- 'Online shopping scams' increased in reports by 42.5 per cent in 2018 with losses exceeding $3.2 million. An analysis of Scamwatch data indicates popular items Australians are trying to buy from scammers include shoes, Apple and Samsung mobile phones, puppies and cars.

2.2 Financial losses to scams in 2018

In 2018, financial loss reported to Scamwatch totalled $107 001 451. This represents an increase of 18 per cent over losses in 2017 and is the highest such amount ever reported to Scamwatch.

Figure 2 shows a comparison of losses reported to Scamwatch over the last 10 years. It shows that annual losses reported to Scamwatch since 2009 have increased by over $37 million.

Figure 2: Reported financial losses to Scamwatch 2009–18



Scamwatch reports in 2018 indicated a number of key trends:

- Losses to 'investment scams' increased by 24 per cent or $7.5 million over 2017 losses to $38.8 million. Combined losses with reports to ACORN and other government agencies brings 'investment scam' losses to $86 million in 2018.
- 'Dating and romance scam' losses decreased between 2016 and 2017 but increased by $4.1 million in 2018 to $24.6 million. Combined losses with reports from ACORN and other agencies for 'dating and romance scams' in 2018 were over $60.5 million.
- Losses to 'false billing' scams reported to Scamwatch increased by 103.7 per cent, from $2.7 million in 2017 to $5.5 million in 2018.
- Losses to 'remote access scams' increased by 95 per cent over 2017 losses to $4.7 million. Reports to Scamwatch revealed an elaborate new version of this scam that convinced the victim they were helping authorities and proved devastating for many victims.
- Scammers threatening arrest, fines, loss of benefits and even deportation resulted in losses of $3.3 million in 2018. This represents a 45 per cent increase over 2017 reports. The significant increase in ATO impersonation scams in late 2018 is a major contributor to this increase.

Top 10 Scamwatch categories in 2018 by losses

Table 2 provides an overview of the top 10 Scamwatch scam categories by losses in 2018.

Table 2: Top 10 scams in order of reported losses

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
Investment scams	$38 846 635	3 508	1 189 (33.9%)	▲24%
Dating & romance scams	$24 648 024	3 981	1 257 (31.6%)	▲20.1%
False billing	$5 512 502	10 996	1 241 (11.3%)	▲97.1%
Remote access scams	$4 762 429	11 344	881 (7.8%)	▲95%
Threats to life, arrest or other	$3 338 986	19 455	344 (1.8%)	▲45.1%
Online shopping scams	$3 278 776	9 691	5 567 (57.4%)	▲137.5%
Hacking	$3 128 908	8 625	502 (5.8%)	▲83.3%
Unexpected prize & lottery scams	$2 745 700	10 049	338 (3.4%)	▲66.9%
Betting & sports investment scams	$2 629 503	273	101 (37%)	▲50.3%
Classified scams	$2 364 745	4 970	1 173 (23.6%)	▲117.2%

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 such as the ATO, state-based consumer protection agencies and other government departments also receive public enquiries and reports about scams.

This report attempts to collate as many of the reports received by other agencies as possible in order to illustrate the extent of the financial loss suffered by Australians in 2018.

Where the ACCC was able to obtain scam report data, when combined, the losses reported to these various agencies exceeded $489.7 million for 2018. However, this does not reflect the total loss suffered by Australians in 2018 because many scams go unreported.

ACORN

The Australian Cybercrime Online Reporting Network offers an online reporting channel for cybercrime including many crimes that are not considered 'scams' such as cyberbullying 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.

The ACCC analysed the ACORN data from 2018 and identified those reports that best match 'scams' as defined by the ACCC. Reports in which the reporter indicated they had also reported to Scamwatch were excluded. The analysis concluded that scam reports to ACORN amounted to over $367.9 million in losses from over 56 000 reports.

A breakdown of those ACORN reports that best match the Scamwatch scam categories is provided in table 3.

Table 3: Top five ACORN scam categories by losses

Scam Category	Reported losses	Reports
Offered an investment opportunity	$42 709 358	674
Asked to pay money up-front or transfer money ('Nigerian' scam)	$40 462 696	1 384
Dating or romance scam	$32 915 024	542
An online account has been hacked into	$29 291 118	1 826
Online identity theft	$26 718 892	1 866

Australian Taxation Office

In 2018, the ATO received 114 625 reports of the ATO impersonation scam with over $2.8 million in reported losses.

Reports to the ATO and Scamwatch increased in November 2018 when an automated message version of the scam emerged.

Although scammers continued to request payments via iTunes cards, 2018 saw the introduction of payment requests via Google Play cards and Bitcoin. In 2018, reports to the ATO indicated losses of $496 701 via iTunes cards, $647 817 via Google Play cards and $732 917 via Bitcoin.

Global networks indicate these scams and payment methods are being deployed across a range of international taxation jurisdictions.

The data shows that the scam is Australia wide and no particular state's residents are specifically targeted.

Office of the Australian Information Commissioner

In February 2018, the Notifiable Data Breaches scheme came into effect. Under the scheme, agencies and organisations regulated under the Australian *Privacy Act 1988* are required to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to individuals whose personal information is involved in the breach.

Data collected by the OAIC from organisations complying with the scheme shows concerted efforts from cybercriminals to access the personal information of Australians. The OAIC received over 800 notifications, with malicious or criminal attacks accounting for more than 60 per cent of breaches. Other breaches were caused by system or human errors. These breaches were suffered by a range of organisations that store personal information such as those in the health, financial and education sectors.

This means that in hundreds of separate incidents, cybercriminals attacked the IT systems of Australian organisations to access the personal information of (potentially) millions of Australians. The most common method of access was phishing to trick people within those organisations into providing access credentials such as usernames and passwords. Hacking, ransomware and malware were also employed to access personal data.

More information about the Notifiable Data Breaches scheme, including detailed reports, can be found at the OAIC website at www.oaic.gov.au.

Department of Human Services

The Department of Human Services (DHS) received 6506 reports in 2018 about government impersonation scams with $1.3 million in reported losses.

There were two main scams reported to the DHS in 2018. One was a text message-based phishing scam in which scammers presented themselves as 'MyGov' or 'Medicare' and stated the recipient was owed a rebate. The text messages also included a link to a convincing, fake website to claim the rebate. If victims visited the website, they were presented with a web form that asked for a wealth of identification information.

The other most common scam reported to the DHS was a landline phone-based rebate scam in which scammers told victims they were owed a rebate by the government. Victims were told that to receive the rebate, they had to first pay a small processing fee.

Of the reports to the DHS, 44.6 per cent came from those aged over 65 years old and 60 per cent were from women.

Department of Mines, Industry Regulation and Safety, Western Australia

The Department of Mines, Industry Regulation and Safety, Western Australia operates the website WA Scamnet (www.scamnet.wa.gov.au) which, like Scamwatch, provides information to help the public identify and avoid scams and a web form to report scams.

In 2018, WA Scamnet received over 22 000 scam reports and 569 Western Australians reported losing almost $10.7 million.

WA Scamnet has based the scam categories on its website on Scamwatch categories. Table 4 provides a breakdown of these scams by category.

Table 4: Scam losses reported to WA Scamnet in 2018

Scam category	Reported losses
Jobs & investment	$4 501 432
Dating & romance	$2 958 633
Buying & selling	$1 710 852
Unexpected money	$756 297
Unexpected winnings	$488 040
Attempts to gain your personal information	$209 087
Other	$56 000
Threats & extortion	$550
Total	**$10 680 891**

WA Scamnet identified business email compromise scams and ATO impersonation scams as particularly problematic in 2018.

United States Federal Trade Commission

The United States Federal Trade Commission (FTC) is the ACCC's counterpart agency in the USA and also accepts reports of various types of fraud. Although not exactly matched to Scamwatch scam categories, the FTC's 2018 report on 'fraud activity' describes many frauds and scams similar to those suffered by Australians. The FTC pulls together reports and information from a number of US federal and state-based authorities to arrive at amalgamated numbers. The US population is much larger than Australia's and this is reflected in the enormous volume of frauds and losses described in the FTC's report.

The FTC reported almost three million frauds with reported losses of almost US$1.48 billion in 2018. This is an increase in losses of over US$406 million from the previous year. The reports included 535 000 'impostor scams' and over 440 000 reports of identity theft. 'Impostor scams' (including romance scams, the impersonation of government and other organisations and the impersonation of relatives) cost US victims over US$488 million in losses.

As in Australia, most scams in the USA continue to be delivered via telephone with 69 per cent of fraud using this contact method. Also, in line with reports to Australian authorities, older Americans reported losing the most money with the 60–69 age range reporting losses of US$184 million.

For detailed information about fraud reported to the FTC, please visit www.consumer.ftc.gov.

2.3 How scammers connect with victims

Figure 3: Contact methods 2018

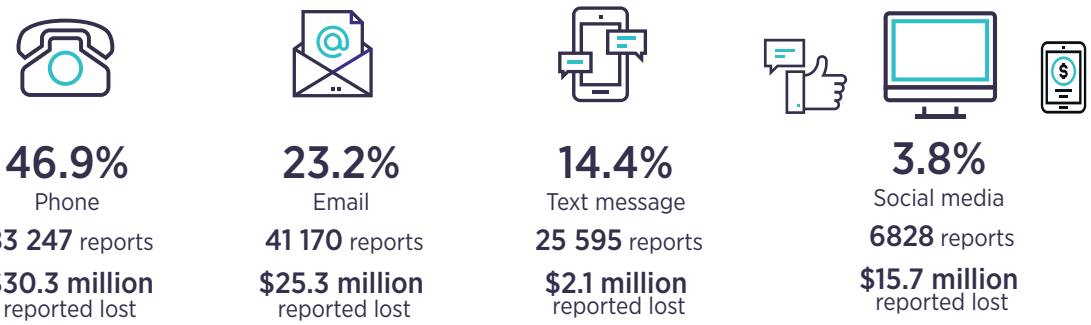


Table 5: Breakdown of reports and losses by contact method

Contact mode	Reports	Reported losses	Reports With loss	Change in losses since 2017
Phone	83 247	$30 334 678	3 066 (3.7%)	▲4%
Email	41 170	$25 318 010	3 345 (8.1%)	▲44.9%
Internet	10 562	$16 940 552	5 423 (51.3%)	▲14.8%
Social Networking/Online Forums	6 828	$15 769 183	3 008 (44.1%)	▲0.1%
In Person	1 862	$9 389 573	685 (36.8%)	▲20.5%
Mobile Apps	2 265	$5 026 961	814 (35.9%)	▲162.1%
Text Message	25 595	$2 176 450	1 007 (3.9%)	▲27.5%
Mail	4 828	$1 948 930	466 (9.7%)	▲7.1%
Fax	213	$42 666	10 (4.7%)	▲27%
N/A	946	$54 448	16 (1.7%)	▼–89%
Total	**177 516**	**$107 001 451**	**17 840 (10%)**	**▲18%**

Phone-based scams

In 2018 telephone calls remained the most common way scammers contacted victims. Impersonation of well-known or trusted organisations such as government departments, the police, banks or utility providers was the most common technique.

Scammers cold call, offering rebates for overpaid taxes, threats of arrest for underpaid taxes or assistance for problems detected on the victim's computer. Phone scammers use pressure tactics, emotional manipulation and scripted technical language to get victims to do what they want.

Losses attributed to phone-based scams exceeded $30.3 million in 2018, which accounts for 28.3 per cent of total losses.

Table 6: Top three phone-based scams by reported losses

Scam category	Reported losses	Reports	Reports with loss
Investment scams	$19 068 142	1 456	370 (25.4%)
Remote access scams	$4 066 850	9 476	668 (7%)
Threats to life, arrest or other	$2 477 817	17 303	289 (1.7%)

The top three phone-based scams of 2018 by reported losses were 'investment scams', 'remote access scams' and 'threats to life, arrest or other' scams.

'Remote access scams' involve the scammer tricking the victim into providing them with access to their computer. In the past, scammers commonly impersonated Microsoft or Telstra and told the victim there was an issue with their computer they needed to fix. A new version of this scam involves the scammer impersonating the Australian Federal Police (AFP) to catch scammers. More information on this is available at section 3.3 of this report.

Table 7: Top three phone-based scams by reports

Scam category	Reported losses	Reports	Reports with loss
Threats to life, arrest or other	$2 477 817	17 303	289 (1.7%)
Phishing	$227 725	10 015	80 (0.8%)
Remote access scams	$4 066 850	9 476	668 (7%)

The most common type of phone-based scam reported in 2018 was 'threats to life, arrest or other', which were mostly ATO impersonation scams. 'Phishing' and 'remote access scams' were also high in number.

Only 1.7 per cent of phone-based 'threats to life, arrest or other' reports included a loss, which indicates that most people who received these messages did not return the call and did not lose any money but still reported the scam to Scamwatch.

Email-based scams

Email was the second most common contact method reported in 2018 and accounted for 23.2 per cent of all scam contacts (compared with 31 per cent of scams in 2017).

Table 8: Top three email-based scams by reported losses

Scam category	Reported losses	Reports	Reports with loss
Investment scams	$5 934 687	592	124 (20.9%)
Dating & romance scams	$4 714 671	753	410 (54.4%)
False billing	$4 126 887	6 316	21 (0.3%)

In terms of losses, 'investment scams' were the most financially devastating email-based scams with $5.9 million reported lost. Losses to 'dating and romance scams' and 'false billing' scams also exceeded $4.1 million each.

Table 9: Top three email-based scams by reports

Scam category	Reported losses	Reports	Reports with loss
Phishing	$476 024	7 039	141 (2%)
False billing	$4 126 887	6 316	172 (2.7%)
Ransomware & malware	$35 259	3 302	410 (12.4%)

In terms of numbers of reports, 'phishing' scams were the most prevalent with over 7000 reports. 'Phishing' scams delivered by email and phone were very high in volume but resulted in lower in reported losses. This is partly because losses resulting from 'phishing' scams usually occur as a consequence of hacking or identity theft and are reported in those scam categories.

'False billing' scams increased by 97 per cent in 2018. Reports showed that business email or marketing systems were compromised by scammers who sent out hundreds or even thousands of fake invoices appearing to come from legitimate businesses to large mailing lists. Many victims responded to these thinking they owed a legitimate payment.

Scams through social media

In 2018, 3.8 per cent of reports with a contact method provided were recorded as 'Social networking/online forums' scams. This represents 6828 reports, an increase of 2117 over 2017 numbers. Despite these reports accounting for only 3.8 per cent of total reports for 2018, the reported losses exceeded $15.7 million or 14.7 per cent of the total losses reported to Scamwatch.

Table 10: Top three social media-based scams by reported losses

Scam category	Reported losses	Reports	Reports with loss
Dating & romance scams	$9 317 569	1 357	460 (33.9%)
Investment scams	$3 311 105	368	241 (65.5%)
Unexpected prize & lottery scams	$786 178	562	82 (14.6%)

The category with the highest losses with this contact mode was 'dating and romance scams'. Scammers search for victims on dating websites or through social media platforms such as Facebook, Google Hangouts and Instagram.

Investment scammers also find victims through social media often via advertisements for get-rich-quick schemes and new foolproof trading platforms.

Table 11: Top three social media-based scams by reports

Scam category	Reported losses	Reports	Reports with loss
Online shopping scams	$486 965	1 875	1 412 (75.3%)
Dating & romance scams	$9 317 569	1 357	460 (33.9%)
Unexpected prize & lottery scams	$786 178	562	82 (14.6%)

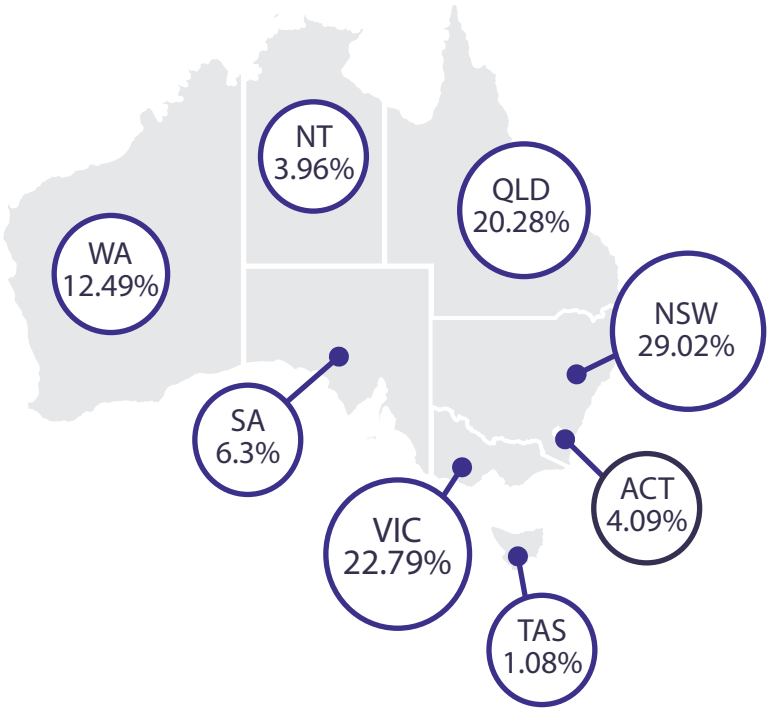
While 'dating and romance' and 'investment' scams are the most financially damaging, the most common scams on social media are 'online shopping scams'. In 2018, there were 1875 reports of Australians identifying scam advertisements and fake pages on social media with reported losses of $486 965. These scams also have a very high conversion rate with 75.3 per cent of reports including a loss. This indicates that people generally report these scams only if they lose money and less so if they simply encounter but scroll past such scams on social media. However it could also mean these scams are harder to identify and more people pay money before they realise it's a scam.

2.4 Who is being scammed

Not every reporter to Scamwatch provides age, gender and location data but those that do provide us with valuable insights about which scams affect different groups in society. Understanding this allows the ACCC and other government agencies to target awareness-raising efforts.

Geography

Figure 5: Percentage of total scam losses by state and territory



The number of reports to Scamwatch broken down by states and territories rank in line with the population of those states and territories. International scammers are not taking aim at any specific region of Australia.

Table 12 provides an overview of state and territory populations[7] mapped against number of reports and total losses reported to Scamwatch.

Table 12: State and territory populations and reported losses[8]

State	% of over 18 Australian population	% of reports made to Scamwatch	% of total reported losses	Reported losses
NSW	32%	30.8%	29%	$26 406 678
Vic	26.1%	23.1%	22.8%	$20 736 575
Qld	19.8%	21.6%	20.3%	$18 452 421
WA	10.3%	10.4%	12.5%	$11 367 443
SA	7.1%	8%	6.3%	$5 737 231
NT	1%	1.2%	4%	$3 701 629
ACT	1.7%	3.1%	4.1%	$3 717 907
Tas	2.1%	2%	1.1%	$980 187

States submitted numbers of reports in keeping with their populations, however Victoria was slightly under represented, and the Australian Capital Territory slightly over represented. Reported losses in the Australian Capital Territory, Northern Territory, Western Australia and Queensland were higher proportionally. Detailed tables in the appendix provide additional insight.

7 Australian Bureau of Statistics, *Australian Demographic Statistics June Quarter 2018*, 20 December 2018, www.abs.gov.au/Population, viewed 14 March 2019.

8 Reports from overseas and unspecified location not included.

In most cases where one state seems disproportionately affected (or not affected) by a particular type of scam, analysis of reports identifies a single or small number of larger losses as the cause. There are few exceptions to this.

One exception is the difference between 'Scratchie scams' affecting Western Australia and South Australia. There were only five reports of 'Scratchie scams' from Western Australia in 2018 and no money was reported lost. In comparison, South Australia, a state with a smaller population than Western Australia, reported 195 'Scratchie scams' with over $18 000 in losses.

The ACCC consulted with the Department of Mines, Industry Regulation and Safety, Western Australia (DMIRS) which runs the WA Scamnet website about why there were so few reports of 'Scratchie scams' from Western Australia. One explanation is that in previous years, DMIRS performed successful mail interceptions that removed envelopes identified as scam related. This both reduced the number of letter-related scams that reached potential victims in Western Australia and also generated media coverage that improved awareness in the community of mail-based scams. There may also be a geographic advantage for Western Australian residents when it comes to mail-based scams because scammers send hundreds or thousands of letters at a time to Australian households, usually from South East Asia, and may find better bulk mail rates when sending to the eastern states and territories.

South Australian reports about 'Scratchie scams' in 2018 seem disproportionately high in number and accounted for about 20 per cent of the total reports for that scam category. For other scam categories, reports from South Australia account for about 8 per cent of the national total. There is no definitive explanation for this difference and the higher report numbers did not result in higher losses. South Australian losses reported for 'Scratchie scams' in 2018 accounted for only 4 per cent of the national total. The ACCC and law enforcement around the country are aware that 'Scratchie scam' letters come in waves with hundreds of households in a given set of postcodes receiving letters in a short period. South Australia's higher report percentage seems to have been pushed up by one such wave. South Australian reports for 'Scratchie scams' increased in later 2018 with 66 per cent of reports submitted between September and December.

A detailed table of reports and losses for each state and territory can be found at appendix 2.

Age

Table 13: Age ranges of those reporting

Age range	Reported loss	Reports	Reports with loss
Under 18	$170 792	1 449 (0.8%)	308 (21.3%)
18–24	$3 194 272	9 366 (5.3%)	2 030 (21.7%)
25–34	$12 567 221	21 714 (12.2%)	3 193 (14.7%)
35–44	$14 304 537	20 597 (11.6%)	2 712 (13.2%)
45–54	$19 260 878	20 032 (11.3%)	2 384 (11.9%)
55–64	$24 886 266	20 212 (11.4%)	2 063 (10.2%)
65 and over	$21 466 193	26 451 (14.9%)	2 056 (7.8%)
N/A	$11 151 292	57 695 (32.5%)	3 094 (5.4%)
Total	**$107 001 451**	**177 516 (100%)**	**17 840 (10%)**

A trend that continues in 2018 from previous years is higher losses suffered by older Australians but higher rates of reports with losses from younger Australians.

Those in older age ranges generally hold more accumulated wealth than those in younger age ranges. This means scams that have the ability to extract large sums of money from victims, such as 'investment' and 'dating and romance' scams, will more significantly affect those with more money to lose.

Table 14: Age ranges against number of reports and Australian population as at 30 June 2018 (excluding under 18s)[9]

Age range	% of population	Population as raw figure	% of reports	Reports received in 2018
18–24	12.2%	2 364 487	7.8%	9 366
25–34	19.3%	3 740 138	18.1%	21 714
35–44	17.1%	3 316 271	17.2%	20 598
45–54	16.5%	3 199 059	16.7%	20 032
55–64	14.9%	2 888 728	16.9%	20 211
65 and over	20.2%	3 915 021	22.1%	26 451

Table 15 shows the top three scams by reported losses by each age group recorded in Scamwatch reports. It shows that younger Australians are more affected by 'online shopping scams' than older Australians and conversely, that 'remote access scams' affect older Australians more than younger Australians. This may be an indication of the difference between younger and older Australians regarding their experience with technology.

9 Australian Bureau of Statistics, *Australian Demographic Statistics June Quarter 2018*, 20 December 2018, www.abs.gov.au/Population, viewed 14 March 2019.

Table 15: Top three scams by reported losses for age ranges

As demonstrated in table 15, 'investment scams' are the most financially devastating for most age groups; only younger Australians, who presumably do not have enough capital to invest, are spared. 'Dating and romance scams' on the other hand appear in the top three scams for all age groups except under 18s.

'Dating and romance'-related losses increased by $4.1 million or 20.1 per cent in 2018. Victims aged 55–64 reported the highest losses at $8.1 million but all age groups from 45–54 up suffered significantly greater financial detriment than those in younger age groups.

According to the experiences reported to Scamwatch in 2018, 'dating and romance' scammers have not changed the stories and excuses they use to scam their victims. However, while the stories and excuses did not change, scammers are always looking for new ways to seek out victims and extract money from them.

DATING AND ROMANCE SCAMS

Scammers take advantage of people looking for love

Scammers create fake online profiles on dating sites or social media

They approach you, gain your trust and profess their love

They promise to visit you but there is always some problem stopping them

They tell you a convincing sob story about why they need to borrow money

But no matter how much you give, they will always ask for more

Victims often suffer a substantial emotional and financial toll

STATISTICS:

Losses: **$24.6 million**

Reports: **3900+**

Over 75% of dating and romance scam losses are reported by women

Reports to Scamwatch in 2018

PROTECT YOURSELF:

Never send money to someone you haven't met in person

Scamwatch received reports of scammers connecting with victims via games on Facebook, and also scammers contacting victims over mobile app games such as Scrabble. Scammers use popular games as a way to introduce themselves instead of approaching victims directly with a friend request out of the blue. This way the introduction may feel more natural.

'Dating and romance' scammers finding victims via other social media platforms also increased in 2018. Reports of scammers contacting victims via Instagram increased by 54 per cent to 245 and losses increased by over 1600 per cent to $565 369. Reports of 'dating and romance scams' via Tinder and Viber also increased. In the case of Tinder, there was a 295 per cent increase in reports to 162 and over $391 000 was reported lost. Viber-related scams were still few in number with 32 reports but this represents an increase of 220 per cent over 2017 reports and more than $213 000 was reported lost.

'Dating and romance' scammers also seem to be exploring new payment options. While bank transfers and money remittance services remain the most common payment method, in 2018, payments via Bitcoin increased by 122 per cent to over $115 400 and iTunes cards increased by almost 740 per cent to over $207 000.

Victim story: 'Dating & romance scam'

Reported loss: $30 000

I was first approached on Instagram by 'Jack' who told me he was a captain in the US Army. He told me he is 45 years old, and is on a peacekeeping mission in Syria. He said he was close to retirement and has a 10 year old son attending the best boarding school in Washington DC.

I fell in love with him and trusted everything he told me. He first asked for money in relation to a precious box containing cash and gold that came into his possession during his mission in Syria. He told me that if he could get the box safely back to the US then he could retire and then come to be with me. He asked for help paying various transport and postage fees to get the box out of Syria because he couldn't access his own money in a war zone.

Last month he asked me for help paying for his vacation which he had to get approved via an application to the United Nations. I paid $5000 but he said he was shot by an ISIS member in his camp and was held up in the hospital. Since he couldn't take his vacation at the approved time he had to pay the $5000 again.

After sending so much money he told me he was finally finishing his mission and would be able to come to me so we could get married. He told me he took a UN jet to Istanbul but he was arrested at the airport and charged with drug trafficking because he picked up the wrong bag. Now he says he's being held by the Turkish police and needs another $3000 to bail him out. He always has a new excuse for needing money.

Gender

Where gender information was provided, women reported more scams than men but suffered lower and fewer losses. Women reported 45.6 per cent of the total losses in 2018 and men reported 53.2 per cent which is an $8.1 million difference.

Table 16: Reports and reported losses by gender

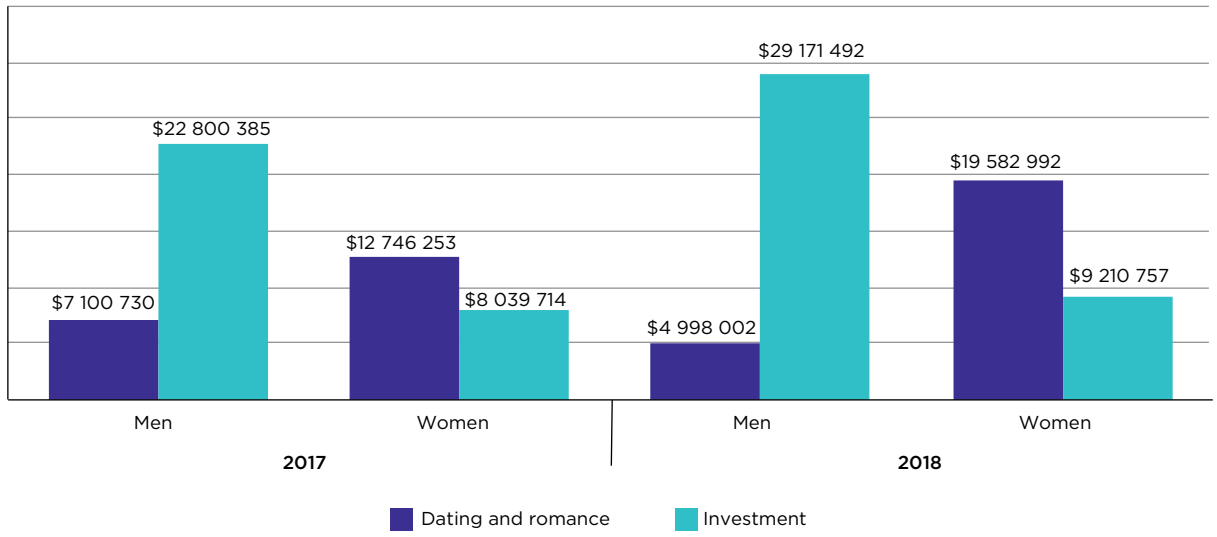
Gender	Reported loss	Reports	Reports with loss
Female	$48 788 396 (45.6%)	94 231 (53.1%)	9 002 (9.6%)
Male	$56 924 335 (53.2%)	79 662 (44.9%)	8 581 (10.8%)
Not specified	$1 288 720 (1.2%)	3 623 (2%)	257 (7.1%)

The disparity in losses between men and women is explained by significant losses by men in 'investment scams'. Men reported over $29.1 million in losses to 'investment scams' and women reported more than $9.2 million. Women on the other hand lost more than men in 'dating and romance scams' with women reporting $19.5 million in losses and men reporting $4.9 million.

The difference in losses suffered by men and women to 'dating and romance scams' and 'investment scams' is a trend that has been observed for a number of years. Reports from 2018 indicate these differences are increasing as can be seen in figure 4. Men reported losing 28 per cent more to 'investment scams' in 2018 versus 2017 but 30 per cent less to 'dating and romance scams'.

In comparison, women reported losing 15 per cent more to 'investment scams' but 54 per cent more to 'dating and romance scams' in 2018.

Figure 4: Difference in losses reported by men and women for 'dating and romance scams' and 'investment scams', 2017 versus 2018



3. Scam trends in 2018

3.1 Investment scams

When combined, 'investment scam'-related losses reported to the ACCC, ACORN and WA Scamnet exceeded $86 million in 2018.

Scamwatch received 3508 reports with a record $38.8 million in losses. This represents an increase in losses of 24 per cent or $7.5 million over 2017 losses. In 2017, losses increased by 33 per cent over the previous year which represented $7.6 million in additional losses compared with 2016.

There does not seem to be any particular new approach adopted by scammers that has caused this increase in losses.

Phone-based cold calling is the most common and most financially devastating approach used by investment scammers to find victims but others report falling for investment schemes mentioned on internet trading forums or advertised in pop-up ads.

While the general approach of investment scammers does not seem to have changed, the specific nature of the offers does change from year to year. In 2018, 'binary options' scams were in decline and 'forex' trading scams increased.

Cryptocurrency in investment scams

In 2017, investment in cryptocurrency grew quickly and dramatically, hitting a fever pitch in the final months of the year. Investors from around the world increased the price of Bitcoin from about $3000 in July 2017 to almost $20 000 in December 2017. Reports to Scamwatch indicate that in the excitement, many would-be investors were actually investing in scams.

Victims reported being tricked by online scammers into purchasing various cryptocurrencies through the scammer's software platform, but, as with other investment scams, when they tried to cash out, the scammers either made excuses or were no longer contactable. These investment scams also included scammers asking for payment in cryptocurrency for forex trading, commodity trading or other investment opportunities. In 2018, victims of 'investment scams' reported losing $2.6 million through payments in cryptocurrencies.

Binary options

Binary options, also known as 'all-or-nothing options', 'fixed return options' or 'digital options', allow you to make bets on financial products, including shares and foreign exchange markets, or economic events. For example, you could bet on whether the share price of a company will be trading above its current price in one hour. Contract times for binary options are usually very short, from a few minutes or hours, to a few months in the future.

Trading binary options appears to be simple, but picking the short-term movements of an underlying asset is extremely difficult, even for professionals. They are high-risk, speculative investments that really just gamble on the movement of an asset price.

In 2018, Scamwatch received 100 reports of binary options scams with reported losses of $2.1 million. This is a reduction from the losses of $3.1 million reported in 2017.

This reduction may be caused in part by action taken by financial regulators internationally in recent years. In 2017 Israeli authorities passed a law banning firms in that country from selling binary options overseas. In 2018 the European Securities and Markets Authority also placed restrictions on the practice to protect consumers. Since 2017 Apple, Facebook and Google have all banned binary options trading advertisements on their platforms, which has surely had an impact on the ability of scammers to attract potential victims online.

Forex trading

While binary options scams seem to be in decline, in 2018 another form of investment scam grew in reports and reported losses.

Foreign exchange (FX or forex) trading is an attempt to make a profit by speculating on the value of one currency compared with another. Exchange rates between currencies are very volatile and fluctuate significantly in short periods of time. Like binary options trading, scammers promote forex investment schemes with online trading platforms that are supposedly easy to learn and can result in huge profits quickly.

In 2018 Scamwatch received over 250 reports about forex trading scams with reported losses of $4.4 million. This is an increase over forex-related reports to Scamwatch in 2017, which numbered 191 reports with $2.8 million in losses.

It is possible that with the restrictions placed upon binary options internationally and the banning of related advertisements on major technology platforms, some binary options scammers have shifted their operations to forex trading. There are similarities in the scammer's approach in both types of scam.

Both binary options and forex trading scammers offer get-rich-quick schemes with 'expert advisers' and 'simple-to-use platforms'. Trading is presented as a simple process that only requires watching basic market trends and timing purchases and sales accordingly. The scammers gather money from victims relatively quickly by offering larger and larger returns for investing more money or upgrading their accounts to 'unlock greater profit-making potential'. In reality the whole online platform is a facade with all the money going to the scammers, and no real trades occur. The platform is geared to make victims think they are making large profits quickly so they invest more.

Victim story: 'Investment scam'

Reported loss: $50 000

I was contacted over the phone by an online trader who specialised in binary options, cryptocurrency and forex trading. He said his company was on the cutting edge and used the latest technology and could offer guaranteed returns. I invested a few thousand and used their online platform which seemed to work very well. I could see my trades were resulting in good profits. I invested more at their insistence and they promised I would earn even more.

When I wanted to withdraw my money I was told I would need to pay taxes on my profits before I could access it. I was never warned about this but they insisted I needed to pay taxes before I could get my money back. After I asked for my money, my trades started to fail and my accumulated profits were starting to decrease. They pressured me to invest more so that I could reverse the situation by increasing my 'trades volume'. They said I would lose everything unless I invested more as an emergency.

I feel very embarrassed by this scam, they were very convincing and professional. They stated I would be 'kicked off the market' because my trades were failing and I was reduced to 3 per cent of my initial investment but by that point I knew it was all fake.

INVESTMENT SCAMS

Scammers trick you into investments that are too good to be true

You discover an investment opportunity online or an 'expert' contacts you out of the blue

They offer a low-risk, high return opportunity using proven techniques

It looks and sounds legitimate with flashy websites and sophisticated looking platforms

You invest a small amount which grows rapidly, they encourage you to invest more and more and even tell all your friends

Once they have your money, you can never get it back

STATISTICS:

Losses:
$38.8 million

Average Loss:
$32 600

75% of investment scam losses are reported by men

Reports to Scamwatch in 2018

PROTECT YOURSELF:

Beware of promises of high returns with little to no risk

Always check with a reputable financial adviser before investing

3.2 Chinese authority scams

In 2018 a unique scam emerged which specifically targeted Mandarin-speaking people in Australia. Victims included Chinese students, recent immigrants and longer term residents of Australia. Mandarin-speaking people without family connections in China were not targets.

These scams involved automated calls in Mandarin, leaving an 'urgent' voice message to call back. The caller either identified themselves as a parcel delivery company or the Chinese authorities, usually 'the embassy'. The caller would state that the victim was in serious trouble with the Chinese authorities. If the call was returned, the scammers impersonated embassy staff, police investigators and prosecutors. Victims were told that someone had been intercepted in China who had in their possession a number of forged documents such as passports and bank cards with the victim's name on them. The victims were told they were implicated in the creation and dissemination of these forged identity documents.

The victims were told that the Chinese authorities had opened a criminal investigation and would need to freeze all the victim's money and property in China. Victims were passed from one fake character to another to give the illusion that a number of officials were working on the case. The victims were threatened with extradition to China to face charges. However, they were told that if they paid a large sum of money, as a sort of secured bond, then their bank accounts would be left unfrozen while the authorities investigated. The scammers told the victims the investigation may seek information from their friends and family in China and they should not talk to anyone about the matter because it may jeopardise the investigation.

An analysis of Scamwatch data for 2018 revealed almost 1820 reports of this scam and over $1.44 million in reported losses. The scam spiked in reports in May and June 2018 with the ACCC receiving six times more reports in those months than in April 2018. In May 2018 there were over 750 reports of these scams with almost half a million dollars in reported losses. Younger females in the 18–24 year old age range reported the largest financial losses and females between the ages of 25 and 34 provided the largest number of reports.

The rapid spike in reports and losses prompted the ACCC to issue a media release in both English and Mandarin to warn people about the scam. The same scam was also reported internationally, prompting announcements from police departments and Chinese embassies in Canada and the USA.

Victim story: Chinese authority scam

Reported loss: $130 000

I received a call from a number that looked local. They claimed they were from the Chinese Embassy and said there were important documents for me to pick up. They gave me a number to call to arrange the pickup. When I called that number, someone [claimed to be] a prosecutor in Beijing.

He told me they intercepted a woman who was travelling with over 100 credit cards and other identity documents and that I was implicated because my name was on the documents. The woman they arrested apparently told them that I sold my identity to her for $230 000. He said that because I was under investigation, all my accounts and any other property in China would be frozen for up to three years.

He asked me a lot of questions about myself and what bank accounts or property I have. I was afraid that I would be arrested upon my return to China and that my relatives in China might also be negatively affected by the investigation. They told me that I would be arrested if I spoke to anyone about the active investigation because I might be trying to tip off accomplices. He made it sound very official and serious so I cooperated and answered all his questions. They told me that my accounts could be frozen for up to three years depending on the scale of the investigation but they told that if I wanted the investigation sped up and continued access to my bank accounts then I would need to transfer $130 000 immediately. They said they would give it back if they found me innocent.

Afterwards I read some information online and realised it was a scam. I tried to get my money back but it was too late. They have all my details and information so they might try something else to harm me still.

3.3 Elaborate remote access scams

In 2018 Scamwatch received over 11 300 reports of 'remote access scams' with $4.7 million in reported losses, an increase of 95 per cent over 2017 losses. Much of this increase can be attributed to a new, more elaborate version of a scam that has been around for years.

Many Australians have received annoying 'tech support' scam calls in which a scammer, claiming to represent Microsoft or Telstra, tells the victim that their computer is 'sending viruses' and this is a serious problem that needs immediate attention. The scammer would ask for remote access to the victim's computer and if granted, they would pretend to fix the imaginary problem, while actually installing malware and searching the computer for personal information that could be used for identity theft.

Thankfully, while Scamwatch still receives reports of this scam, more and more Australians are aware of it and hang up when they receive such calls. However, a new remote access scam has recently emerged with an elaborate set-up that has caught many Australians off guard. The scammer's objective is still to get access to the victim's computer, but the story they tell to achieve that has become more complex.

Scammers now call victims stating that they are the police or Telstra working with the police. They tell victims that their computer has been identified as one already hacked by scammers and used as one of many nodes set up to send out scams and viruses. However, if the victim cooperates by providing remote access to their computer, the police can track the scammers. To do this, the victim is told they must send money to the scammer via online banking because it will allow the police to 'trace the flow of the money' and locate the scammer. The victim is told they will not lose anything because the government will reimburse any money sent.

REMOTE ACCESS SCAMS

Scammers trick you into providing remote access to your computer

A scammer calls you impersonating your phone company, a tech or computer company or the police

They tell you your computer has been compromised by scammers and is being used to scam others

You are convinced to grant the scammers access to your computer

As part of the scam, you are tricked into logging into your bank account

They tell you they can 'trace' the scammers by sending them money but the government will pay it all back to you so there is no risk

Scammers steal money from your online accounts or get you to transfer funds via gift cards. They also gather your personal information for identity theft

STATISTICS:

Losses: **$4.7 million**

Reports: **11 300**

Over 65 year olds reported the highest losses at **$2.2 million**

Reports to Scamwatch in 2018

PROTECT YOURSELF:

Never give unsolicited callers access to your computer

If the victim starts to doubt what they are being told, the scammers re-assure them that they are facing no risk and would be helping an important investigation. Alternatively, they may threaten the victim with legal action for not assisting the police. The scammers sometimes play a number of roles including the police, the scammer who supposedly hacked the victim's computer, 'Telstra' and a representative of the victim's bank. All these characters back up the story told to the victim and convince them they are in the middle of an important police operation.

In many cases, victims are asked to purchase gift cards such as iTunes or Google Play cards as part of the scam. The scammers install software on the victim's computer that allows them to enter gift card serial numbers. This system is also explained as a method of catching the scammer but is just another method of extracting money from the victim.

Victim story: 'Remote access scam'

Reported loss: $30 000

A scammer called my elderly mother at her home claiming to be from Telstra technical support. They told her there are scammers trying to access her computer and that a lot of pensioners are being targeted in her area. Apparently people were being hacked and losing money and they asked if she would like to help other pensioners by tracking the flow of money via iTunes cards so they could nab the scammers.

Then the scammers gave her instructions over the phone to give them remote access to her computer. They asked her to purchase $15 000 worth of iTunes cards at different times and from different stores in the area. After she got home they got her to log the iTunes card numbers into an app they installed on her computer and to destroy the cards afterwards. They promised this was helping catch scammers and asked her to buy more and more cards.

They continued to ring my mum and pressure her to give more money and managed to get her to give them about $15 000 more. She still has a pile of cut-up iTunes cards and has lost almost $30 000.

3.4 Scams and cryptocurrencies in 2018

In 2018, reports to Scamwatch where cryptocurrencies were used to pay the scammer numbered 674 with reported losses of $6.1 million. This is a 190 per cent increase over the $2.1 million reported in 2017. The scam category with the highest reported losses to cryptocurrencies was 'investment scams' with $2.6 million in reported losses.

Scamwatch has also received reports from victims of various types of scams being directed by a scammer to the nearest Bitcoin automatic teller machine to convert money to Bitcoin and then transfer it to the scammer.

Almost 50 per cent of the losses reported where cryptocurrency was the payment method were men in the 25–34 age group. As would be expected for an online phenomenon, 80 per cent of reports involving cryptocurrency identified an online mode of communication ('internet', 'social networking/online forums' or 'email') as the method by which the scammer and victim made contact.

UNUSUAL PAYMENT METHODS

The government or legitimate businesses will never ask for payment via gift cards or cryptocurrencies

PROTECT YOURSELF:

No legitimate business or government agency will ask for payment via unusual methods

Scammers ask for payment via various gift cards such as iTunes or Google Play cards...

money remitters like Western Union...

or virtual currency such as Bitcoin

Transfers occur instantly and are not subject to security and banking systems

Gift card numbers are then sold on the black market and turned into money

You can't get your money back once it's been sent

STATISTICS:

Losses:
$19 million
reported lost via unusual payment methods

$6.1 million lost via cryptocurrenicies

$4.3 million lost via gift cards

$8.6 million lost via money remittance services

Reports to Scamwatch in 2018

BEWARE OF:

Being pressured into buying gift cards or transferring money through Bitcoin ATMs

Government or businesses demanding money by unusual payment methods

Victim story: 'Jobs & employment scam' via cryptocurrency

Reported loss: $1200

I applied for a job I saw advertised online for an 'assistant manager' for an international business operating online. It was supposed to be a probation period of 30 days with a salary of $2200.

I filled out an employment agreement which I realise now was just a way to get all my personal information. I had a number of Skype chats about the business and my role and they gave me three initial tasks. One of these tasks was to receive funds into my bank account and deposit it to 'investors' via a Bitcoin ATM in the city.

I did this a number of times and transferred thousands of dollars to them. Eventually my bank contacted me claiming I was involved in a fraud and that my accounts will be blocked pending an investigation.

I'm cooperating with the bank and hope to get my accounts unlocked and my name cleared. It's clear to me now that this was just a money laundering scheme and I fell for it.

The above victim story is an example of money laundering which is a criminal offence and can lead to imprisonment. Scammers and criminal groups use money laundering to hide the proceeds of a range of serious criminal activity.

3.5 Gift cards as a payment method

In the past, scammers usually extracted money from their victims via bank transfers, money remittance services or by obtaining credit card details. However, in more recent years, scammers have been asking for money via a range of unusual payment methods. These include cryptocurrencies such as Bitcoin but also Apple iTunes cards, Google Play cards and other gift cards.

In the case of gift cards, scammers ask victims, often frightened by threats of arrest or deportation, to go to a local shop and buy hundreds or even thousands of dollars' worth of cards. The victim then reads the codes on the back of the cards to the scammer over the phone. The scammer can then sell them at a reduced price on the black market or use the cards directly to make purchases on the iStore, such as in-app purchases or applications. The developer of the application receives 70 per cent of the payment made in such purchases.

An analysis of Scamwatch data revealed that in 2018, total reported losses via gift cards exceeded $4.3 million from almost 1500 reports. iTunes cards accounted for 72 per cent of these losses or $3.1 million, an increase from the $1.2 million reported in 2017. While iTunes cards are the most common card requested by scammers, Scamwatch has received reports of Steam cards, Amazon cards and a range of other gift cards being requested.

In the latter months of 2018, reports to Scamwatch of Google Play cards used in scams started to increase, mostly in relation to ATO impersonation scams. While still relatively few, reports to Scamwatch with Google Play cards as the payment method increased from just three in July to 66 in December 2018. Losses also increased from $1250 in July to over $179 000 in December. Scams reported to the ATO indicated that iTunes cards were identified as the payment method in 252 reports and Google Play cards in 214 reports. Despite more reports of iTunes cards being used in scams, there were greater losses via Google Play cards. According to ATO data, related losses by iTunes cards exceeded $490 000 while payments made to scammers by Google Play cards exceeded $647 000.

This increase in the use of Google Play cards indicates a shift away from iTunes cards as the preferred method of scam payment. This is most likely due to concerted efforts of Australian government departments including the ACCC and ATO to encourage major Australian retailers to display warnings about the use of iTunes cards in scams. Over the past few years, thousands of supermarkets and department stores have introduced point-of-sale warnings about scammers asking victims to pay via iTunes cards.

GOVERNMENT IMPERSONATION SCAMS

Scammers threaten you with arrest or legal action for money they claim you owe

Scammers call you impersonating a government department

They tell you that you must pay a fee or fine to resolve a tax debt, speeding fine, unpaid bill or overpayment of benefits

They threaten you with arrest, loss of benefits or legal action if you do not comply immediately

They often ask for payment via unusual methods like gift cards or cryptocurrency

Once you pay they make up reasons why you need to pay more

STATISTICS:

The most commonly impersonated department in 2018 was the **Australian Taxation Office** with:

Over:
$4.2 million
reported lost

Over:
137 000
reports

Combined reports to Scamwatch and the ATO in 2018

PROTECT YOURSELF:

Hang up on anyone threatening you with immediate arrest, loss of benefits or deportation

3.6 The automation of scams in 2018

In 2018, the ACCC noticed an increase of scammers employing automation in telephone communications by making tens of thousands of phone calls but leaving voice messages asking potential victims to call back. The ATO impersonation scam and Chinese authority scams are examples of scams that employed this approach.

The traditional version of this type of scam involves scammers making a large number of phone calls, one after another and attempting to scam each person who answers. Many Australians hang up on these scammers because they are aware of such scams. This means that a scammer may call many people before finding someone who is willing to engage in a conversation which may lead to them transferring money to the scammer. The resource cost of this approach is high because the scammers spend a lot of time making individual calls and attempting to convince each person to send money.

In comparison, the automated approach uses technology to make many thousands of phone calls at once and leaves a message. The message makes the opening argument on behalf of the scammer. In the case of the ATO impersonation scam, the message states the recipient owes the government taxes and must call back or face serious penalties. The scammer is then able to wait for phone calls from potential victims. Those who are already aware this is a scam will not call back and those who do call back are assumedly unaware and a better target for the scammers. This approach has a much lower up-front resource cost for the scammers and it allows them to increase the volume of calls they make.

While the chance of tricking a victim into parting with their money is reduced according to the statistics, the increased numbers of calls can result in more money for the scammers because they have contacted so many more potential victims.

A key characteristic of these automated calls in 2018 was the short-term 'campaign' nature of the sudden peak in calls and then a drop off back to previous levels. The below charts show two of the most prominent examples of this in 2018 which occurred in May 2018 with the Chinese authority scam and in November 2018 with the ATO impersonation scam.

Figure 6: Chinese authority scams reported to the ACCC in 2018

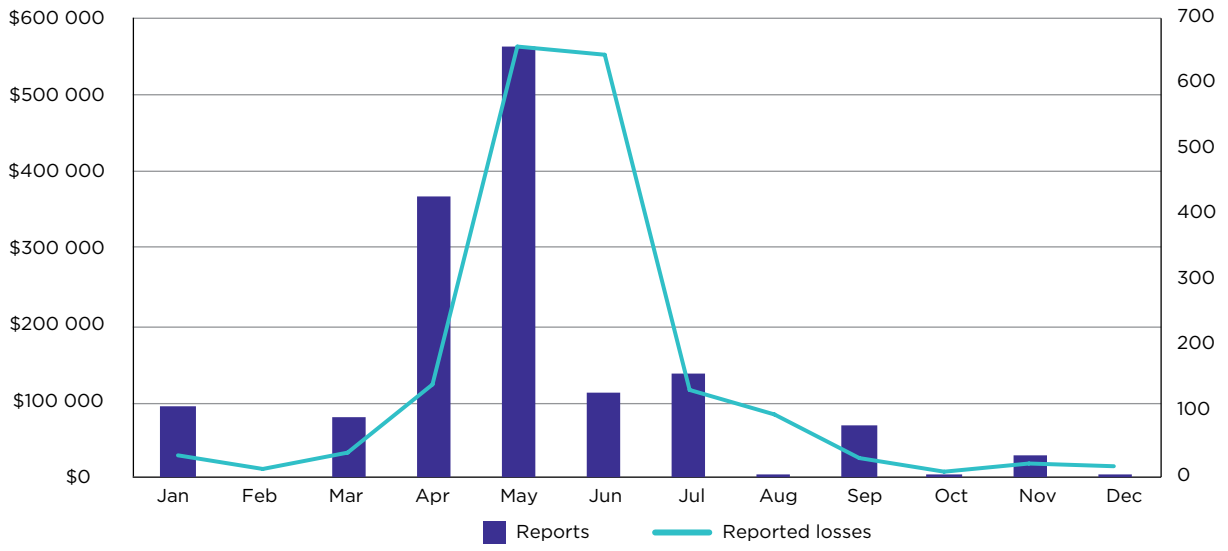
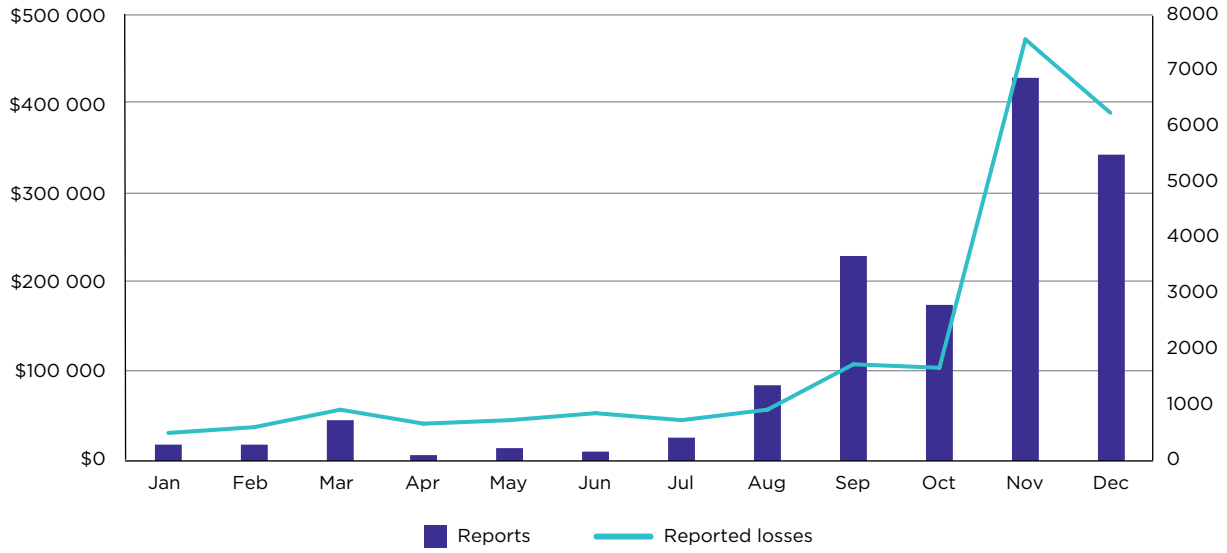


Figure 7: ATO impersonation scams reported to the ACCC in 2018



In the above examples scammers launched what could effectively be called dedicated phone scam campaigns. These present a unique challenge to Scamwatch and Australian authorities because the calls increase in volume very quickly and can quickly cause serious financial harm before authorities are aware and able to issue appropriate warnings to the public.

In the case of ATO impersonation scams, the ATO and a number of other Australian government and law enforcement agencies regularly spread warning messages via social media and traditional media, including updates to the scam alerts web page. The ACCC's Deputy Chair, Delia Rickard, engaged in a number of media interviews to warn Australians about the huge volume of these scams.

In the case of Chinese authority scams, the Australian Federal Police and Chinese Embassy in Australia issued warnings, and the ACCC issued a media release in both English and Mandarin warning potential victims of the scam and issued further warnings during media engagements.

While these warnings undoubtedly helped to reduce harm in the community, it is not clear whether the scammers always planned a dedicated campaign that would have run for a set time. The ACCC, other government agencies and law enforcement work as quickly as possible to issue warnings about emerging scam trends. This requires constant vigilance and, unfortunately, many people receive the warnings too late.

Victim story: ATO impersonation scam

I received a voice message asking me to contact the ATO due to an outstanding tax bill. When I phoned back, I said I had no idea that it was due. They asked me to give them the name of my accountant, which I did. The scammer then initiated a conference call with [a second scammer] who seemed to be another accountant in the firm. They said that they had made a mistake on their end and suggested I pay the outstanding amount, advising they would reimburse the funds to me on Monday. He also warned me not to pay with Visa or MasterCard as it would reflect badly on my credit history.

When speaking to the officer at the 'ATO' he told me not to hang up the phone until the transaction was finalised. He told me in very strict instructions to go to the bank and get the cash out and to pay with 'currency' of Google Play cards. I did what he asked and took photos of the back of the cards. He then went on to tell me that I had four counts of tax evasion, fraud and two others and to clear my name with the AFP, I would have to pay $5000 for each case to be dropped. That's when I became suspicious and I messaged my accountant while still on the phone to the 'ATO'.

My accountant called me and told me to get off the phone straight away. I feel like such an idiot being fooled. As a 31 year old businesswoman, I'm usually a good judge of these things. The pressure of getting on top of all your taxes, payroll tax and BAS is enough and I fell vulnerable to someone who got me at a bad time.

4. Scams reported by businesses

In 2018 those reporting to Scamwatch on behalf of a business reported 5846 scams with $7.2 million in losses. This is an 8 per cent increase in reports and 58 per cent increase in losses. The increase in losses in 2018 for businesses is largely explained by business email compromise scams reported to Scamwatch as 'false billing' or 'hacking' scams.

Reports to Scamwatch indicated that $3.8 million was lost to business email compromise scams, but, when combined with losses reported to ACORN, Australian businesses are seen to have suffered losses of over $60 million to these scams.

The prevalence of this scam in 2018 is reflected in the comparatively large number of 'false billing' scams, due in part to hackers gaining access to the mass emailing systems used by businesses to send marketing emails or invoices to customers. Hackers used these systems to send large numbers of fake invoices from the businesses' real email accounts but provided the scammers' payment details instead of the businesses'.

There were also a number of reports of 'investment scams' suffered by those reporting on behalf of a business with losses of $2.1 million. A number of these reports describe offers from scammers to invest in other businesses, property, gold and even Syrian oil.

Table 17 provides an overview of the top scams that targeted businesses in 2018.

Table 17: Overview of top scams targeted at businesses

Scam category	Reported losses	Reports	Reports with losses
False billing	$3 144 085	1 819	170 (9.3%)
Investment scams	$2 152 309	59	16 (27.1%)
Hacking	$807 364	304	24 (7.9%)
Phishing	$241 911	637	13 (2%)
Classified scams	$211 127	153	41 (26.8%)

Since nine in 10 businesses in Australia are small businesses, the bulk of our scam reports submitted by businesses were from this cohort as shown in table 18.

Table 18: Breakdown of scams by business size (where size information is provided)

Business size	Reported loss	Reports	Reports with loss
Micro (0–4 staff)	$1 920 514	1 826	206 (11.3%)
Small (5–19 staff)	$2 595 172	1 574	143 (9.1%)
Medium (20–199 staff)	$1 827 673	835	79 (9.5%)
Large (Over 200 staff)	$645 325	311	27 (8.7%)
Total	**$6 988 684**	**4 546**	**455 (10%)**

4.1 Business email compromise scams

The most financially harmful scam affecting Australian businesses is the 'business email compromise' scam. Combined reports to the ACCC and ACORN indicate $60 million in losses reported by Australian businesses in 2018.

Scamwatch recorded over $3.8 million in reported losses to business email compromise scams and ACORN recorded over $56.3 million in reported losses.[10]

This is a global problem. The United States Federal Bureau of Investigation estimates global losses of US$12.5 billion to business email compromise scams between 2013 and May 2018.

The scam involves a scammer gaining access to a business's entire email or IT systems or at least the email account of a key person in a business who deals with the transfer and receipt of money. Scammers evidently trawl the internet for the details of chief financial officers, accountants, payroll officers and even the treasurers of small community sports clubs to target. It is believed that scammers either hack their way into the email accounts or use information gathered in phishing scams to log in.

There are two broad variants of what scammers do once they gain access to the organisation's email systems.

In the first scenario, the scammer impersonates the chief financial officer or some other high-ranking manager of the business and asks for funds to be transferred into an account for a variety of reasons. A common reason is the manager travelling overseas and needing funds because of some unforeseen emergency. The urgency expressed in the email can catch junior staff off guard, meaning they react quickly by transferring funds.

The second scenario involves the scammer impersonating the business in an email to another business, such as a supplier, asking for a regularly paid invoice to be paid into a new account. Scamwatch receives reports from both sides of this scenario—the business impersonated and the business scammed into paying into the wrong account.

The payroll areas of a business may also be targeted by scammers impersonating employees asking for upcoming pay to be paid into a different account.

Business email compromise in the real estate sector

There were a number of reports in 2018 indicating business email compromise scammers specifically targeting real estate deals. In these cases, the victims are usually consumers engaging with a real estate agency to buy a property. The scammer hacks the real estate agency's email systems and sends an email advising of a change to the bank account into which the deposit for the property should be sent. The customer pays the scammer's account and, for many victims, this means losing both a large sum of money and the ability to purchase the property at all. The real estate sector is particularly attractive for scammers because of these large lump sum transfers between parties without a history of previous interaction.

10 More businesses report business email compromise scams to ACORN than to Scamwatch because a report to ACORN is a method of reporting cybercrime to the police whereas reports to Scamwatch are used for scam awareness-raising and prevention initiatives.

BUSINESS EMAIL COMPROMISE

Scammers trick you into changing payment details to divert money

Scammers hack your email and IT systems

They observe transactions and identify opportunities to divert money to their own accounts

They impersonate the intended recipient of a payment or your own CEO. Real estate deals are also commonly targeted

They send emails advising changes to payment details. The emails appear legitimate because they are sent using your own email system, or are convincing spoofs

You update the payment details accordingly and pay the scammer instead of who you mean to pay

You may not realise you paid a scammer until the intended recipient complains they never received the payment

STATISTICS:

Losses:
$60 million
(Reported to Scamwatch and ACORN)

170% increase in losses over previous year

According to the FBI, global losses to BEC scams between 2013 and 2018 = **US$12.5 billion**

Reports to Scamwatch in 2018

PROTECT YOURSELF:

Beware of emails requesting changes to payment details

Operation WireWire

In July 2018 the FBI, in partnership with international law enforcement agencies, announced a major coordinated effort to disrupt international BEC scams, called Operation WireWire[11]. The operation involved a six-month sweep that culminated in over two weeks of intensified law enforcement activity resulting in 74 arrests in the USA, Nigeria, Canada, Mauritius and Poland. The operation also resulted in the seizure of nearly US$2.4 million and the disruption and recovery of approximately US$14 million in fraudulent wire transfers.

Victim story: Business email compromise

Reported loss: $190 000

We are the victims of an email hacking scam. The scammers appear to have hacked a supplier's email and advised us of a change in bank details.

The scammers sent us invoices with amended bank details as well as the prior email trail to and from the supplier so they must have been in their IT system.

Everything was a perfect copy of a real version of the invoices we were so used to. We didn't notice the difference.

Thinking it was real we sent an amount of $190 000 but the real supplier never received it.

The email address was also correct for the supplier, but they told us that they did not receive our responses. The scammers seem to have some way of hiding our responses from the supplier.

We didn't find out about this until our supplier contacted us via phone to talk about not receiving the money.

11 www.fbi.gov/news/stories/international-bec-takedown-061118.

5. Scams reported by Indigenous consumers

5.1 Scam trends

In 2018, those identifying as Indigenous consumers reported 2434 scams with just over $3 million in losses. This is an increase of 34 per cent in reports and 79 per cent in reported losses. A review of these reports does not indicate specific targeting of Indigenous consumers by scammers.

As with the broader population, those people identifying as Indigenous reported the highest losses to 'investment scams' and 'dating and romance scams'.

Table 19: Top five scams by reported loss by Indigenous consumers

Scam category	Reported losses	Reports	Reports with loss
Investment scams	$1 198 961	62	30 (48.4%)
Dating & romance scams	$905 399	128	39 (30.5%)
Classified scams	$94 627	77	20 (26%)
Phishing	$68 871	237	8 (3.4%)
False billing	$65 759	155	31 (20%)

The age demographics for reports from Indigenous consumers largely follow the trends of the larger population. As with the larger population, the 55–64 age range reported the highest losses at $1.4 million. Unlike the larger population, the percentage of scam reports from younger Indigenous consumers was higher.

Table 20: Breakdown of age ranges in reports from Indigenous consumers

Age range	Reported losses	Reports	Reports with loss
Under 18	$6240	51 (2.1%)	12 (3%)
18–24	$27 779	254 (10.4%)	46 (11.5%)
25–34	$87 179	501 (20.6%)	82 (20.5%)
35–44	$410 741	430 (17.7%)	81 (20.3%)
45–54	$352 562	363 (14.9%)	66 (16.5%)
55–64	$1 443 890	250 (10.3%)	49 (12.3%)
65 and over	$649 703	155 (6.4%)	22 (5.5%)
N/A	$28 901	430 (17.7%)	42 (10.5%)
Total	**$3 006 995**	**2 434 (100%)**	**400 (100%)**

Contact methods reported by those identifying as Indigenous consumers differ slightly from the trends of the larger population. Instead of phone-based scams, email-based scams were the highest in number and reported losses and 'social networking/online forums'-based scams accounted for 9 per cent of the total reports compared with 4 per cent in the larger population.

Table 21: Contact methods in reports from Indigenous consumers

Contact mode	Reported losses	Reports	Reports with loss	Percentage of Indigenous reports
Email	$1 591 864	564	85 (15.1%)	23.2%
Social networking/online forums	$698 368	225	91 (40.4%)	9.3%
Internet	$214 011	247	112 (45.3%)	10.2%
Phone	$210 056	878	31 (3.5%)	36.1%
Mobile apps	$112 637	56	19 (33.9%)	2.3%
In person	$106 449	59	22 (37.3%)	2.4%
Text message	$62 627	319	28 (8.8%)	13.1%
Mail	$10 973	75	11 (14.7%)	3.1%
Fax	$10	6	1 (16.7%)	0.2%
Total	**$3 006 995**	**2 429**	**400 (16.5%)**	**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. This project continued in 2018.

To engage effectively, the office identified nine Indigenous communities as scam hotspots by analysing international financial transactions being sent from these communities to countries of concern overseas. These are countries that do not seem to present any familial or other link to members of those communities and which are known hotspots for scam activity.

Tailored workshops were then held in these communities to raise awareness of scams to help reduce their impact. Staff travelled to communities across the Northern Territory to deliver a range of tailored programs related to scams. Information about scams was also delivered via social media, poster and outreach in urban centres.

The programs are designed to raise awareness, empower and support Aboriginal and Torres Strait Islander peoples through education and training to create positive changes to their lives and in their communities.

5.3 National Indigenous Consumer Strategy

The ACCC is the current Chair of the National Indigenous Consumer Strategy (NICS), which comprises representatives of Australian consumer protection agencies as well as several independent members, including the Indigenous Consumer Assistance Network (ICAN). NICS focuses its efforts in a collaborative manner in order to improve consumer outcomes for Indigenous Australians. NICS manages an annual project with a specific focus on a contemporary consumer issue nominated by and impacting upon Indigenous Australians.

'Too good to be true' is the NICS project for the 2018–19 financial year and aims to raise awareness of scams impacting Indigenous Australians. The project team reached out to Indigenous communities through face-to-face discussions and also raised awareness about how to report scams by distributing fridge magnets with relevant agency names and contact numbers.

Some of the communities visited by the ACCC as part of this initiative include Wujal Wujal, Yarrabah and Palm Island in North Queensland, and Belyuen and Palmerston Indigenous Village in the Northern Territory.

State and territory consumer protection agencies were also actively engaging with Indigenous consumers in 2018 to raise scams awareness. One example of this is South Australia Consumer and Business Services undertaking outreach visits to Port Augusta in addition to liaison work with Indigenous advocacy agencies. These included Money Mob, Aboriginal Legal Rights Movement and Pika Wiya Health Service.

Victim story: 'Dating & romance scam' report from an Indigenous consumer

Reported loss: $27 000

This person contacted me on Twitter with a very friendly hello. We started chatting and discussed a lot about our families and lives. He started throwing romantic messages at me and after three weeks he hooked me romantically.

Then he started asking for money for water because he was working on an oil rig and he told me the workers needed water. He was talking to me daily about the various activities on the oil rig. About three months in, he told me a crane broke down and he needed another $10 000 to repair it and then he needed $9000 for technicians to fly in from Scotland to repair the crane. I sent that money too.

He then asked me for airfare and for hotel money. He told me he deposited a huge sum from his work on the oil rig but to move it, he needed more money from me first. He told me he needed money to pay his workers. Even after I worked out this was a scam and stopped talking to him, he came back six weeks later trying again. He really took me to the cleaners.

6. Scam disruption

6.1 Scam intermediaries project

In 2018 the ACCC engaged with a range of private sector 'intermediaries' whose businesses are commonly used in the course of scams. Intermediaries included social media and online platforms where scammers connect with potential victims and financial services through which money is sent to scammers. These included Australia's four major banks (ANZ, Commonwealth, NAB and Westpac), money remitters, and online classified sites. The ACCC recognised that these intermediaries are in a unique position to identify and intervene in scams using their facilities. For example, the point of transferring funds to a scammer is a key point of potential intervention. These businesses actively take steps to reduce the ability of scammers and fraudsters to use their systems in an effort to protect their customers.

The ACCC first engaged with the intermediaries to better understand their systems and to work with them to reduce the harm caused by scams. The ACCC then established a system by which scam reporters can give permission for their report to be shared with a relevant intermediary, which allowed the ACCC to provide the intermediaries with specific and actionable intelligence.

The ACCC sent scam reports (where the reporter gave permission) to financial intermediaries which were used to inform their internal fraud teams about trending scams. The provision of these reports will now be automated, including via the Australian Financial Crimes Exchange (AFCX), which is an industry-led initiative to coordinate responses to financial crime and cybercrime.

Feedback from the project participants confirmed that these reports improved their scam prevention efforts. In some cases, financial institutions were able to recover funds and block scam transfers for customers. Dozens of domestic and international bank accounts have also been blacklisted as a result of scam reports provided by the ACCC, which significantly disrupts the ability of scammers to extract money from victims. Scam reports from the ACCC have also been used to create 'red flags' that alert the intermediary to suspicious transactions before funds are sent to a scammer. Hundreds of frontline staff at bank branches are also being informed about scams so they can better identify the signs that customers are being manipulated by scammers, and dedicated scam teams have been established to tackle this important challenge.

6.2 Scam technology project

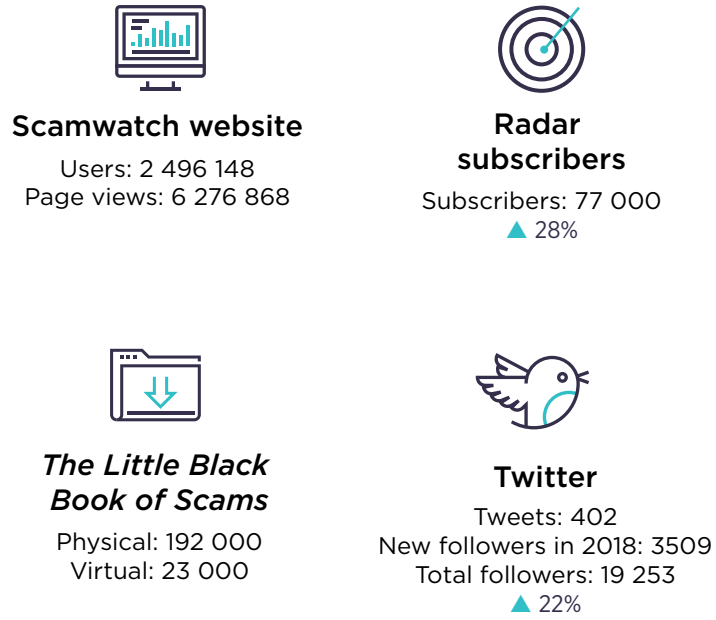
The Australian Communications and Media Authority (ACMA) recently commenced a project to explore practical technical solutions to address the proliferation of scams over Australian telecommunication networks. The project is assisted by a reference group with representatives from the ACCC and the Australian Cyber Security Centre. The project will engage with the telecommunications industry to seek their expertise and experience and will investigate what can be done to disrupt scam communications activity, including possible consumer or network-based solutions like call blocking and network traffic authentication protocols.

The project was initiated as a response to concerns by government and regulators such as the ACCC as well as ACMA research which found that more than half of Australian adults have received scam calls daily or weekly and that three-quarters of Australian adults believe that not enough is done to protect individuals from scam calls.

7. Education and engagement

Due to the international nature of scams and the jurisdictional and enforcement challenges in bringing scammers to justice, the main tool to reduce the impact of scams on 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.gov.au website and its resources, such as *The Little Black Book of Scams*, as well as our ongoing engagement with government and private organisations. Awareness raising on social media platforms and through interviews with traditional media also helps spread the warnings about new and emerging scams.

Figure 6: Education and engagement



In 2018 the Scamwatch website received over 6.2 million page views, an increase over 2017's 4.8 million 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 almost 23 000 times. It is also highly sought after in physical form for distribution by community groups, financial institutions and government organisations with over 192 000 copies sent around the country in 2018.

The Scamwatch radar email subscription service grew in subscribers from 60 000 at the end of 2017 to over 77 000 at the end of 2018. Fifteen radar alerts were sent to subscribers informing them of trending scams and how to avoid them throughout the year.

ACCC and Scamwatch media releases throughout 2018 generated hundreds of media requests for information and for interviews that resulted in hundreds of radio, newspaper and television appearances. These interviews were broadcast both locally and nationally and reached millions of Australians.

The Scamwatch Twitter account also grew in subscribers by 22 per cent to 19 253 followers. The account posted 402 tweets and retweets alerting Australians to current scams and other scam-related information in 2018.

To ensure Australia's linguistically diverse population has greater access to 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.

7.1 Western Union remission scheme

In January 2018, as a result of legal action by the United States Department of Justice, the international money remittance service Western Union admitted to criminal violations including wilfully failing to maintain an effective anti-money laundering program and aiding and abetting wire fraud. Western Union entered into agreements with the DOJ in which it agreed to forfeit US$586 million. The money forfeited was made available to claimants who suffered financial losses in scams and other frauds via Western Union money transfers.

In response to this, the ACCC encouraged Australian scam victims who lost money via Western Union to submit refund claims to try to get their money back. The ACCC utilised Scamwatch reports to identify Australian scam victims who sent money to scammers via Western Union and emailed them to inform them about the remission scheme. The ACCC also updated Australians about the extension for the remission scheme.

7.2 Engagement

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 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.

7.3 Scams Awareness Network

The Scams Awareness Network, formerly the Australasian Consumer Fraud Taskforce (ACFT), is made up of 40 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 Scams Awareness Network. The ACCC also provides secretariat services to the Scams Awareness Network. Each month, the network members share scams intelligence, research, and upcoming awareness campaigns. The Scams Awareness Network delivers a coordinated awareness campaign for consumers, Scams Awareness Week, each year, which also involves private sector and community partners.

On 7 April 2018, the Scamwatch portal was updated to include an option for users to give their specific permission to share their report with other government agencies as part of their 'enforcement, intelligence gathering or scam prevention strategies'. Since then, the ACCC has shared Scamwatch reports (where permission given) with 13 of the Scams Awareness Network member agencies, including law enforcement. Direct access to scam reports about government agencies' areas of interest allows agencies to better target their awareness raising or investigate and disrupt scams.

The ACCC as Chair of the Scams Awareness Network welcomed several new members to the organisation, which seeks to coordinate efforts to inform the Australian public about scams.

7.4 Scams Awareness Week 2018

Every year the Scams Awareness Network collaborates on Scams Awareness Week.[12] The aim of the week is to promote scams awareness about a particular theme to help the Australian public recognise threats and avoid victimisation. In 2018, the Scams Awareness Week slogan was 'Stop and check: is this for real?' and the week ran from 21–25 May 2018, focusing on threat-based impersonation scams. In addition to the Scams Awareness Network member agencies, 47 government and industry partners participated in raising awareness about this ongoing threat throughout the week.

In threat-based impersonation scams, scammers impersonate government agencies, well-known companies or law enforcement and threaten victims with arrest, deportation or the cutting off of a service unless a fee is paid. The campaign asked Australians to 'Stop and check: is this for real?' when presented with such threats and not allow scammers to frighten them into parting with their money.

The ACCC and Scams Awareness Network partners spread warnings and awareness-raising information about threat-based impersonation scams during the week through social media, traditional media and in internal communications to staff.

The campaign attracted significant media attention and resulted in the publication of articles, and broadcast of radio and television segments that helped spread the message to an audience of millions.

7.5 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.

12 Previously named 'National Consumer Fraud Week'.

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 61 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.

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

Overview of scam categories reported to the ACCC in 2018 by reported loss

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
Investment scams	$38 846 635	3 508	1 189 (33.9%)	▲24%
Dating & romance scams	$24 648 024	3 981	1 257 (31.6%)	▲20.1%
False billing	$5 512 502	10 996	1 241 (11.3%)	▲97.1%
Remote access scams	$4 762 429	11 344	881 (7.8%)	▲95%
Threats to life, arrest or other	$3 338 986	19 455	344 (1.8%)	▲45.1%
Online shopping scams	$3 278 776	9 691	5 567 (57.4%)	▲137.5%
Hacking	$3 128 908	8 625	502 (5.8%)	▲83.3%
Unexpected prize & lottery scams	$2 745 700	10 049	338 (3.4%)	▲66.9%
Betting & sports investment scams	$2 629 503	273	101 (37%)	▲50.3%
Classified scams	$2 364 745	4 970	1 173 (23.6%)	▲117.2%
Inheritance scams	$2 172 157	2 828	86 (3%)	▼-21.6%
Jobs & employment scams	$1 525 168	2 841	349 (12.3%)	▲6.7%
Identity theft	$1 472 388	12 800	445 (3.5%)	▲44.6%
Nigerian scams	$1 379 285	878	162 (18.5%)	▼-17.2%
Phishing	$933 470	24 291	357 (1.5%)	▲15.2%
Overpayment scams	$740 279	1 928	401 (20.8%)	▲105.8%
Up-front payment & advance fee frauds	$622 802	1 511	289 (19.1%)	▼-85%
Pyramid Schemes	$607 030	324	85 (26.2%)	▲67.1%
Rebate scams	$598 224	3 804	94 (2.5%)	▼-14.2%
Scratchie scams	$471 028	1 006	43 (4.3%)	▲5.1%
Health & medical products	$274 814	1 038	249 (24%)	▼-47.5%
Fake charity scams	$211 165	941	130 (13.8%)	▼-32.7%
Psychic & clairvoyant	$191 734	194	78 (40.2%)	▲8%
Travel prize scams	$151 782	1 016	59 (5.8%)	▲82%
Ransomware & malware	$151 195	4 356	92 (2.1%)	▼-36.8%
Mobile premium services	$84 584	1 942	297 (15.3%)	▲73.2%
Other/old categories	$4 158 138	32 926	2 031 (6.2%)	N/A
Total	**$107 001 451**	**177 516**	**17 840 (10%)**	**▲17.7%**

Overview of scam categories reported to the ACCC in 2018 by reports

Scam category	Reports	Reported losses	Reports with loss	Change in reports since 2017
Phishing	24 291	$933 470	357 (1.5%)	▼–7.9%
Threats to life, arrest or other	19 455	$3 338 986	344 (1.8%)	▲134.5%
Identity theft	12 800	$1 472 388	445 (3.5%)	▼–18.5%
Remote access scams	11 344	$4 762 429	881 (7.8%)	▲30.6%
False billing	10 996	$5 512 502	1 241 (11.3%)	▼–18.3%
Unexpected prize & lottery scams	10 049	$2 745 700	338 (3.4%)	▼–21%
Online shopping scams	9 691	$3 278 776	5 567 (57.4%)	▲42.5%
Hacking	8 625	$3 128 908	502 (5.8%)	▲49.8%
Classified scams	4 970	$2 364 745	1 173 (23.6%)	▲82.1%
Ransomware & malware	4 356	$151 195	92 (2.1%)	▼–1.3%
Dating & romance scams	3 981	$24 648 024	1 257 (31.6%)	▲5.8%
Rebate scams	3 804	$598 224	94 (2.5%)	▼–59.2%
Investment scams	3 508	$38 846 635	1 189 (33.9%)	▲75.7%
Jobs & employment scams	2 841	$1 525 168	349 (12.3%)	▲10.7%
Inheritance scams	2 828	$2 172 157	86 (3%)	▼–1.6%
Mobile premium services	1 942	$84 584	297 (15.3%)	▲5.1%
Overpayment scams	1 928	$740 279	401 (20.8%)	▲6.2%
Up–front payment & advance fee frauds	1 511	$622 802	289 (19.1%)	▼–82.4%
Health & medical products	1 038	$274 814	249 (24%)	▼–2.7%
Travel prize scams	1 016	$151 782	59 (5.8%)	▼–41.5%
Scratchie scams	1 006	$471 028	43 (4.3%)	▼–24.4%
Fake charity scams	941	$211 165	130 (13.8%)	▼–17.9%
Nigerian scams	878	$1 379 285	162 (18.5%)	▼–31.8%
Pyramid Schemes	324	$607 030	85 (26.2%)	▼–0.3%
Betting & sports investment scams	273	$2 629 503	101 (37%)	▲10.5%
Psychic & clairvoyant	194	$191 734	78 (40.2%)	▼–18.1%
Other/old categories	32 926	$4 158 138	2 031 (6.2%)	N/A
Total	**177 516**	**$107 001 451**	**17 840 (10%)**	**▲10%**

Appendix 2: Scam reports by state and territory

Australian Capital Territory

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
Betting & sports investment scams	$1 700 010	4	2 (50%)	▲Very low loss in 2017
Investment scams	$963 999	101	24 (23.8%)	▲67.7%
Dating & romance scams	$429 871	71	18 (25.4%)	▲314%
Remote access scams	$154 617	227	25 (11%)	▲140.7%
Hacking	$94 881	200	15 (7.5%)	▲13.2%
Online shopping scams	$72 955	269	150 (55.8%)	▲137.5%
Other/old categories	$68 169	1 005	53 (5.3%)	N/A
Identity theft	$44 763	350	14 (4%)	▲93.6%
Classified scams	$41 439	160	33 (20.6%)	▲140.9%
Threats to life, arrest or other	$34 463	668	12 (1.8%)	▼–81.6%
False billing	$28 464	336	36 (10.7%)	▲346.8%
Phishing	$16 502	814	14 (1.7%)	▼–19.4%
Pyramid Schemes	$15 165	6	2 (33.3%)	▼–83.5%
Inheritance scams	$15 000	71	1 (1.4%)	No loss in 2017
Jobs & employment scams	$9 592	58	8 (13.8%)	▼–37.9%
Scratchie scams	$6 060	96	4 (4.2%)	▼–86.6%
Ransomware & malware	$3 650	154	2 (1.3%)	▲40.4%
Health & medical products	$3 458	30	4 (13.3%)	▲315.6%
Rebate scams	$3 000	103	1 (1%)	▲2.1%
Psychic & clairvoyant	$2 950	4	2 (50%)	No loss in 2017
Up-front payment & advance fee frauds	$2 769	26	4 (15.4%)	▼–97%
Unexpected prize & lottery scams	$2 730	289	4 (1.4%)	▼–96.2%
Overpayment scams	$1 568	41	9 (22%)	▼–61.1%
Mobile premium services	$1 082	72	8 (11.1%)	▼–14.2%
Fake charity scams	$750	23	1 (4.3%)	▼–77.2%
Nigerian scams	$0	21	(0%)	▼–100%
Travel prize scams	$0	52	(0%)	▼–100%
Total	**$3 717 907**	**5 251**	**446 (8.5%)**	**▲122.1%**

New South Wales

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
Investment scams	$9 488 605	972	284 (29.2%)	▼–5.5%
Dating & romance scams	$5 806 543	838	234 (27.9%)	▼–6.7%
False billing	$1 597 567	3 331	364 (10.9%)	▲18.5%
Remote access scams	$1 399 709	3 770	273 (7.2%)	▲53.7%
Hacking	$1 169 554	2 856	151 (5.3%)	▲108.2%
Threats to life, arrest or other	$1 046 137	6 273	92 (1.5%)	▲384.5%
Online shopping scams	$736 640	2 757	1 610 (58.4%)	▲81.5%
Classified scams	$702 010	1 410	326 (23.1%)	▲104.2%
Betting & sports investment scams	$490 765	69	22 (31.9%)	▼–11.7%
Identity theft	$453 048	4 069	140 (3.4%)	▼–20.8%
Unexpected prize & lottery scams	$338 051	2 914	82 (2.8%)	▼–26.3%
Overpayment scams	$298 120	555	118 (21.3%)	▲169.7%
Nigerian scams	$280 416	178	25 (14%)	▲177%
Jobs & employment scams	$245 011	569	79 (13.9%)	▼–57.5%
Phishing	$210 480	7 391	117 (1.6%)	▼–40.4%
Pyramid Schemes	$196 134	87	21 (24.1%)	▲44.8%
Up-front payment & advance fee frauds	$191 853	414	74 (17.9%)	▼–73.3%
Inheritance scams	$186 488	759	19 (2.5%)	▼–85%
Scratchie scams	$125 818	174	9 (5.2%)	▼–21.3%
Psychic & clairvoyant	$122 198	67	26 (38.8%)	▲21.3%
Fake charity scams	$110 147	283	41 (14.5%)	▼–55%
Travel prize scams	$84 605	258	15 (5.8%)	▲98.4%
Ransomware & malware	$57 322	1 334	26 (1.9%)	▼–10.4%
Health & medical products	$40 701	297	71 (23.9%)	▼–50.4%
Mobile premium services	$21 934	582	87 (14.9%)	▲39.7%
Rebate scams	$12 295	1 029	22 (2.1%)	▼–89%
Other/old categories	$994 527	9 477	573 (6%)	N/A
Total	**$26 406 678**	**52 713**	**4 901 (9.3%)**	**▼–5.7%**

Northern Territory

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
Investment scams	$2 509 317	38	18 (47.4%)	▲Very low loss in 2017
Dating & romance scams	$527 436	210	79 (37.6%)	▲57.2%
Inheritance scams	$234 480	50	6 (12%)	▲Very low loss in 2017
Identity theft	$78 209	102	6 (5.9%)	▲Very low loss in 2017
Classified scams	$64 010	62	21 (33.9%)	▲218.3%
False billing	$50 116	134	13 (9.7%)	▲653.5%
Threats to life, arrest or other	$43 290	197	6 (3%)	▲901.9%
Unexpected prize & lottery scams	$36 577	107	18 (16.8%)	▲16.4%
Nigerian scams	$27 444	40	14 (35%)	▲259.2%
Remote access scams	$19 725	85	6 (7.1%)	▲Very low loss in 2017
Online shopping scams	$17 443	111	62 (55.9%)	▲87.5%
Jobs & employment scams	$13 480	46	6 (13%)	▲461.9%
Up-front payment & advance fee frauds	$9 272	37	12 (32.4%)	▼–85.6%
Overpayment scams	$8 567	30	6 (20%)	▲531.8%
Ransomware & malware	$8 109	40	2 (5%)	▲207.7%
Hacking	$8 081	78	7 (9%)	▲76.1%
Betting & sports investment scams	$8 000	1	1 (100%)	▲Very low loss in 2017
Health & medical products	$4 915	11	2 (18.2%)	▼–93.1%
Phishing	$4 370	183	3 (1.6%)	▲142.8%
Pyramid Schemes	$3 652	6	3 (50%)	▼–64.7%
Mobile premium services	$633	29	3 (10.3%)	▲257.6%
Fake charity scams	$250	9	1 (11.1%)	▼–87.1%
Rebate scams	$30	29	2 (6.9%)	▼–88%
Psychic & clairvoyant	$9	4	1 (25%)	▼–99.8%
Scratchie scams	$0	2	(0%)	No loss in 2017
Travel prize scams	$0	6	(0%)	▼–100%
Other/old categories	$24 214	316	30 (9.5%)	N/A
Total	**$3 701 629**	**1 963**	**328 (16.7%)**	**▲284.7%**

Queensland

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
Investment scams	$6 939 935	648	210 (32.4%)	▲23.9%
Dating & romance scams	$4 407 351	537	199 (37.1%)	▲39.8%
False billing	$999 539	2 349	238 (10.1%)	▲134%
Remote access scams	$871 433	2 376	175 (7.4%)	▲80.4%
Classified scams	$601 236	1 102	239 (21.7%)	▲154.4%
Threats to life, arrest or other	$596 694	3 556	46 (1.3%)	▲120.4%
Online shopping scams	$550 412	1 756	968 (55.1%)	▲92.5%
Jobs & employment scams	$437 913	474	45 (9.5%)	▲163.5%
Hacking	$394 225	1 826	105 (5.8%)	▼–4.9%
Inheritance scams	$286 600	526	10 (1.9%)	▲104.3%
Unexpected prize & lottery scams	$279 701	2 186	63 (2.9%)	▼–22.5%
Nigerian scams	$230 940	163	22 (13.5%)	▲2.3%
Identity theft	$200 596	2 715	67 (2.5%)	▲27%
Up-front payment & advance fee frauds	$142 582	319	58 (18.2%)	▼–66.6%
Phishing	$140 056	5 125	61 (1.2%)	▲70.6%
Scratchie scams	$111 699	257	10 (3.9%)	▲110.1%
Betting & sports investment scams	$109 221	58	18 (31%)	▼–59.1%
Overpayment scams	$100 017	357	66 (18.5%)	▼–8.9%
Rebate scams	$55 570	736	14 (1.9%)	▼–12.6%
Fake charity scams	$47 947	187	27 (14.4%)	▲213.6%
Pyramid Schemes	$47 238	72	15 (20.8%)	▲79.7%
Ransomware & malware	$27 216	952	18 (1.9%)	▼–38%
Health & medical products	$19 110	272	48 (17.6%)	▼–17.6%
Mobile premium services	$12 304	344	56 (16.3%)	▲58.1%
Travel prize scams	$5 639	230	15 (6.5%)	▼–59.9%
Psychic & clairvoyant	$1 794	20	8 (40%)	▼–94.3%
Other/old categories	$835 453	7 718	355 (4.6%)	N/A
Total	**$18 452 421**	**36 861**	**3 156 (8.6%)**	**▲30.2%**

South Australia

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
Investment scams	$2 103 030	222	69 (31.1%)	▲15.8%
Dating & romance scams	$1 274 886	182	59 (32.4%)	▲113.1%
False billing	$427 854	853	91 (10.7%)	▲Very low loss in 2017
Threats to life, arrest or other	$334 870	1 288	20 (1.6%)	▲Very low loss in 2017
Online shopping scams	$227 350	695	345 (49.6%)	▲227.6%
Remote access scams	$190 495	922	67 (7.3%)	▲12.6%
Phishing	$183 082	1 888	27 (1.4%)	▲117.2%
Pyramid Schemes	$131 650	19	8 (42.1%)	▲730.3%
Inheritance scams	$111 036	203	6 (3%)	No loss in 2017
Unexpected prize & lottery scams	$86 713	849	20 (2.4%)	▲327.4%
Classified scams	$80 685	420	89 (21.2%)	▼-4.6%
Nigerian scams	$77 309	60	6 (10%)	▲Very low loss in 2017
Hacking	$59 902	689	34 (4.9%)	▲57.7%
Identity theft	$59 096	1 042	27 (2.6%)	▲213%
Overpayment scams	$44 619	132	28 (21.2%)	▲38.4%
Scratchie scams	$18 657	195	4 (2.1%)	▲56.8%
Rebate scams	$15 964	320	10 (3.1%)	▼-74.1%
Betting & sports investment scams	$12 900	18	3 (16.7%)	▼-92.9%
Up-front payment & advance fee frauds	$10 312	97	14 (14.4%)	▼-88%
Mobile premium services	$9 427	136	23 (16.9%)	▲263.4%
Jobs & employment scams	$5 500	135	20 (14.8%)	▼-90.4%
Psychic & clairvoyant	$3 608	12	2 (16.7%)	▲Very low loss in 2017
Health & medical products	$3 090	81	15 (18.5%)	▼-48.2%
Travel prize scams	$1 800	106	2 (1.9%)	▼-61.5%
Fake charity scams	$624	70	5 (7.1%)	▼-85.9%
Ransomware & malware	$570	377	3 (0.8%)	▼-96.9%
Other/old categories	$262 202	2 600	145 (5.6%)	N/A
Total	**$5 737 231**	**13 611**	**1 142 (8.4%)**	**▲56.3%**

Tasmania

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
Investment scams	$377 485	64	25 (39.1%)	▲189.6%
Dating & romance scams	$120 716	64	17 (26.6%)	▼–83.2%
Remote access scams	$71 829	262	19 (7.3%)	▲442.6%
Unexpected prize & lottery scams	$54 205	254	8 (3.1%)	▼–34.4%
Betting & sports investment scams	$51 150	3	2 (66.7%)	▲130.7%
Online shopping scams	$34 770	181	98 (54.1%)	▼–27.1%
Phishing	$28 681	479	8 (1.7%)	▲Very low loss in 2017
False billing	$23 412	253	27 (10.7%)	▼–35.8%
Hacking	$22 187	182	13 (7.1%)	▼–77.1%
Threats to life, arrest or other	$8 200	296	2 (0.7%)	No loss in 2017
Classified scams	$8 008	113	19 (16.8%)	▲69.5%
Identity theft	$7 336	237	11 (4.6%)	▲321.1%
Up-front payment & advance fee frauds	$5 752	21	4 (19%)	▼–75.2%
Jobs & employment scams	$5 160	22	4 (18.2%)	▲Very low loss in 2017
Inheritance scams	$3 850	60	1 (1.7%)	No loss in 2017
Pyramid Schemes	$3 500	5	2 (40%)	No loss in 2017
Ransomware & malware	$2 724	102	3 (2.9%)	▼–7.5%
Mobile premium services	$2 155	31	7 (22.6%)	▲329.3%
Nigerian scams	$2 010	13	2 (15.4%)	No loss in 2017
Overpayment scams	$800	32	2 (6.3%)	▲45.5%
Health & medical products	$470	19	3 (15.8%)	▼–79.5%
Travel prize scams	$250	25	1 (4%)	▼–84.1%
Fake charity scams	$85	27	4 (14.8%)	▼–99.7%
Scratchie scams	$19	37	1 (2.7%)	▼–99.8%
Psychic & clairvoyant	$0	4	(0%)	▼–100%
Rebate scams	$0	80	(0%)	▼–100%
Other/old categories	$145 433	565	34 (6%)	N/A
Total	**$980 187**	**3 431**	**317 (9.2%)**	**▼–31.7%**

Victoria

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
Investment scams	$6 449 300	675	200 (29.6%)	▼–0.6%
Dating & romance scams	$4 159 570	594	203 (34.2%)	▼–12.2%
Unexpected prize & lottery scams	$1 501 028	2 203	69 (3.1%)	▲299.4%
Remote access scams	$1 423 841	2 595	197 (7.6%)	▲155.5%
Threats to life, arrest or other	$907 405	4 856	109 (2.2%)	▼–40.6%
False billing	$855 707	2 350	255 (10.9%)	▲30.4%
Hacking	$770 288	1 872	95 (5.1%)	▲89.3%
Online shopping scams	$551 350	2 076	1 257 (60.5%)	▲145%
Rebate scams	$495 887	1 103	37 (3.4%)	▲652.3%
Classified scams	$439 152	1 007	259 (25.7%)	▲86%
Identity theft	$317 261	2 989	112 (3.7%)	▲140.1%
Phishing	$254 446	5 470	75 (1.4%)	▲20%
Nigerian scams	$254 439	123	19 (15.4%)	▼–39.1%
Scratchie scams	$208 775	229	15 (6.6%)	▲28.4%
Inheritance scams	$199 832	544	12 (2.2%)	▼–80.6%
Betting & sports investment scams	$161 865	56	16 (28.6%)	▼–55.8%
Health & medical products	$156 155	191	65 (34%)	▲57.7%
Jobs & employment scams	$150 872	561	90 (16%)	▼–59.1%
Pyramid Schemes	$119 327	50	16 (32%)	▲238.3%
Overpayment scams	$109 920	486	98 (20.2%)	▲153.1%
Up-front payment & advance fee frauds	$68 036	346	60 (17.3%)	▼–96.1%
Ransomware & malware	$46 161	890	27 (3%)	▼–36%
Psychic & clairvoyant	$38 444	30	16 (53.3%)	▲245.9%
Fake charity scams	$34 954	201	31 (15.4%)	▲125.5%
Travel prize scams	$31 733	227	15 (6.6%)	▲167.1%
Mobile premium services	$25 809	510	61 (12%)	▲46.6%
Other/old categories	$1 005 018	7 166	465 (6.5%)	N/A
Total	**$20 736 575**	**39 400**	**3 874 (9.8%)**	**▼–9.7%**

Western Australia

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
Investment scams	$4 858 884	353	105 (29.7%)	▲74.8%
Dating & romance scams	$2 018 155	257	93 (36.2%)	▲71.3%
False billing	$869 070	1 174	136 (11.6%)	▲Very low loss in 2017
Inheritance scams	$837 100	329	8 (2.4%)	▲Very low loss in 2017
Hacking	$447 845	766	44 (5.7%)	▲580.3%
Remote access scams	$401 900	996	84 (8.4%)	▲119.1%
Online shopping scams	$275 592	904	505 (55.9%)	▲101.8%
Unexpected prize & lottery scams	$263 124	975	29 (3%)	▲377.8%
Identity theft	$227 174	1 082	40 (3.7%)	▲455.9%
Threats to life, arrest or other	$148 430	2 189	36 (1.6%)	▲348.9%
Classified scams	$142 427	499	102 (20.4%)	▲186.8%
Nigerian scams	$136 966	49	9 (18.4%)	▼–4.1%
Overpayment scams	$114 776	183	29 (15.8%)	▲162.3%
Phishing	$73 813	2 560	26 (1%)	▲47.8%
Jobs & employment scams	$45 184	523	13 (2.5%)	▲29.1%
Pyramid Schemes	$39 464	41	9 (22%)	▲343.4%
Up-front payment & advance fee frauds	$33 806	156	31 (19.9%)	▼–87.7%
Betting & sports investment scams	$30 950	18	7 (38.9%)	▼–90%
Travel prize scams	$26 154	90	8 (8.9%)	▲Very low loss in 2017
Rebate scams	$14 938	352	3 (9%)	▼–11.6%
Mobile premium services	$8 261	203	36 (17.7%)	▲176.8%
Fake charity scams	$6 665	58	6 (10.3%)	▲906.8%
Health & medical products	$5 022	90	17 (18.9%)	▼–13.2%
Ransomware & malware	$3 343	414	7 (1.7%)	▼–85.5%
Psychic & clairvoyant	$460	8	2 (25%)	No loss in 2017
Scratchie scams	$0	5	(0%)	No loss in 2017
Other/old categories	$337 940	3 448	203 (5.9%)	N/A
Total	**$11 367 443**	**17 722**	**1 588 (9%)**	**▲80.2%**

Appendix 3: Scam reports from businesses

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
False billing	$3 144 085	1 820	171 (9.4%)	▲113.9%
Investment scams	$2 152 309	59	16 (27.1%)	▲Very low loss in 2017
Hacking	$807 364	304	24 (7.9%)	▲38.8%
Phishing	$241 911	638	13 (2%)	▲730.2%
Classified scams	$211 127	153	41 (26.8%)	▲296.8%
Online shopping scams	$148 322	174	56 (32.2%)	▲552.6%
Overpayment scams	$70 933	144	14 (9.7%)	▲99.8%
Remote access scams	$62 569	252	10 (4%)	▲12%
Identity theft	$55 263	246	15 (6.1%)	▼–59.9%
Up-front payment & advance fee frauds	$35 405	91	12 (13.2%)	▼–70.1%
Fake charity scams	$23 200	89	19 (21.3%)	▲9.6%
Health & medical products	$21 483	31	5 (16.1%)	▲421.6%
Dating & romance scams	$15 000	10	1 (10%)	No loss in 2017
Jobs & employment scams	$8 948	55	2 (3.6%)	No loss in 2017
Mobile premium services	$3 316	30	7 (23.3%)	▲90.8%
Threats to life, arrest or other	$2 500	219	1 (0.5%)	▲19.6%
Betting & sports investment scams	$2 000	1	1 (100%)	▼–66.9%
Inheritance scams	$1 732	42	1 (2.4%)	No loss in 2017
Ransomware & malware	$724	176	1 (0.6%)	▼–98.1%
Nigerian scams	$0	16	(0%)	▼–100%
Psychic & clairvoyant	$0	1	(0%)	No loss in 2017
Pyramid Schemes	$0	1	(0%)	No loss in 2018
Rebate scams	$0	38	(0%)	▼–100%
Scratchie scams	$0	2	(0%)	No loss in 2017
Travel prize scams	$0	7	(0%)	No loss in 2017
Unexpected prize & lottery scams	$0	46	(0%)	No loss in 2017
Other/old categories	$269 207	1 207	101 (8.4%)	N/A
Total	**$7 277 398**	**5 852**	**511 (8.7%)**	**▲55.9%**

Appendix 4: Scam reports from Indigenous consumers

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2017
Investment scams	$1 198 961	62	30 (48.4%)	▲627.1%
Dating & romance scams	$905 399	128	39 (30.5%)	▲21.2%
Classified scams	$94 627	77	20 (26%)	▲556.5%
Phishing	$68 871	237	8 (3.4%)	▲Very low loss in 2017
False billing	$65 759	155	31 (20%)	▲Very low loss in 2017
Unexpected prize & lottery scams	$65 450	180	21 (11.7%)	▲14.9%
Jobs & employment scams	$58 532	57	8 (14%)	▼-86.5%
Nigerian scams	$54 960	40	15 (37.5%)	▲694.9%
Pyramid Schemes	$34 549	8	4 (50%)	▲245.1%
Remote access scams	$32 115	87	9 (10.3%)	▲Very low loss in 2017
Online shopping scams	$31 254	160	97 (60.6%)	▼-48.1%
Inheritance scams	$25 217	54	3 (05.6%)	No loss in 2017
Hacking	$22 734	141	9 (6.4%)	▲122.3%
Travel prize scams	$22 450	7	1 (14.3%)	▲654.4%
Fake charity scams	$13 435	24	6 (25%)	▼-47.1%
Identity theft	$11 389	189	14 (7.4%)	▲33.2%
Up-front payment & advance fee frauds	$10 258	32	12 (37.5%)	▼-80.4%
Health & medical products	$7 939	21	8 (38.1%)	▲727.8%
Betting & sports investment scams	$6 884	12	8 (66.7%)	▼-32.4%
Overpayment scams	$5 629	29	8 (27.6%)	▲117.4%
Ransomware & malware	$5 600	33	1 (3%)	▲72.6%
Rebate scams	$1 200	43	2 (4.7%)	No loss in 2017
Threats to life, arrest or other	$1 000	175	1 (0.6%)	▼-60%
Mobile premium services	$6	29	1 (3.4%)	▼-98.7%
Psychic & clairvoyant	$0	7	1 (14.3%)	▼-100%
Scratchie scams	$0	14	(0%)	▼-100%
Other/old categories	$262 777	433	43 (9.9%)	N/A
Total	**$3 006 995**	**2 434**	**400 (16.4%)**	**▲78.9%**