ACCC

AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

Targeting scams 2019

A review of scam activity since 2009

June 2020

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

ACCC 06/20_1657
www.accc.gov.au

Foreword

This report marks 11 years of the ACCC's annual *Targeting scams* report.

The world has changed since the ACCC issued the first *Targeting scams* report in 2009.

The way we communicate and transact has been transformed with the advent—and now proliferation—of smartphones. New payment technologies and online platforms have also emerged, and social media now connects people with families, communities and networks globally. Only around 27 per cent of Australians still use cash for payments, down from 61 per cent in 2010.[1]

All of these significant technological and social changes, while undoubtedly benefiting consumers and businesses, have provided scammers with easier ways to find victims. The stark reality is most years we are seeing greater financial losses affecting more people, despite the ACCC's and other government agencies' concerted and continuing efforts.

Scam losses grossly underreported

Australians lost over **$634 million** to scams in 2019. This is a 30 per cent increase on 2018, when $489 million was reported lost.[2] Australians made 167 797 reports to Scamwatch in 2019 and, concerningly, although we received 5 per cent fewer reports than in 2018, financial losses increased by 34 per cent.

While Scamwatch.gov.au is the primary government website used by Australians to report scams, only around 13 per cent of victims make a report.[3] To paint a clearer picture of the impact of scams, in recent *Targeting scams* reports we have included scams data from reports made to other government agencies. This year, for the first time, we have also included losses reported to the big four banks.

Around 33 per cent of people who had lost money to scams in the previous five years did not report that loss to any organisation.[4] So we know that unfortunately financial losses to scams are grossly understated even by the dollar amounts estimated in this report.

Losses by scam type

Based on the combined data, the greatest losses in 2019 by type of scam were:

- $132 million lost to business email compromise scams
- $126 million lost to investment scams, and
- $83 million lost to dating and romance scams.

Scammers continued to target businesses in 2019, with business email compromise scams causing the largest losses of any scam type. These scams affect businesses, suppliers and individuals by tricking people into paying invoices to scammers' bank accounts instead of the legitimate account.

Investment scam losses reported to Scamwatch increased by 59 per cent in 2019. High-profile investment scams using 'celebrity' endorsements contributed to significant individual financial losses.

1 J Caddy, L Delaney, C Fisher and C Noone, *Consumer Payment Behaviour in Australia*, 2020, RBA Bulletin March https://www.rba.gov.au/publications/bulletin/2020/ar/pdf/consumer-payment-behaviour-in-australia.pdf.

2 2018 losses do not include losses reported to the big four banks, which were included for the first time in 2019.

3 Roy Morgan ACCC scam survey 2019.

4 Roy Morgan ACCC scam survey 2019.

The changing scam landscape

Scammers continue to adapt their strategies and technology use. In the past scams have relied on persuading a victim to hand over money or personal information. While this is still the norm, many scams, including phone porting scams, now operate with limited contact or none at all, making it difficult for targets to recognise and avoid them.

Scammers have moved to unexpected platforms to target victims. For example, in 2019 we saw dating and romance scammers targeting unsuspecting victims through gaming apps such as Words With Friends, and investment scammers targeting Facebook and Instagram users with 'get rich quick' cryptocurrency investment scams.

One consistently strong message we have maintained throughout the decade is that Australians need to protect their personal information. Scammers seek to steal money but, more often than not, their methods also involve the collection of personal information and data. Scammers use personal data to steal identities, open loans, and steal or launder money.

One piece of good news is that increasing numbers of people are now able to recognise and avoid scams. In 2019, only 11.8 per cent of scam reports included a financial loss. Most people reporting to Scamwatch have not lost money or personal data to scammers. In this report we have explored why they were better able to identify scams than other people were, and we've shared the red flags that helped them avoid scams.

Preventing scams

A key pillar in scam prevention is the importance of telling others about scam experiences, or 'word of mouth'. Many people who avoided scams did so because their friends or family had told them about the scams, or that the approach or experience seemed suspicious. We have also explored the psychology of scams to better understand how scammers manipulate their victims.

Scamwatch.gov.au provides information to help people identify, avoid and report scams. We use scam reports to spot emerging issues and warn the public through media releases, social media updates and radar alerts. We also engage with the community at public forums and events to provide more targeted messaging for particular groups.

On the disruption side, we engage with businesses that scammers use to source victims or receive money through. Through the Scams Intermediaries project, we have established automated systems to share scams reports with intermediaries so they can ultimately disrupt them.

In July 2019, the ACCC released its *Digital Platforms Inquiry final report*. The report found that Facebook and Google need to do more to remove scam content from their platforms. It also recommended that both platforms develop improved internal dispute resolution schemes, and that an ombudsman be established to deal with complaints about the platforms, including scam complaints.

The ACCC also initiated the Scam Watchlist project, which shares anonymised scam data with digital platforms and businesses to aid scams prevention and disruption.

In 2019 the Australian Communications and Media Authority supported telecommunications companies to do more to prevent scam calls reaching Australians, with assistance from the ACCC and the Australian Cyber Security Centre.

Our decade of data shows that scams continue to be a pervasive problem for Australia. In the coming years we expect scams to adapt and evolve even faster, as they manipulate new technologies to target new victims.

Scammers are also quick to adapt to local events or global crises. The start of 2020 has seen an explosion of scams exploiting the bushfire crisis in Australia as well as the global COVID-19 pandemic. At a time when Australians can least afford to lose money to scammers we need more than ever to stay on top of scams, look out for each other and find innovative ways to disrupt scams.

Scams are a whole-of-community problem and governments, industry and business all have a role in preventing them. It is not enough to react to scams; we must all work together to find ways to disrupt them early or prevent them. Only then can we limit the significant financial and emotional harm that Australians experience as a result of being scammed. We look forward to continuing this increased cooperation and action with government and private sector organisations throughout 2020.

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

Contents

Glossary

Scam terms

Advance fee fraud

Advance fee fraud is a scam that typically involves promising large sums of money in return for a small up-front payment that the scammer says they require to arrange the transfer of money. Once the first initial payment is paid, the scammer will request more and more money. The ACCC stopped using this scam term because many scams could be classified as 'advance fee fraud'.

ATO impersonation scams

Scammers are increasingly impersonating the Australian Taxation Office and offering Australians rebates for overpaid taxes or threatening them with legal action for unpaid taxes.

Betting and sports investment scams (formerly known as 'computer prediction software schemes')

Betting and sports investment scams can include computer prediction software or betting syndicates. These scams try to convince people to bet in 'foolproof' systems that guarantee a profit on sporting events such as football or horse racing.

Business email compromise scams

These scams involve targeted phishing and hacking of a business. Scammers commonly send emails to the business's clients requesting payment to a fraudulent account, often by manipulating legitimate invoices to include fraudulent account details. Scammers also impersonate senior company managers requesting money transfers for a supposedly legitimate business purpose, or employees requesting a change of account for salary payment.

Chinese Authority Scams

These scams often target Mandarin-speaking people in Australia. Scammers contact people by phone and impersonate authorities such as the Chinese embassy, police or other government officials. They demand that you pay money to prove you did not commit a crime. These scams use threats designed to frighten people into paying the scammer and can include threats of arrest and deportation.

Classified scams

Scammers use online and paper-based classifieds and auction sites to advertise popular products (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.

Clickbait

Clickbait is a form of false advertising designed to attract attention and encourage people to click on a link that often takes them to misleading or scam content.

Cloud mining cryptocurrency scams

Mining is the only way to extract new Bitcoins without buying or exchanging them, but it has become an incredibly resource-intensive activity. It takes massive amounts of computer processing power and electricity, and thus money, to mine a coin. In cloud mining scams, a company offers to rent server time or space to mine new coins. They resemble Ponzi schemes, where investors can withdraw profits for a short time but then the platform ceases to trade and victims lose their investments.

Computer prediction software schemes

See 'betting and sports investment scams'.

Dating and romance scams

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

Deepfakes

A deepfake is a computer-generated replication of a person. Deepfakes use artificial intelligence to replace an existing image or video with another person's likeness (usually their voice).

Fake charity scams

Scammers impersonate genuine charities and ask for donations. These scams are particularly prolific after public tragedies such as natural disasters and other events, for example the 2020 bushfires and the coronavirus pandemic.

False billing scams

False billing scammers send invoices demanding payment for directory listings, advertising, domain name renewals or office supplies that were never ordered. They tend to target businesses over individuals. These scams often take advantage of businesses' limited resources and rely on them paying the amount before realising the invoice is fake.

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 may sell victims healthcare products at low prices that they never receive or make false promises about their products, such as medicines and treatments that will 'cure you' or have special healing properties.

Identity theft

Identity theft is fraud that involves using someone else's personal information to steal money or gain other benefits. Identity theft has become a significant risk in most scam types.

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 scammers offer a range of fake financial opportunities and the promise of high returns with low risk. These may include fake initial stock or coin offerings, brokerage services or an investment in expensive software or online trading platforms. These 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 or personal information to scammers while applying for a new job. Some iterations of this scam will offer a 'guaranteed' way to make fast money or a high-paying job for little effort.

Mobile phone number porting

Mobile phone number porting occurs when a phone number is transferred from one telecommunications provider to another. This can legitimately occur when a consumer changes their provider to seek a better deal and wants to keep their existing phone number. Scammers can port mobile phone numbers without the owner's knowledge and set up their own mobile phone to receive the ported phone number's messages. 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 can now come from anywhere in the world.

Online shopping scams

Online shopping scams involve scammers pretending to be legitimate online sellers, by using a fake website or setting up a fake profile on a genuine website or social media platform.

Other buying and selling scams

Any other scam not already identified where something is supposedly bought or sold. We classify scams into more specific categories wherever possible.

Overpayment scams

Overpayment scams work by getting victims to 'refund' a scammer who has sent them too much money for an item they are selling, or an item they have purchased online and have purportedly been charged too much money for. The victim later discovers the scammer never paid the initial amount in the first place.

Phishing

Phishing scams trick victims into giving out personal information such as bank account numbers, passwords, credit card numbers and superannuation details. A common form of phishing involves the impersonation of trusted organisations such as banks, telecommunications providers or government departments. This can occur via emails, text messages or websites, or over the phone.

Psychic and clairvoyant scams

Psychic and clairvoyant scams are designed to trick victims into giving away their money, usually offering 'help' in exchange for a fee. The 'help' may come in the form of winning lottery numbers, a lucky charm, the removal of a curse or jinx or details of secret wealth.

Pyramid schemes

Pyramid schemes are illegal and risky 'get-rich-quick' schemes. 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 a 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 to collect personal information or just damage the computer. Often the malware will cause the computer to freeze or lock and scammers will demand a payment to have it 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, scammers say an up-front fee must be paid before the larger rebate can be provided.

Reclaim scams

Scammers contact a victim pretending to be from the government or a utility company, bank or other well-known entity and ask for an up-front fee to reclaim money. Reasons this money is said to be owed can include overcharged bank fees, tax refunds or compensation. The ACCC no longer uses this scam category.

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 victim that they need to purchase antivirus software to remove the infection or they may spin a complex story claiming they are working with authorities and need to make transactions from the victim's bank account to 'track scammers'.

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.

Spoofing

Spoofing, in scam terms, is the practice of disguising a scam communication (email, website or phone number) to appear as though it came from a trusted source. Usually, scammers spoof government agencies, banks or utility companies.

'Threats to life, arrest or other'

'Threats to life, arrest or other' scams involve scammers demanding that victims pay money they supposedly owe, for example for a tax bill or because they have committed a crime, and threats against them if they do not cooperate. Chinese authority scams are also examples of this type of scam, as are 'sextortion' scams—in which scammers threaten to release embarrassing photos of victims to their mail or Facebook contacts unless the victim pays money.

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.

Payment methods

Cardless cash

Cardless cash is a service provided by some banks that allows you to withdraw cash without a card. You can also send codes to other people to withdraw the cash from your account on your behalf.

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. Cryptocurrencies are common in investment scams, and are also often requested as a payment method by scammers.

Ethereum

Ethereum is a global open-source publicly available blockchain platform. Ether (ETH) is the cryptocurrency used on the Ethereum network.

Skrill

Skrill is an e-commerce business that allows users to make payments and transfer money over the internet to other people or businesses around the world.

Neosurf

Neosurf is an instant way of depositing money into an e-commerce account. A Neosurf voucher can be bought at participating outlets and used to pay for shopping, gambling and other services over the internet.

Payment apps

Payment apps allow you to make payments using your phone. They allow you to transfer money quickly and securely to friends and family without the need for physical money. Common payment apps are Cash App, Zelle, Venmo, Apple Pay and Beem It.

Steam

Steam is a video game digital distribution service. It allows users to play games, enter discussion forums and create their own games.

Steam gift cards and Steam Wallets

Steam is free, but if people wish to play games or access other content there may be costs. Steam Wallet is an online method allowing people to pay for games. Users can add value to Steam Wallets by credit card payment, or by purchasing Steam gift cards in stores.

WorldRemit

WorldRemit is an online money transfer service that provides international remittance services.

TransferWise

TransferWise is a British online multi-currency money transfer service. People can send, receive and spend money internationally.

The role of Scamwatch

Scamwatch is run by the Australian Competition and Consumer Commission (ACCC). Established in 2002, its primary goal is to make Australia a harder target for scammers. To achieve this we raise awareness, share intelligence, and work with government and the private sector to disrupt scams.

The ACCC outlines its approach to scams each year in its Compliance and Enforcement Policy. In 2019–20, we committed to continuing to analyse and share Scamwatch data to identify trends, monitor financial losses and inform our scam prevention strategies.

The ACCC also collaborates on campaigns and shares intelligence with the Scams Awareness Network (SAN). On behalf of the network, the ACCC runs Scams Awareness Week—an annual campaign to warn consumers about the ongoing risk of scams.

We also prioritise targeted activities where appropriate in response to emerging issues affecting vulnerable and disadvantaged consumers.

The ACCC focuses on scams disruption and prevention to minimise harm to Australians. Because most scammers targeting Australians are based overseas, it is difficult for regulators such as the ACCC or even law enforcement agencies to track them down and act against them. These same challenges often also prevent victims from recovering monies lost to scams.

Notes on data in this report

Most of the detail in this report is based on reports made to the Scamwatch website. However, this year we also obtained data from several government agencies[5] and the big four banks to better illustrate the harm caused by scams. Due to the known under-reporting of scams, we believe the financial losses referred to in this report are only a fraction of the true losses suffered.

This report also discusses the impact of scams over the past decade. We have chosen to include data from 2009 to 2019 (inclusive). The first *Targeting scams* report was published in 2009, and we examine reports from this time until 2019, using our analysis to anticipate future trends.

Banks

For the first time, we obtained scam data from the big four banks to inform this report. This is because scam victims are more likely to report financial losses to their bank than anywhere else. The inclusion of this data helps paint a clearer picture of the impact of scams in Australia. The Australia and New Zealand Banking Group (ANZ), Commonwealth Bank of Australia (Commonwealth Bank), National Australia Bank (NAB) and Westpac Banking Corporation (Westpac) all contributed data to this report.

ACORN and ReportCyber

On 30 June 2019, the Australian Cybercrime Online Reporting Network (ACORN) ceased as the online reporting portal for cybercrime.[6] It was replaced by ReportCyber on 1 July 2019.[7] We obtained data from each reporting portal to make up the full 2019 year.

Managing data from various sources

As we have included data from various sources in this report, there was a risk of double counting particular reports or losses. This could occur where a scam victim reported their experience to more than one organisation—for example, Scamwatch and their bank.

In requesting and analysing external data, we made all reasonable efforts to avoid double counting reports or losses, but some duplication may have occurred.

Unless otherwise stated, statistics in this report refer to Scamwatch data only. Please note that these figures understate the extent of losses as only 13 per cent of people who lost money or personal information reported the loss to Scamwatch.[8]

Where we refer to 'combined reports or losses', this includes data from Scamwatch, ACORN, ReportCyber, other government agencies and the big four banks, unless otherwise stated.

5 Australian Communications and Media Authority, Australian Taxation Office, Services Australia and WA ScamNet.

6 Operated by the Australian Criminal Intelligence Commission.

7 Operated by the Australian Cyber Security Centre.

8 Roy Morgan ACCC scam survey 2019.

Targeting scams 2019

Losses

$634 million

2019 combined financial losses to scams as reported to Scamwatch, other government agencies and the big four banks (ANZ, Commonwealth Bank, NAB and Westpac)

$143 million

Amount reported lost to Scamwatch

167 797

reports to Scamwatch

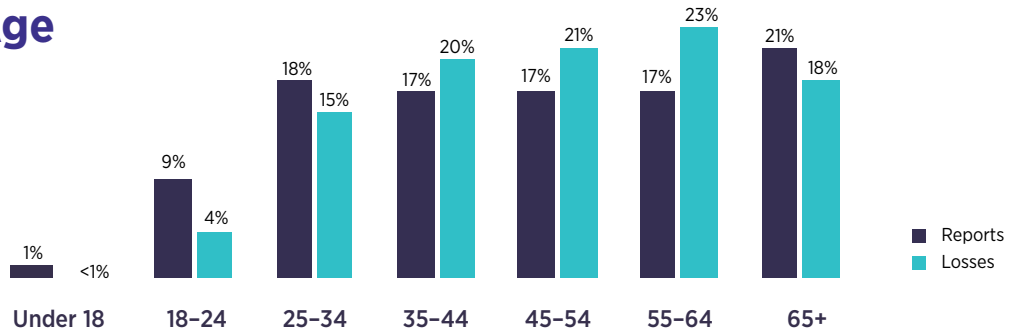
▲ **34%** since 2018

Average loss: $7224

Top scams by loss

As reported to Scamwatch

Age



Gender

Men

$77.5 million

78 551 reports

Males were more affected by investment scams, reporting losses of **$44.7 million**

Women

$63.6 million

85 486 reports

Females reported losing more to dating and romance scams with **$21.5 million** in losses

Non-specified

$1.8 million

3760 reports

Top contact methods by reports

41.4%

Phone

69 522 reports

$32.6 million

reported lost

24%

Email

40 277 reports

$28.4 million

reported lost

16.6%

Text message

27 894 reports

$3.03 million

reported lost

7.0%

Internet

11 776 reports

$31.6 million

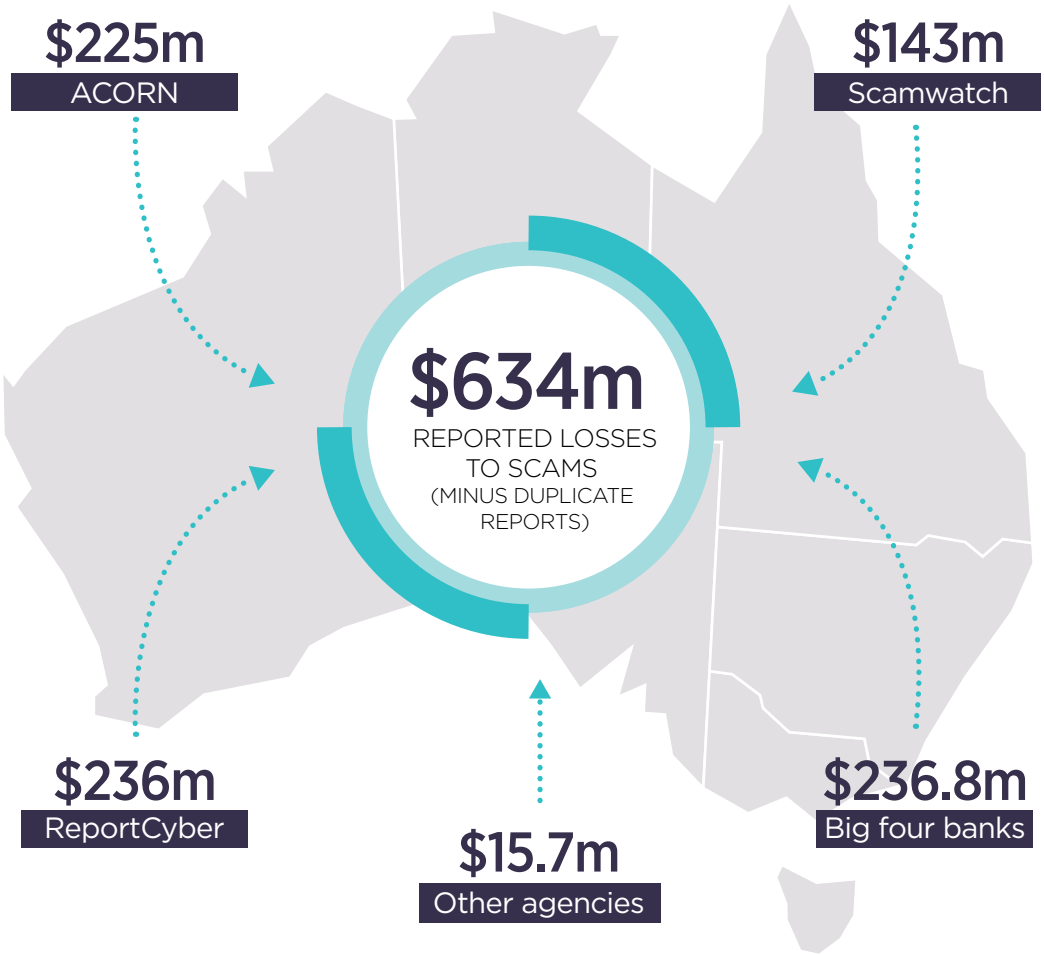
reported lost

1. Key findings

1.1 A decade of scams

- The ACCC published the first *Targeting scams* report in 2009 and has released 11 overall.
- Australians have reported losing $2.5 billion to scams between 2009 and 2019.[9]
- Since 2009, financial losses reported to Scamwatch have more than doubled (from $69.9 million to $142.9 million).
- We received eight times more reports in 2019 (167 000) than we did in 2009 (20 500).
- Significant advances in technology over the past decade have contributed to the proliferation of scams affecting Australians.
- While most scams remain fundamentally the same as in 2009, many have adapted over time to use social media, new payment methods and online services to source new victims or legitimise their stories.
- New scams have also emerged, such as business email compromise and cryptocurrency investment scams. These are now some of the most financially damaging scams for Australians.

Figure 1: Losses to scams[10]



9 Figure based on Scamwatch reports from 2009 to 2014, and combined reports from 2015 to 2019.

10 Excludes potential duplicate reports so that losses are not double counted.

1.2 Key statistics from 2019

Scamwatch, other government agencies and the big four banks received over 336 000 scam reports in 2019, with losses of $634 million.

- Financial losses reported to Scamwatch in 2019 exceeded every previous year, with $143 million lost. This is a 34 per cent increase over 2018, which totalled $107 million.
- Scamwatch received 167 797 scam reports in 2019. This is a decrease of 5.5 per cent from the previous year.
- The average loss reported to Scamwatch increased by 20 per cent ($7224 in 2019, up from to $5997 in 2018).
- The most financially damaging scams reported to Scamwatch were investment scams, consistent with previous years. Losses in 2019 increased by 59 per cent to $62 million (compared with $38.8 million in 2018).

Business email compromise scams caused the highest financial losses in 2019, with $132 million in combined losses.

Table 1: Top 10 scams reported to Scamwatch 2019[11]

Scam type	Reports	Reports with loss	Reported losses	Change in reports since 2018
Phishing	25 168	513 (2.0%)	$1 517 864	▲3.6%
Threats to life, arrest or other	13 375	414 (3.1%)	$4 250 689	▼-31.3%
Identity theft	11 373	562 (4.9%)	$4 311 066	▼-11.1%
False billing	11 255	1 881 (16.7%)	$10 110 756	▲2.4%
Online shopping scams	9 953	6 027 (60.6%)	$4 845 452	▲2.7%
Unexpected prize and lottery scams	9 456	471 (5.0%)	$2 385 669	▼-5.9%
Remote access scams	9 019	682 (7.6%)	$4 836 812	▼-20.5%
Hacking	8 321	509 (6.1%)	$5 139 414	▼-3.5%
Investment scams	5 005	2 128 (42.5%)	$61 813 401	▲42.7%
Classified scams	4 958	1 528 (30.8%)	$2 816 076	▼-0.2%

1.3 The scams

The top three scams in terms of combined financial losses were business email compromise ($132 million), investment ($126 million), and dating and romance scams ($83 million).

- The top three scams in terms of losses reported to Scamwatch were investment scams ($62 million), dating and romance scams ($29 million), and false billing scams ($10 million).
- The top three scams in terms of number of Scamwatch reports were phishing (25 168), threats to life, arrest or other (13 375) and identity theft (11 373).
- The top three payment methods for scams in 2019 were bank transfers ($70 million), Bitcoin ($19 million) and other payment methods ($15 million).
- Phone remained the most common contact method used by scammers at 41 per cent (a 6 per cent decrease since 2018). Scams received via text message increased by 2 per cent in 2019, with nearly 28 000 scams reported.
- Scams received through social media increased substantially in 2019: social networking contacts increased by 20 per cent and mobile app contacts increased by 29 per cent.

11 Eight of the top 10 scams reported to Scamwatch were also in the 10 scams causing the highest losses. See appendix for full tables of scams and losses.

1.4 Scam trends of 2019

Business email compromise scams[12]

- Business email compromise scams continued to target both businesses and individuals.
- In 2019, Scamwatch reports alone showed a 37 per cent increase in losses over the previous year. Losses in 2018 were $3.8 million, but this had grown to $5.3 million in 2019.
- The most financially damaging business email compromise scams involved invoices between businesses, suppliers or individuals being intercepted and amended with fraudulent banking details.

Celebrity endorsement scams

- Celebrity endorsement scams caused reported losses of over $1 million through 400 scam reports, where scammers used the image, name and personal characteristics of a well-known person to sell a product or service. In 2019 billionaire Andrew Forrest, celebrity chef Maggie Beer, television show *Shark tank* and others were impersonated in these scams.

Cryptocurrency investment scams

- Cryptocurrency investment scams increased in 2019, with Australians losing over $21 million. Cloud mining farms became a common adaptation of this type of scam. Most were Ponzi schemes, with no real cryptocurrency involved.

Crowdfunding scams

- There was an increase of reports about charity scammers using crowdfunding platforms in 2019, with losses of $4500. While crowdfunding platforms have existed in Australia for some years, they are now becoming a mainstream scam tool. Common scams include impersonating charities to fundraise, or impersonating victims of tragic events (or their family members) to raise funds for health, funeral or support expenses. We expect crowdfunding charity scams to grow in the future.
- In early 2020, scams on crowdfunding platforms became a concern due to the Australian bushfire crisis. People around the world were keen to donate to help those in need, and scammers took advantage of this by setting up fake crowdfunding pages with a bushfire theme.

Dating and romance scams

- Dating and romance scams became more insidious, as scammers moved to new platforms not designed for dating. In 2019, 31 per cent of dating and romance scams reported to Scamwatch originated on social media or online forums, with $9.5 million in losses to social media alone.

> **Combined losses for all dating and romance scams were $83 million.**

1.5 The people

- People aged 55 to 64 reported higher losses than any other age group, with losses of $30 million.
- Women reported more scams but lost less money than men. Women reported over 85 000 scams with losses of $64 million. In contrast, men reported over 78 000 scams with losses of $78 million.
- Similar to 2018, men experienced their highest losses to investment scams ($45 million) and women to dating and romance scams ($22 million).
- People identifying as 'unspecified gender' made 3760 reports with losses of $1.8 million. While report numbers are similar to 2018 (3623), this is a 38 per cent increase in losses from $1.3 million.
- Scamwatch received over 7770 reports with losses of $14 million from people whose first language was not English.

12 Business email compromise scams involve targeted phishing and hacking of businesses. Scammers commonly send emails to the business's clients requesting payment to a fraudulent account.

- Indigenous consumers reported 2767 scams with over $2 million in losses, a 30 per cent decrease in losses from 2018.

1.6 The businesses

- In 2019, businesses reported 5904 scams to Scamwatch with losses of over $5.3 million.
- Scamwatch reports from businesses show that false billing scams caused the highest losses, at $2.7 million (including some business email compromise reports).
- Businesses were targeted by scammers impersonating senior managers, staff and suppliers; consumers were targeted by scammers impersonating real estate agents, conveyancers and builders.

Business email compromise scams caused $132 million in combined reported losses.

1.7 The failed attempts

- Of the Scamwatch reports in 2019, 88 per cent did not incur a financial loss, and 84 per cent did not involve a loss of personal information.

1.8 The fight against scams

- In 2019 there were 112 413 subscribers to the Scamwatch scam radars, with 11 alerts issued.
- The Scamwatch website had 6.8 million page views, and the ACCC's *Little black book of scams* was downloaded 20 985 times. We also distributed 142 521 physical copies of the book (in addition, some banks print their own copies to give to customers).
- The Scamwatch Twitter account grew by 18 per cent, to 27 700 followers. The account posted 1251 tweets and retweets alerting Australians to current scams and other relevant information in 2019.
- We responded to hundreds of media requests in 2019, keeping the public informed about new scam trends. ACCC Deputy Chair Delia Rickard appeared on many television and radio programs promoting scams awareness and sharing tips on how people can protect themselves from scams.
- Scams Awareness Week ran in August 2019 with the tag line 'Too smart to be scammed?' The campaign was headed by the ACCC as Chair of the SAN and focused on showing people that scams are more sophisticated and harder to spot than ever.
- We automated intelligence-sharing with intermediaries to share scams on a daily basis.
- We engaged with various private businesses about scam trends on their websites. By sharing targeted scams intelligence with these businesses, we are able to help them build front-end scams disruption measures to prevent further harm to Australians.
- We expanded our sharing of Scamwatch reports with government partners and law enforcement.
- We were partners in the Australian Communications and Media Authority's (ACMA) Scam Technology Project. Outcomes between late 2019 and mid 2020 included:
  - establishing a joint government-industry taskforce
  - developing new enforceable obligations, and
  - trialling a 'Do Not Originate' list with the ATO.

  Details of these measures can be found in the ACMA's 'Combating scams' summary report.

2. A decade of scams

Since 2009, Australians have reported losing $992.7 million through over 990 000 reports to Scamwatch alone. In today's terms, that equates to over $1 billion in reported losses ($1.08 billion).[13]

> **When we combine Scamwatch data with other data over a three-year period we see that nearly $1.5 billion was reported lost.**
>
> **Research shows that 33 per cent of people who lose information or money to a scam will not report it, so figures in this report underestimate the extent of the loss.**[14]

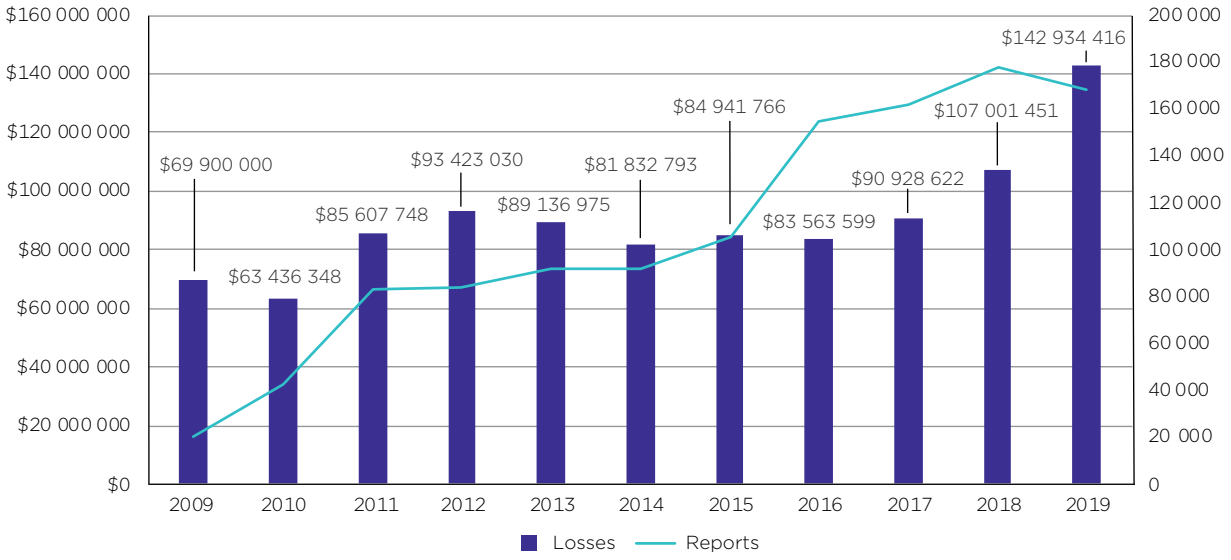
Our review of scams over the decade shows that scammers adapt to technology as quickly as it changes and build knowledge of local environments to impersonate trusted organisations. They are also quick to take advantage of local events and crises.

In 2009 the most common scam was advance fee fraud, including traditional 'Nigerian prince' spam emails. By 2019 these scams had given way to more complex and financially devastating scams including fraudulent phone ports and deepfakes.[15]

2.1 From 2009 to 2019

In 2009 Scamwatch received 20 500 reports of scams, with losses of $69.9 million. By 2019 reports exceeded 167 000, with reported losses of almost $143 million.

Figure 2: A decade of scams in reports and losses



As shown in figure 2, Scamwatch reports have been steadily increasing, particularly over the last five years, with a peak of nearly 180 000 reports in 2018. The drop in 2019 was the first substantial decrease in a decade. This drop may be a result of the ACCC's move to an online webform—people who haven't lost money would be less likely to take the time to complete an online report than those who have. In addition, reporting avenues have recently been implemented to allow people to make online reports to police and law enforcement. Despite the recent drop we attribute the longer term increase in reports to a combination of escalating scam activity, greater use of technology to reach

13 Real loss value calculated using Reserve Bank of Australia's Inflation Calculator https://www.rba.gov.au/calculator/annualDecimal.html.

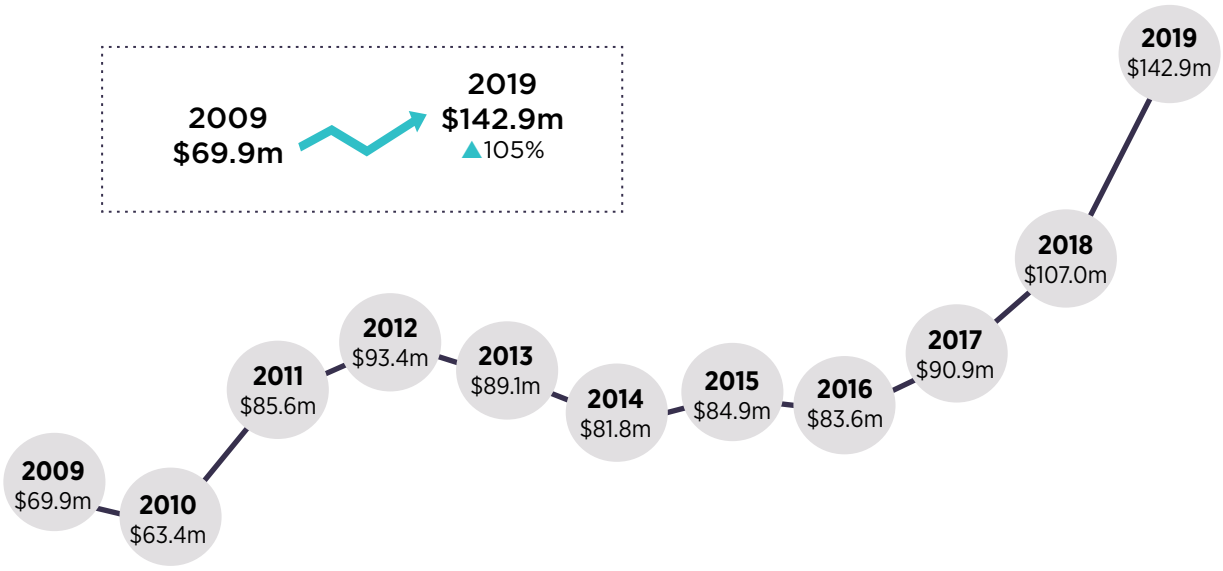
14 Roy Morgan ACCC scam survey 2019.

15 A deepfake is a computer-generated replication of a person. Deepfakes use artificial intelligence to replace an existing image or video with another person's likeness (usually their voice).

victims and heightened public awareness about Scamwatch and other scams work conducted by law enforcement agencies.

Financial losses have fluctuated over this time (details in figure 3 below). Losses increased by nearly 35 per cent in 2011, then remained fairly steady for seven years. However, in 2018 losses increased by 18 per cent, and increased again by 34 per cent the following year. Since 2009, financial losses have more than doubled.

Figure 3: Losses to Scamwatch over the past decade



Scamwatch is the only Commonwealth scam-reporting portal that publishes annual statistics. Since the establishment of ACORN in 2015, we have included losses reported to other agencies in the *Targeting scams* report to show the bigger picture of scams in Australia.

Table 2: Scam losses as reported to Australian agencies/organisations 2015–2019

Year	Scamwatch losses	Combined losses[16]
2015	$84.9 million	$229 million
2016	$83.6 million	$300 million
2017	$90.9 million	$340 million
2018	$107 million	$489 million
2019	$143 million	$634 million
Total	**$509 million**	**$2 billion**

The sharp increase in losses over the past two years is largely due to new cryptocurrency investment scams. Five years ago, losses to investment scams reported to Scamwatch were $12.5 million. In 2019 that had increased to $61.8 million. The number of reports about investment scams also increased, from 938 reports in 2014 to 5005 reports in 2019.

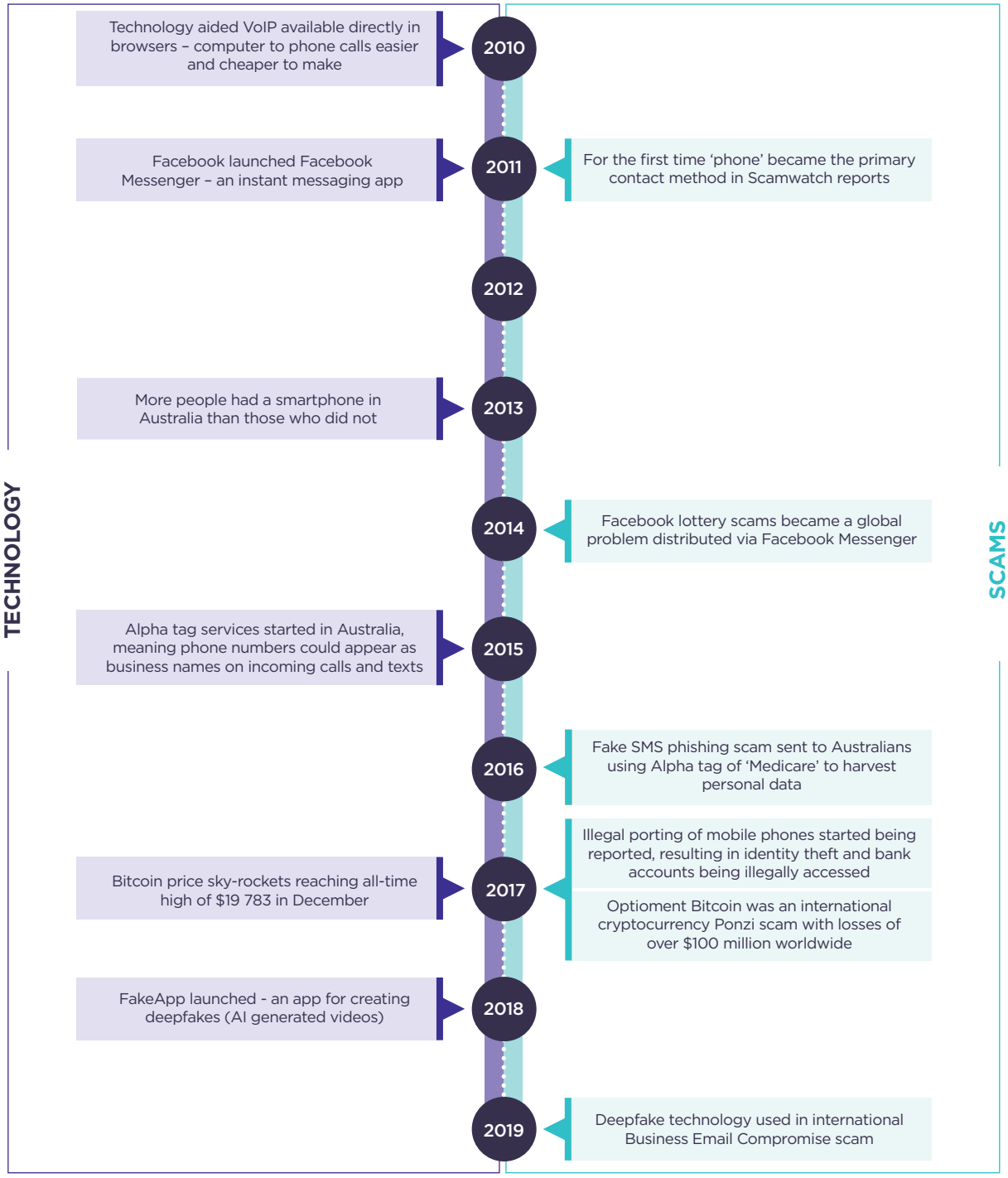
▶ **Australians lost $126 million to investment scams in 2019 (combined losses).**

16 Combined losses excludes duplicate reports (where a person reported the same scam to multiple agencies); includes reports made to ACORN, ReportCyber (2019 only) and other government agencies pre–2019. 2019 data includes scams reported to the Commonwealth Bank, ANZ, Westpac and NAB.

2.2 Advances in technology

Scam developments have been largely driven by technological advances, as shown in the timeline in figure 4.

Figure 4: A snapshot of scams adapting to new technologies since 2010



This decade has seen significant advances in technology, which have made it cheaper and easier to perpetrate scams on a large scale. While scammers have quickly capitalised on some new opportunities, others have been incorporated into scam strategies over longer periods.

An example is the use of Voice over Internet Protocol (VoIP) technology to perpetrate scams.[17] VoIP provides businesses, government agencies and organisations with high-quality and inexpensive phone services. When VoIP became more accessible in 2010, the era of phone scams soon followed. By 2011, for the first time, 'phone' became the most common contact method used by scammers.

At around the same time, internet access also opened more opportunities for scammers. In 2004–05 just 56 per cent of Australian households had internet access—within five years, that had increased to 80 per cent.[18] In 2011 one of the most common scams was the 'Microsoft scam', in which scammers would call people and say their computer had a virus and they could fix it over the phone. This scam was an early version of what we now call remote access scams. Remote access scams have become common and cost Australians millions every year.

In contrast, mobile phone porting scams took years to develop. Australia first introduced phone porting in 2001, and in 2009 regulatory changes made it faster and easier to port a number. In recent years more Australians have taken up mobile banking and now use their phone to pay their bills and manage their finances. By 2017, scammers began to take advantage of this technology and the significant amount of personal and financial information stored in a mobile phone. In 2013 only 22 per cent of Australians used a smartphone or tablet to access banking. By 2019 it was estimated that more Australians than not were using mobile banking apps. Scamwatch began receiving reports about phone porting scams via mobile banking in 2018, with many reports of large financial losses and identity compromise.

Over the last decade, scammers have manipulated important social developments as banks, governments and businesses have taken their goods and services online. We expect this trend to increase as Australia's economy continues to move to online platforms. For these reasons it is critical that scam prevention measures are built into new technologies when they are designed.

2.3 What has changed since 2009?

In 2009 advance fee fraud (also known as up-front payment scams) was the most common scam reported to Scamwatch, at 32 per cent of all reports. The ACCC no longer uses this category, and phishing scams (seeking personal information) are now the most commonly reported. While the most successful scams have changed, all the same types of scam are still in circulation. Over time there has been a shift from reports of scams seeking money, to reports about scams seeking information (phishing).

Table 3: Top 10 scam types reported to the ACCC, by number of reports

Top 10 scams of the year	2009	2014	2019
1	Advance fee fraud	Reclaim scams	Phishing scams
2	Online auction and shopping	Phishing scams	Threats to life, arrest or other
3	Lottery and sweepstakes	Remote access scams	Identity theft
4	Unexpected prize	Identity theft	False billing
5	False billing	Other buying and selling scams	Online shopping scams
6	Banking and online account (phishing)	Hacking	Unexpected prize and lottery scams
7	Job and employment scams	Inheritance scams	Remote access scams
8	Dating and romance scams	Up-front and advance fee scams	Hacking
9	Mobile phone	Unexpected prize and lottery scams	Investment scams
10	Computer prediction software	False billing	Classified scams

17 Hardware and software that allows telephone calls over the internet.

18 Australian Bureau of Statistics (ABS). Household Use of Information Technology, Australia, 2016–17. Cat. No. 8146.0. 2018.

In 2009, scammers used deception to manipulate and confuse. Scams relied on conning a victim into sending money, providing personal information or both. By 2019 many scams had developed to require very little communication between scammers and victims. Scams such as hacking, ransomware and malware, and online shopping have increased significantly, often involving little direct interaction between parties.

This change from active conning to almost contactless fraud is demonstrated by business email compromise scams, which have become the most financially damaging scams. In 2009, these scams did not exist—they have become successful due to new hacking technology and editing tools available over the past decade.

Another example of the shift to contactless fraud is phone porting scams. Fraudulent phone porting increased in Australia in 2019, with financial losses of over $1 million and psychological damage flowing from identity theft. Scammers steal a mobile phone number and port it to another provider not only without the owner's consent, but without contacting them at all. As mobile numbers are used for two-factor authentication, particularly by banks, this poses a serious risk of financial fraud and identity theft. The ACMA introduced new rules commencing 30 April 2020 requiring all mobile carriage service providers to use additional identity verification before a mobile number is ported from one provider to another.[19]

At the time of writing this report, Australia is in lockdown due to the global coronavirus pandemic. Because of this, we are seeing an increase in other cyber-based scams in 2020 where scammers don't need to actively interact with the victim, such as online shopping and phishing scams.

Contact methods

Communication methods have changed over the last 10 years, particularly through social media. In 2009 Facebook had become mainstream, MySpace was still common and gaming apps such as Words With Friends were gaining popularity. Instagram launched in 2010 and Tinder arrived in 2012. By 2019, social media had expanded to include new entrants such as TikTok.

Phone has been the most common contact method for scammers since 2011, with over 40 per cent of scams received by this method alone in 2019. Ten years ago most people received scams by email.

Mail scams have decreased over the years. In 2009, 13 per cent of all scams were received this way, but by 2019 that had reduced to 2 per cent. Scamwatch introduced categories for social media and mobile apps to respond to the growing number of scams on new platforms, which were unheard of in 2009.

Figure 5: Contact methods

Telephone

2009	2014	2019
10% of scams reported	**49%** of scams reported	**41%** of scams reported

Mail

2009	2014	2019
13% of scams reported	**7%** of scams reported	**2%** of scams reported

Internet and Email

2009	2014	2019
69% of scams reported	**34.8%** of scams reported	**31%** of scams reported

19 The Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 came into effect on 30 April 2020 with the goal of reducing the number of phone porting scams.

Payment methods

One of the biggest developments in scams over the past decade was the introduction of new payment methods. In 2009 the main scam payment methods were credit card, bank transfer, debit card, cash, telephone/internet banking and cheque. Since then many new payment methods have entered the market and scammers quickly took advantage of these to steal money from targets.[20]

While bank transfers remained the top payment method in 2019, a range of other payment methods are now used in scams.

Table 4: New payment methods used by scammers since 2009

Bank payments	Most banks now offer cardless cash, transfers to mobile phone numbers and BPAY.
Peer-to-peer payments (P2P)	P2P allows users to transfer money to another person or company without using a third party. Platforms such as Facebook Messenger, Zelle and Circle Pay use P2P payments.
Payment apps	Payment apps allow users to make payments using their phones. They are commonly used on donation portals, browser games, social media networks and dating sites. Examples include Apple Pay, Venmo, Cash App, Square Cash and Google Pay.
Payment gateways	These are merchant services provided by e-commerce applications that authorise and process payments for online businesses. PayPal, Stripe, WePay and Worldpay are payment gateways.
Fintech	Short for 'financial technology', fintech finds ways to use technology with payments. Since 2011, 750 new fintech companies have launched, including 'buy now pay later' services such as Afterpay and ZipPay.
E-wallets or digital wallets	These provide a way for users to store their bank account or credit card payment details online. Users can pay for something online by entering a username and password when prompted. Examples are Google Pay, Apple Pay, M-Pesa and Alipay.
Gift cards	Gift cards as payment methods have become popular in scams. Common examples are iTunes, Google Play, Amazon and Steam gift cards.
Cryptocurrencies	These digital currencies are slowly being introduced as a mainstream means of making payments. Bitcoin is the most common, but others such as DSH, ETH, Ripple, Litecoin and EOS are also popular. In 2019 more than 2900 cryptocurrencies were available.

Scams awareness

Australians have become more scam-savvy since 2009. Through the work of various government agencies, private businesses and the media, the public has a better understanding of scams and where to report them. This is reflected in the increase in Scamwatch reports over the last decade: we received over 160 000 reports in 2019, up from just over 20 000 reports in 2009—a 700 per cent increase in just over 10 years.

The ACCC has evolved in this time and now uses Scamwatch data to help in the fight against scammers. We share intelligence with other agencies and businesses to assist with their disruption efforts. We take action to have scam websites removed and to get scams removed from social media sites. We monitor trends and alert the public to emerging issues. We also engage with the media to provide useful statistics and 'protect yourself' tips that they can distribute through their channels.

Social media has also proven useful in raising scams awareness. Media consumption since 2009 has changed—more people than ever are sourcing their news online or on social media platforms. We harness this by promoting our messages on the Scamwatch Twitter account and ACCC Facebook page, in some cases reaching audiences faster than through traditional media. We also continue to publish and distribute hard copies of our *Little black book of scams* as we realise that not everyone is online.

20 We are not alleging that scammers deliberately target these payment methods, nor that the payment methods are insecure. Rather, we have observed that as new payment methods become popular, scammers adapt their scams to use these popular payment methods.

2.4 What hasn't changed?

At their core, scams involve fraudulent, deceptive and manipulative conduct aimed at gaining a financial benefit from victims. Some scams have remained largely unchanged since 2009. For example, dating and romance scammers are using the same tactics, but have moved to new apps to find more victims.

There aren't many entirely new scams; rather, scams have cleverly adapted over time. Ten years ago, most investment scam reports were about 'get rich quick' seminars and real estate. Bitcoin was publicly released in 2009, leading to a surge in popular interest in cryptocurrency. Now, most investment scams involve cryptocurrency and modern versions of Ponzi schemes. Investment scams have become the scam category with the highest reported losses to Scamwatch, with over $61 million in 2019 (43 per cent of all reported losses).

3. The scams

3.1 Scamwatch in 2019

The ACCC received 167 797 scam reports in 2019, with losses of nearly $143 million. Reports dropped by 5 per cent since 2018, and financial losses increased by 35 per cent.

Investment scams increased by 43 per cent over 2018. For the first time, losses to investment scams were more than double those of the next highest loss category. Forty-two per cent of people who reported an investment scam lost money, with an average loss of $12 350.

Table 5: Scam categories by losses in 2019

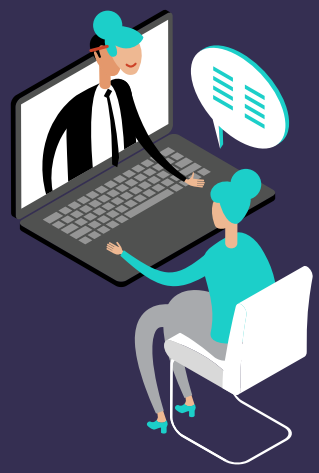
Scam category	Losses	Reports	Reports with losses	Change in losses since 2018
Investment scams	$61 813 401	5 005	2 128 (42.5%)	▲59.1%
Dating and romance scams	$28 606 215	3 948	1 380 (35.0%)	▲16.1%
False billing	$10 110 756	11 255	1 881 (16.7%)	▲83.4%
Hacking	$5 139 414	8 321	509 (6.1%)	▲64.3%
Online shopping scams	$4 845 452	9 953	6 027 (60.6%)	▲47.8%
Remote access scams	$4 836 812	9 019	682 (7.6%)	▲1.6%
Identity theft	$4 311 066	11 373	562 (4.9%)	▲193.0%
Threats to life, arrest or other	$4 250 689	13 375	414 (3.1%)	▲27.3%
Classified scams	$2 816 076	4 958	1 528 (30.8%)	▲19.1%
Inheritance scams	$2 622 355	2 920	67 (2.3%)	▲20.7%

Note: In this report, some tables, such as this one, only present select data. These tables do not include overall totals as the results would not reflect the entirety of the data.

The top three reported scams were phishing, threats to life, arrest or other and identity theft. While Australians made 25 168 reports about phishing in 2019, few people had lost money to these scams at the time of reporting—total losses were $1.5 million. It is likely that many suffered future losses as a result of phishing scams.

Losses to identity theft, false billing and hacking scams increased in 2019. Losses to identity theft scams increased by 193 per cent over 2018. The top loss for identity theft was $800 000 to a phone porting scam.

Losses to false billing scams increased by nearly 80 per cent, and hacking by 64 per cent. These scams have become more effective as scammers deceive people with less direct communication. For example, scammers send fake invoices to businesses anticipating they will pay them without thinking too carefully, and hackers steal login data to access accounts remotely.



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:
$4.3 million

Reports:
11 373

100% of scams have the potential for identity theft

Reports to Scamwatch in 2019

PROTECT YOURSELF:

- Ensure your passwords are strong
- Don't respond to phishing scams
  Know who you are dealing with

The bigger picture

In 2019, Scamwatch received reports with $143 million in losses. Research commissioned by the ACCC tells us that Scamwatch is just one of many places people report scams. Those who experience a scam are more likely to report to their bank than to any other organisation.[21] Overall, only a third of people who respond to a scam go on to report that scam to a government agency.[22]

This year the ACCC obtained scams data from the big four banks and other government agencies to better understand how scams are affecting Australians.

Australians reported losing $634 million to scams in 2019 (combined losses).

Table 6: Losses reported to all agencies and banks

Organisation	Scam losses
Scamwatch	$143 million
ACORN	$225 million
ReportCyber	$236 million
Australian Taxation Office	$2 million
WA Scamnet	$14 million
Big four banks	$237 million
Total	**$634 million[23]**

Government agencies

We expect that people who experience scams will report to different agencies depending on the situation. Through ReportCyber or ACORN, scam reports are triaged and forwarded to local police for further investigation where appropriate. People report to Scamwatch to inform the government about their experience and assist with awareness-raising and disruption efforts.

There is no uniform terminology when it comes to scams. Government agencies and other organisations all use different terms to describe different types of scams, which can make comparing data challenging. We have, however, been able to calculate loss amounts for the top four most costly scams of 2019 in table 7 below.

Table 7: Top four most costly scams across top government reporting portals

Agency	Investment scams	Dating and romance scams	Business email compromise scams	Identity theft scams
Scamwatch	$61.8 million	$28.6 million	$5.3 million	$4.3 million
ACORN	$44.5 million	$18.3 million	$16.7 million	$17.9 million
ReportCyber[24]	-	$25.0 million	$63.2 million	$46.5 million
Total	**$106.3 million**	**$71.9 million**	**$85.2 million**	**$68.7 million**

Banks

ANZ, Commonwealth Bank, NAB and Westpac provided high-level anonymised data about the reports and losses their customers experienced in 2019.

Overall, these four banks received 11 264 reports with $237 million in losses. They also prevented or recovered nearly $230 million from being sent to scammers. The most common scams were generally also the most financially harmful. Business email compromise, remote access scams, investment, and dating and romance scams caused substantial losses to customers across these banks.

21 Roy Morgan ACCC scam survey research 2019.

22 Australian Bureau of Statistics Personal Fraud 2014–15, 4528.0, released April 2016.

23 Duplicate reports have been removed from this total figure.

24 ReportCyber does not have a category for investment scams. The closest match is 'fraud', which had losses of $48 million in 2019, but potentially includes other types of scams as well as investment.

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:
$61.8 million
Combined losses **$126 million**
(Reported to Scamwatch, other government agencies and the big four banks)

Losses from investment scams increased by **59%** from 2018 to 2019

Over **$21 million** was lost to cryptocurrency investment scams in 2019
Reports to Scamwatch in 2019

PROTECT YOURSELF:

Beware of promises of high returns with little to no risk

Always check with a reputable financial adviser before investing

3.2 Scam trends in 2019

Cryptocurrency investment scams

In 2019, reported losses for cryptocurrency scams exceeded $21.6 million from 1810 reports, more than four times those in 2018. Younger Australians (aged 25 to 34) made the most reports.

How it works

Scammers tend to target people who are already interested in investing and cryptocurrencies. As with other investment scams, victims are offered an opportunity to make high returns quickly. They trade in cryptocurrency and often communicate with the scammers on modern platforms such as Discord and Telegram. Victims will find the trading platform suddenly shuts down, the scammers can't be contacted and their money disappears. Some cryptocurrency scams are long running, with the scammers making excuses for delays in withdrawals before 'banning' complaining victims from their discussion forums to prevent their notifying others that the company is illegitimate.

In 2019 an international Ponzi cryptocurrency scam hit Australia. Scamwatch received over 200 reports about USI Tech with losses of $3.3 million, mostly Bitcoin. USI Tech is now known as one of the biggest cryptocurrency scams in the world.

Protect yourself

- Scammers use cryptocurrency because it is hard to trace. Many cryptocurrency brokers have been revealed to be scams and should be avoided.
- Be wary about unsolicited investment opportunities, including by email or online advertising.
- Don't feel pressured to act quickly—take the time to research the offer and talk to a financial adviser, friends or family.
- Diversify your investments—never put all your eggs in one basket.

Celebrity endorsement scams

We received 407 reports about celebrity endorsement scams with over $1 million in losses in 2019. This scam attracted media attention through variants using the name and image of well-known figures.

Many of these scams occur on social media. There is strong community concern in Australia and overseas that social media platforms need to do more to remove scams like this before they can harm users. The ACCC's *Digital Platforms Inquiry final report* made recommendations about scams issues on social media platforms (discussed in section 6 below).

How it works

Scammers use fake celebrity endorsements to add legitimacy to traditional scams such as online shopping and investment scams. They portray celebrities in fake advertisements or news articles to promote skincare products, weight loss pills or investment schemes. Victims are directed to a page with more detail about the scam, often with quotes said to be from the celebrity and a request to pay money for the product or service. This works because people recognise and trust the celebrities. It also gives the impression that the company behind the fake product can afford the official endorsement by high-profile celebrities.

> ***'Cheap pills for slimming - via "shark tank". I fell for it hook, line & sinker'***
> December 2019—$394 loss

CELEBRITY ENDORSEMENT SCAMS

Scammers use the likeness of celebrities to deceive you into parting with your money

Reader clicks on 'article' about celebrity and cryptocurrencies

Registers interest for more information, providing contact details

Called by salesperson (scammer) to invest just US$250 to begin trading

Scammer guides person on how to use website to track trades. Scammer strongly encourages investing more money to access better trades

Investor wanting to withdraw money cannot access the site or make contact with scammer

Celebrity endorsement scams are also used to advertise cosmetics, weight loss pills, skin care products and erectile dysfunction medications.

STATISTICS:

Losses:
$1.04 million

Reports:
407

Reports to Scamwatch in 2019

PROTECT YOURSELF:

Be aware of clickbait ads

Do not invest more money than you can afford

Be careful with products that are free and you just pay for postage — there are likely hidden costs

In 2019, reports followed two distinct patterns: skincare subscriptions and Bitcoin investments:

- Maggie Beer was impersonated in a skincare subscription scam that offered a free product. Victims were required to provide credit card details for postage, but found that they had in fact been signed up to an ongoing subscription costing around $130 a month. These subscriptions were nearly impossible to cancel.
- Mining billionaire Andrew Forrest was impersonated recommending a Bitcoin investment scam. Victims were offered the opportunity to make fast money on a trading platform with a relatively small entry fee (US$250). They were then pressured to invest more and more money until the platform shut down and they lost everything.

In 2019, celebrities started fighting back against these scams internationally. For example:

- in January, Martin Lewis (founder of the MoneySavingExpert website) and Facebook struck an agreement. Mr Lewis agreed to drop his defamation case in the United Kingdom in exchange for anti-scam initiatives from Facebook
- in November, Australian Andrew Forrest published an open letter to Facebook calling for it to remove celebrity-endorsed scams from its platform after one victim was found to have lost $670 000 to a cryptocurrency scam using Mr Forrest's likeness
- also in November, a Dutch court ordered Facebook to pre-emptively remove fake cryptocurrency investment scam ads carrying the image of certain local celebrities and to provide information about the sponsoring companies to police.

Until recently, celebrities could do little to remove scams using their likeness from the internet and social media. These events, and the ACCC's own *Digital Platforms Inquiry final report*, indicate the public expects platforms to do more to remove scam content and protect users.

Protect yourself

- Learn about clickbait and avoid engaging with it.
- Do your own research and consult with independent experts before making investment decisions.
- If a price seems too good to be true, check for hidden catches.

Dating and romance scams

Combined losses to dating and romance scams were $83 million in 2019.

Dating and romance scams evolved in 2019, with scammers using newer platforms to source unwitting targets. Reports of dating and romance scams on social media and mobile apps increased by 4 per cent over 2018, causing $12.8 million in financial losses.

Facebook and Instagram each had over 300 reports of these scams in 2019, with $2.1 million and $975 000 in losses respectively. There were only 23 reports about scams on Viber, but these cost victims over $909 000.

Table 8: Dating and romance scams reported to Scamwatch by contact method in 2019

Contact method	Reports	Losses
Social networking/online forums	1 242	$9 478 028
Internet	807	$9 438 983
Mobile apps	740	$3 327 698
Email	668	$3 278 944
Text message	280	$771 891
In person	87	$717 700
Phone	81	$1 255 971
Mail	20	$337 000
N/A	17	-
Fax	3	-
Total	**3 946**	**$28 606 215**

Dating services are now widely available on a range of platforms, with many offering multi-platform options to users. We analysed the data to further break down where people were meeting dating and romance scammers online and through apps. Table 9 shows the number of reports relating to known dating services (for example, eHarmony, RSVP, Plenty of Fish and Tinder) and those originating on non-romantic platforms (for example, Facebook, Instagram, WeChat and Pinterest).

Table 9: Dating and romance scams originating through dating services vs non-romantic platforms

Contact mode	Dating site	Non-dating site	Unspecified	Total
Social networking/ online forums	483	610	149	**1 242**
Internet	449	303	55	**807**
Mobile apps	327	248	165	**740**

How it works

A scammer contacts a victim, builds a relationship and quickly professes their love. They suggest that the relationship continue on a private channel, shifting victims away from official websites or platforms. In 2019, many scammers moved victims to WhatsApp. The scammer acts in an adoring way, shares personal information and sends small gifts. They often pose as military personnel, foreign aid workers, doctors, nurses or other professionals working remotely. They also commonly pose as widowers with children. The scammer's stories all aim to gain sympathy and trust.

The scammer soon asks for money, gifts or financial details to assist them in a personal emergency. If a victim hesitates, the scammer will use emotional blackmail by threatening self-harm or describing the dire situation they face without the victim's assistance.

Often, scammers have multiple victims and work in networks of professional scammers. They refer to victims as 'clients' and share information about those who have been more willing to pay or easier to exploit.

Protect yourself

- Never send money to someone you have not met in person.
- Be alert to inconsistencies: has your admirer's story changed, or does their description of themselves differ from their photo?
- Do an image search with photos they send and their profile picture (this can be done through Google.com or TinEye.com). Scammers often steal photos off the internet to hide their true identity.
- Don't share intimate photos or videos that could be used to blackmail you in the future.

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:
$28.6 million
Combined losses **$83 million**
(Reported to Scamwatch, other government agencies and the big four banks)

Reports:
3940+

$22 million, or **76%** of all losses to dating and romance scams were lost by women

Reports to Scamwatch in 2019

PROTECT YOURSELF:

Remember if your admirer's story changes — they may not be who they say they are.

3.3 Psychology of scams

Scammers use psychological tools to manipulate victims into believing their stories and handing over their money. Below are some common examples of scam psychology that is used across different types of scams. By sharing this information, we hope to strengthen the Australian public's defence against scammers.

Reciprocity

Reciprocity is a feeling of wanting to 'return the favour'. If someone does something for us, we feel obliged to do something for them in return.

Scammers can take advantage of reciprocity at the beginning of a transaction by offering a small gift, or extending an invitation to an 'exclusive offer'. This creates a feeling of indebtedness, which could lead scam targets to engage with the scammer and offer something valuable in return.

- **Tip:** be wary of accepting gifts or free or exclusive offers.

Foot in the door

We like to be consistent and keep our commitments. Most of us also like to think of ourselves as helpful and polite. Scammers can take advantage of this by getting us to commit to little steps that then escalate.

Trivial first commitments can create a 'momentum of compliance' that induces more significant future commitments. And the initial commitment can be as simple as answering a question. Having answered one question, it would be inconsistent not to answer another one. And so the scammer has their foot in the door with you and starts to ask for more money or more personal information.

- **Tip:** don't feel like you have to be polite to a scammer or make small commitments to do anything.

Door in the face

The 'door in the face' technique involves a scammer making an initial large request, followed up by a smaller request if the initial request is denied.

Because the scammer has made a concession by asking for less than they originally wanted, the scam target can feel obligated to return the favour by agreeing to the smaller request.

- **Tip:** take your time before agreeing to anything—talk to your friends or family first. Remember you can say no, and don't feel like you owe a stranger anything.

Social proof

We are social creatures and we often look to others for cues about the right way to behave in certain situations. This is especially true when we are unsure of ourselves, and when the situation is unclear or ambiguous.

If a scammer tells us a majority of people have signed up for a particular scheme, or even that a growing number of people are signing up, this can make us likely to sign up too.

- **Tip:** don't say yes to an offer just because you think everybody else has. Stop and consider whether it is right for you.

Similarity

We naturally tend to like and trust people who are similar to us. Similarity can be incredibly broad, and is often related to seemingly trivial traits—from sharing a star sign, to sharing a geographical location or a hobby.

Some scammers spend time trying to learn things about us to appear to be like us. Once they've established a similarity, it can have the unconscious effect of increasing our trust in them—and hence we are more likely to agree to their requests.

- **Tip:** remember scammers may gather information about you from social media or other platforms.

Authority

There are many circumstances where we defer to and obey authorities.

Scammers often invoke an authoritative tone or persona in an attempt to make a demand or offer seem more legitimate.

They can invoke authority by pretending to be a rule enforcer (for example, the scammer claims to be from a government department, demanding payment of an overdue bill) or authority due to expertise (for example, a renowned businessman endorsing an investment scheme).

- **Tip:** genuine authorities are unlikely to threaten you. Don't agree to anything when under pressure or feeling threatened. Take your time to seek independent advice.

Sunk costs (throwing good money after bad)

A sunk cost refers to money (or other investments, such as time and effort) that has already been spent and which cannot be recovered. In theory, past sunk costs should not influence future decisions. But in reality we often 'throw good money after bad' because we want to make sure the initial investment wasn't wasted or in vain.

Scammers can take advantage of this by reminding scam targets of all the money/time/effort they've already spent, and promising that the big payoff is just around the corner—after this one last investment.

- **Tip:** if you suspect a situation is a scam, don't make any further payments even if your contact promises you'll get your money back. Seek help first.

Scarcity and urgency

We all suffer from FOMO (fear of missing out) from time to time. If there is a limited quantity of something, or a time limit, this can create a sense of urgency, leading us to act without thinking things through.

Scammers often use scarcity to their advantage—by suggesting that opportunities are only available for a limited time or to a limited number of people—and warning us how awful we'll feel if we miss out. Of course some genuine opportunities are time limited. But by rushing us into acting quickly, scammers can prevent us from properly weighing the costs and benefits or seeking a second opinion.

- **Tip:** take your time and do your research. Remember that offers that seem too good to be true are often scams.

3.4 Payment methods

Scammers are shifting to more modern payment methods, which are often harder to trace than traditional ones. The anonymity of unregulated cryptocurrencies and other real-time payment channels impedes the ability to recover funds or identify scammers. While most people are still using bank payments, Bitcoin and other payment methods now make up the top three ways scammers receive money.

Table 10: Payment methods used to pay scammers by highest loss[25]

Payment method	Losses	Reports
Bank transfers and payments	$69 740 943	6 434
Bitcoin	$19 434 209	1 369
Other payment method	$15 497 414	1 576
Cash	$14 563 504	1 558
Credit card	$9 803 855	6 431
Western Union	$4 145 076	414
PayPal	$2 814 285	1 590
iTunes gift card	$1 831 787	497
WorldRemit	$1 782 373	97
Other gift cards	$1 496 805	636
MoneyGram	$793 238	
Australia Post Load & Go prepaid debit card	$685 344	120
Google Wallet	$258 259	50
Ukash	$5 600	2
Not provided	$21 310	7

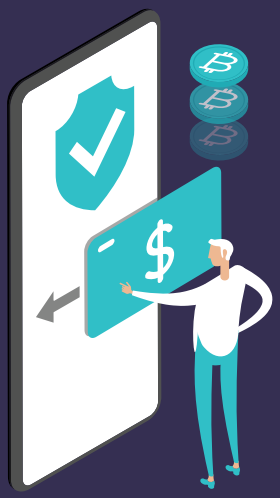
Bitcoin is by far the most popular cryptocurrency used in scams. Sixty-five per cent of scam payments by Bitcoin were investment scams, with $19.4 million in losses.

Other payment methods include those not explicitly included in other categories. The most common are in table 11 and include cryptocurrencies other than Bitcoin (for example, ETH using Ethereum), online game values, online transfer services such as TransferWise, and payment apps such as Apple Pay, Zelle, Beem It and Cash App, to list a few.

Table 11: Most common other payment methods reported to Scamwatch in 2019

Payment method	Losses	Reports
Steam	$632 065	37
Goods/items sent and not paid for	$293 916	112
Phone bill	$280 750	115
TransferWise	$275 845	27
BPAY	$220 877	29
Superannuation funds	$208 953	3
Ria Money Transfer	$201 079	29
Fintech FX	$189 197	35
Cryptocurrencies not Bitcoin	$158 492	17
Payment apps	$146 671	52
Neosurf vouchers	$67 320	99
Skrill	$20 849	22
Cardless cash	$10 450	26
Afterpay	$8 018	38

25 The table only includes payment methods where a financial loss was experienced by the reporter.



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

Losses:
$27 million
reported lost via unusual payment methods

STATISTICS:

$19.6 million lost via cryptocurrencies

$4 million lost via gift cards

$7.2 million lost via money remittance services

Reports to Scamwatch in 2019

BEWARE OF:

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

Government or businesses demanding money by unusual payment methods

Gift cards and scams

Scammers will often request unusual methods of payment from victims to make it more difficult to trace. For the past few years scammers have commonly requested payment by gift cards, such as iTunes cards and Google Play cards. This was particularly prevalent in an ATO impersonation scam. Scammers would contact people saying they had a bill and needed to make payment immediately, or an arrest warrant would be issued. People were told that one way they could avoid arrest was to make a smaller payment via gift cards.

The ATO and ACCC worked closely with supermarkets and department stores to warn the public about this scam and many stores now display warning signs near the gift card section and at the checkout. Some also place a limit on the amount that can be spent on gift cards.

Phone bills were the most common method of other scam payment. This involves fraudulent charges to phone bills and is common in Wangiri scams. These scams are also known as 'one ring and drop' scams, and usually involve an overseas scammer calling a target and hanging up after one ring. If the target calls back, they are routed to a premium rate number and the scammer will try to keep them on the line as long as possible. Some reports in 2019 advised that scammers would let the line connect and say, 'Hello' before hanging up, hoping the victim would call back. The victim only realised they'd been scammed when they received high charges on their next phone bill.

In December 2019 the Mobile Premium Services Code came into effect, which limits third-party charges to $20 monthly.[26] People who wish to spend above $20 must now apply directly with their mobile service provider, protecting them from unauthorised charges for premium mobile services.

3.5 Contact methods

In 2019 there were substantial increases in losses from victims contacted over the internet, in person, over social media and by text message.

Table 12: Contact methods used by scammers by number of reports

Contact method	Reports	Change in reports since 2018	Reported losses	Reports with loss	Change in losses since 2018
Phone	69 522	▼-16.5%	$32 582 135	2 776	▲7.4%
Email	40 277	▼-2.2%	$28 355 839	3 631	▲12.0%
Text message	27 894	▲9.0%	$3 035 675	1 222	▲39.5%
Internet	11 776	▲11.5%	$31 631 553	6 029	▲86.7%
Social networking/ online forums	8 194	▲20.0%	$22 095 119	3 763	▲40.1%
Mail	3 995	▼-17.3%	$2 412 451	376	▲23.8%
Mobile apps	2 912	▲28.6%	$6 911 184	1 135	▲37.5%
In person	2 157	▲15.8%	$15 806 850	831	▲68.3%
Fax	287	▲34.7%	$53 196	13	▲24.7%

Social media

Phone has been the primary contact method for scammers since 2011, but scammers are increasingly moving online through the internet, apps and social media.

Scams using social media platforms are diverse. The most common scams are on popular platforms such as Facebook, Instagram, LinkedIn and online dating platforms. Specific scams on these platforms include online shopping scams, dating and romance scams, investment scams and pyramid schemes.

The Loom pyramid scheme was distributed over Instagram and WhatsApp in 2019, causing over $8000 in reported losses to 170 victims. Disguising the scheme with a spiritual theme, Loom asked

26 Communications Alliance Ltd https://www.commsalliance.com.au/Documents/all/codes/c637.

people to pay $300 and recruit friends and family to do the same. Scammers lured victims with the promise of an individual 'cash out' of $2400.

Text messages

Losses to text message scams increased by 40 per cent ($96 821) in 2019, despite there being only 9 per cent more reports of them. Many of these were phishing scams impersonating banks, myGov, Australia Post and JB Hi-Fi.

Text message phishing scams were most financially damaging when impersonating banks. One particularly damaging phishing scam impersonated NAB with a legitimate-looking link for people to click on. The scam harvested victims' personal information, including internet banking details. Australians lost almost $20 000 to this scam in 2019, but the personal data was worth more to the scammers.

Mobile messaging apps

We received many reports of scammers and victims communicating on mobile messaging apps in 2019. Scammers frequently used Facebook Messenger and Viber to initiate contact with targets. In contrast, WhatsApp was used more as a secondary form of communication; scammers would meet victims on another platform and suggest the conversation move to WhatsApp. We are monitoring this trend in 2020.

3.6 Scams reported to other Commonwealth agencies

We obtained scam data from ACORN, ReportCyber, the ATO, Services Australia, ACMA and the Office of the Australian Information Commissioner (OAIC). While these agencies don't use the same scam categories as Scamwatch, there are many similar trends in reported scams.

ACORN

Until 30 June 2019, ACORN was a central system for reporting cybercrimes including online scams. Some of these were referred to Australian law enforcement agencies to investigate potential crimes.

ACORN received 25 416 scam reports with losses of $224.5 million in the first half of 2019. The top five scams were investment, dating and romance, online identity theft, online shopping and Nigerian scams.

ReportCyber

ReportCyber replaced ACORN as the Australian Government's online cybercrime reporting portal in July 2019.

It received 28 950 scam reports with $235.9 million in losses in the second half of 2019. The highest losses were due to business email compromise scams, with losses of $63.2 million.

Australian Taxation Office

In 2019 the ATO received 107 828 scam reports. Of those, 639 victims lost $2.1 million to scammers. This was a decrease in reports (6 per cent) and losses (25 per cent) from 2018.

The ATO observed concerning new scam trends in 2019. The first was that scammers started to spoof genuine ATO phone numbers, adding an air of authenticity to their scams. The ATO liaised with telecommunications providers to stop these scam calls and increased the scams awareness information it provided to taxpayers.

The ATO also observed scams moving away from gift card payments to cardless cash. Cardless cash allows people to withdraw money from an ATM using a secret code instead of a physical card, and to arrange for others to collect the cash on their behalf. ATO scammers directed victims to share cardless

cash codes so they could withdraw funds from the victims' accounts. Once withdrawn, the cash could not be traced or recovered.

Services Australia

Services Australia verified 4790 scam reports in 2019. Most reports involved loss of personal information and came from people aged 65 and over.

In 2019 the agency announced a three-year partnership with IDCARE to better support victims of scams and identity theft. In the first year, the agency referred 1526 customers to IDCARE for specialised support.

The agency has noted an increase in myGov phishing scams since 2018. These are usually sent by email, text message or social media claiming to be from a legitimate government agency, such as Services Australia or myGov. These scams ask the target to complete an online form or provide personal information including identification documents to a fake website. Scammers harvest this personal information, including credentials, to apply for government benefits or complete fraudulent tax returns.

Note: Scamwatch has also observed a rise in scammers impersonating myGov, Services Australia and the ATO. In 2020 these scams have increased, especially in the context of the COVID-19 pandemic.

Australian Communications and Media Authority

ACMA manages the spam intelligence database and receives complaints about scams (mainly phone scams). The most common scam in 2019 was the NBN robocall scam, with 4548 reports.

The top five scam categories reported to the ACMA were computer virus and tech support scams, Do Not Call Register scams, accident claim scams and Chinese authority robocalls.

Office of the Australian Information Commissioner[27]

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 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 shows concerted efforts by cybercriminals to access the personal information of Australians. In the first six months of 2019 the OAIC received 460 notifications, with malicious or criminal attacks accounting for more than 60 per cent of breaches.[28] Data breaches usually involved the personal information of 100 or fewer individuals.

27 Information in this section was obtained from data publicly available on the OAIC website.

28 Information on the OAIC website is current to June 2019 at time of report.

4. The people

People are affected by scams in different ways. This section outlines our findings on the people who report scams: the targets, the victims and the observers.

4.1 Who reports to Scamwatch?

Roy Morgan research

In June 2019 the ACCC commissioned independent research into how many Australians are affected by scams, including whether they had reported the incident and, if so, where they reported it. The research found that nearly one in five people had experienced a scam in the past five years, with one in four people affected more than once.

Sixty-seven per cent of people who identified as a victim in the survey reported the scam to an organisation or government agency. Consequently, one-third of people who experienced a scam did not report it to any agency or organisation, which demonstrates how high the 'unknown losses' to scams are. The most common government reporting portals were Scamwatch (13 per cent), the police (11 per cent) and ACORN (5 per cent).

Interestingly, people reported to their banks more than any agency, police department or private organisation. In 2019, Scamwatch placed greater emphasis on advising people to report to their banks before doing anything else, to prevent further financial harm.

4.2 Demographics

Not everybody who reports a scam tells us their age, gender or location, but those that do provide us with valuable insights into how scams affect different demographics. This allows the ACCC and other government agencies to target disruption and awareness-raising efforts.

Age

In 2019, people aged 65 and over made the most reports to Scamwatch, followed by those aged 25 to 34. However, neither of these age groups experienced the highest losses—those were reported by people aged 55 to 64, who lost nearly $30 million. This is likely due to this group's accumulated wealth, coupled with their interest in investment opportunities.

Of the total of 167 797 Scamwatch reports, 19 783 involved lost money, with losses totalling nearly $143 million.

Young people were more likely to report a scam that included a financial loss. For people under 18, 26 per cent of all reports involved a financial loss. This age group lost $471 595, an increase of over 170 per cent from 2018.

Table 13: Number of Scamwatch reports by age group (2019)

Age group	Number of reports	Reports with loss	Percentage of total reports in age group	Losses	Percentage change in losses from 2018
Under 18	1 645	431	26.2%	$471 595	▲176%
18–24	10 357	2 473	23.9%	$4 677 469	▲46%
25–34	21 823	3 570	16.4%	$19 032 736	▲51%
35–44	20 294	3 241	16.0%	$26 062 082	▲82%
45–54	19 810	2 791	14.1%	$26 868 460	▲39%
55–64	19 655	2 120	10.8%	$29 866 466	▲20%
65 and over	25 149	2 219	8.8%	$23 613 316	▲10%
Not provided	49 064	2 938	6.0%	$12 313 448	▲10%
Total	**167 797**	**19 783**	**11.8%**	**$ 142 905 572**	**▲34%**

Location

With the largest population of all Australian states, it isn't surprising that New South Wales residents made the most reports and suffered the highest financial losses in the country. Investment scams caused the most financial damage in this state, with $12.3 million lost in 2019. More people lost money to online shopping scams, but these losses were smaller. The median loss to online shopping scams by people in New South Wales was $161.

Although Victoria has a larger population than Queensland, it made fewer reports and lost less money to scams in 2019. Queensland scam victims parted with more money per scam than Victorian victims. Investment scams, followed by dating and romance scams, were the most financially damaging in both these states: Victoria lost $11.2 million to these scams, and Queensland $17.5 million.

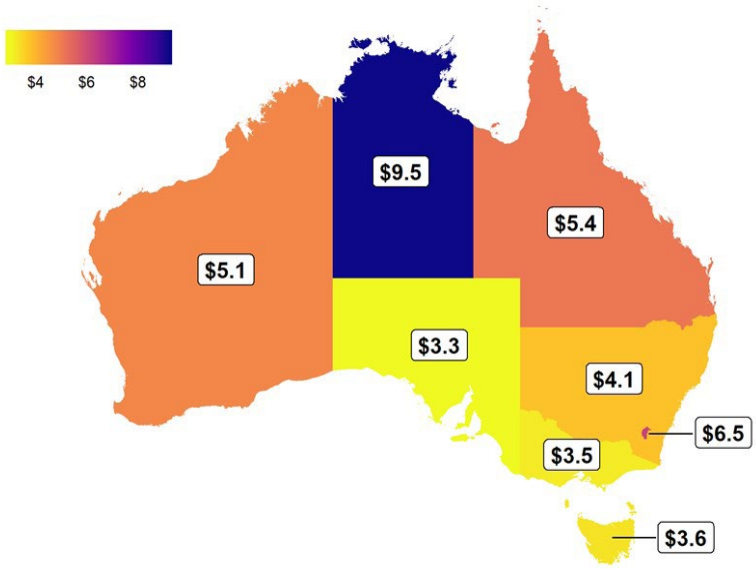
Like many other states, Western Australia lost the most money to investment scams ($7.3 million). It was one of only two states that did not lose money to every scam type in 2019; while Western Australians reported ransomware and psychic scams, they did not lose any money to them.

Tasmania was less affected than other states. Based on population, Tasmanians made the lowest number of reports and suffered the lowest financial losses in the country. Tasmania's highest losses were to investment scams at just under $1.2 million, but this was the lowest state loss to investment scams in Australia. Tasmania also had the most 'no loss' scams in the country, with no reported losses for jobs and employment, ransomware, rebate and scratchie scams. Tasmania was the only state to report zero psychic/clairvoyant scams in 2019.

South Australians lost $2.6 million to investment scams, with this scam type again causing the highest losses in the state. The second highest losses in South Australia were from false billing scams, with losses of almost $462 000. Reported losses to fake charity scams rose by over 1000 per cent to $14 000 in 2019.

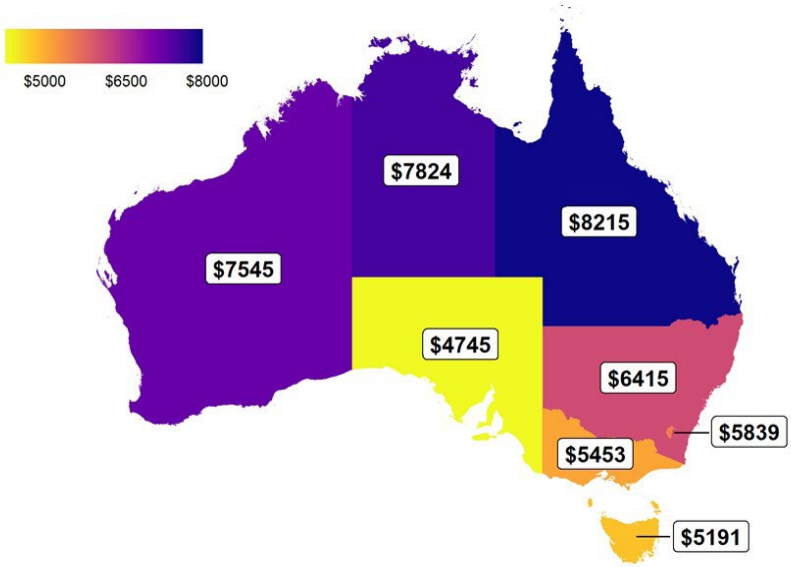
The Australian Capital Territory and Northern Territory differed from every other Australian jurisdiction as dating and romance was the top loss category in each. The Australian Capital Territory lost $1.1 million to these scams in 2019, and the Northern Territory $1 million.

Figure 6: Amount lost to scams per capita[29]



Heat maps illustrate the different ways that scams affected the states in 2019. The Northern Territory lost the most money to scams per capita, which is concerning as it had the lowest number of scam reports in Australia. The Australian Capital Territory lost the second highest amount to scams per capita, despite also reporting fewer scams than many other states. South Australia, Tasmania and Victoria had the lowest per capita losses in the country.

Figure 7: Average value of scams with losses in each state[30]



The average value of each scam tells a different story. Queensland residents reported the highest losses to scams, with an average of $8000. The Northern Territory and Western Australia also experienced high average losses. South Australia reported the lowest average losses at under $5000. However, while the average loss was under $5000, losses for that state ranged from $15 to $500 000.

29 Total amount lost to scams per state divided by latest state population estimate (Australian Bureau of Statistics).

30 Total amount lost to scams by state divided by number of scam reports that included a loss.

Table 14: Reports by location[31]

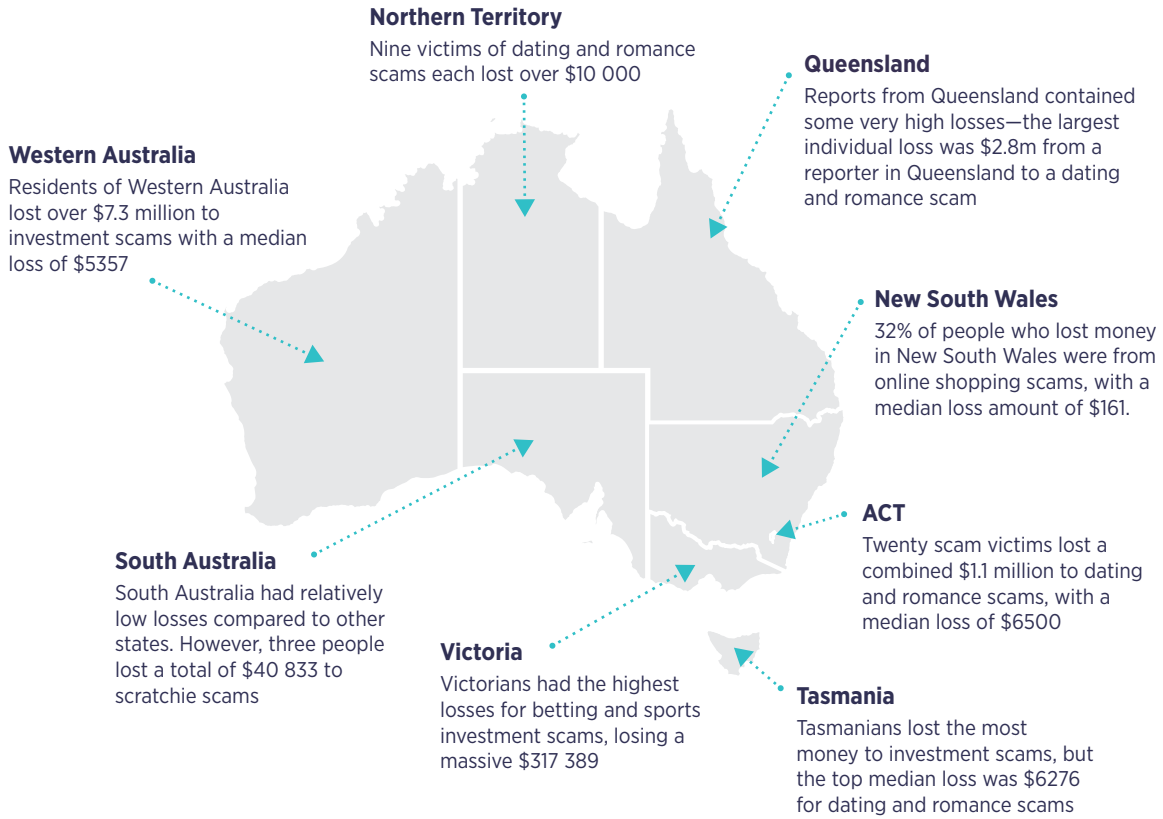
Jurisdiction of report	Reports	Reports with loss	Losses
NSW	46 061	5 179	$33 222 164
Vic	36 739	4 180	$22 794 040
Qld	33 042	3 324	$27 307 132
WA	17 378	1 764	$13 308 657
SA	12 467	1 215	$5 764 794
Tas	3 270	375	$1 946 555
ACT	5 064	473	$1 762 033
NT	1 820	297	$2 323 763
Overseas	6 451	2 291	$18 186 957
Not provided	5 505	685	$15 289 477
Total	**167 797**	**19 783**	**$142 905 572**

Case study 1: Overseas reports—Innovamine investment scam

Innovamine pretended to be a cloud mining company that could mine Bitcoins using pooled resources, splitting the profits. In fact, Innovamine was a Ponzi scheme that crashed in July 2019. Reported losses to this scam were over $7 million.

Innovamine operated out of Ukraine, but as the company was registered in Australia many overseas victims reported to Scamwatch. Eighty-two per cent of reports were from overseas, with losses of $5.9 million.

Figure 8: Scam losses by state and territory



31 While Scamwatch is intended for use by people in Australia, we do receive reports from people overseas. We generally do not include overseas reports unless there is a connection to Australia, such as the scammer being located or registered in Australia.

Table 15: State and territory populations and reported losses

State	Percentage of Australian population	Percentage of reports made to Scamwatch	Percentage of total reported losses	Reported losses
NSW	31.9	27.5	23.2	$33 222 164
Vic	26.0	21.9	16.1	$22 794 040
Qld	20.1	19.7	19.1	$27 307 132
WA	10.3	10.4	9.3	$13 308 657
SA	6.9	7.4	4.0	$5 764 794
Tas	2.1	1.9	1.4	$1 946 555
ACT	1.7	3.0	1.9	$2 762 033
NT	1.0	1.1	1.6	$2 323 763

4.3 Who is targeted by scams?

Scamwatch data provides insights into the key characteristics of Australians that are 'typically' affected by scams.[32]

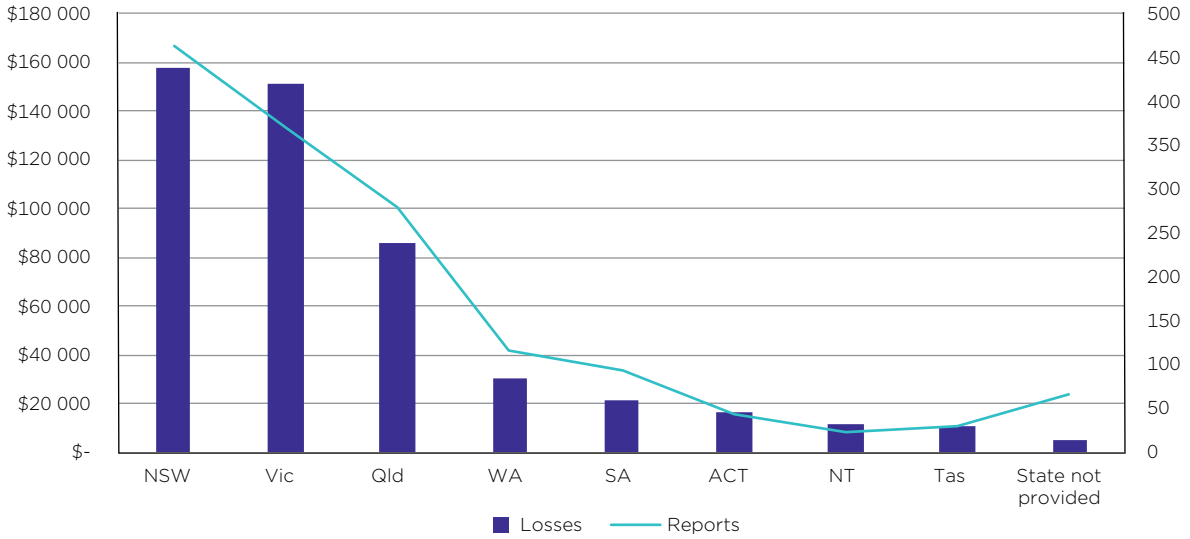
Young people

The 'typical' young person experiencing scams is aged 24 or under, living in New South Wales and looking to buy electronic products online.

In 2019 Scamwatch received 12 002 scam reports from people in this age group. Online shopping scams most commonly resulted in financial harm, with losses of $620 550. Many scams occurred on eBay, Gumtree and Facebook Marketplace, with most involving people not receiving payment for goods they were selling, or paying for goods they never received. Products commonly sought by young people are phones, AirPods and tickets to concerts or festivals.

Threats to life, arrest or other scams caused the highest financial losses for people under 24, at $1.8 million. Chinese authority scams affected the international student community severely in 2019, with over $1.1 million lost. Young people in Victoria suffered around three times the losses of other states.

Figure 9: Online shopping scam reports and losses for under 24 year olds



32 By 'typically', we mean where a large number of reports demonstrated the prevalence of the particular type of scam affecting a certain segment of the population.

Online shopping and classified scams can target both buyers and sellers. People selling items can be tricked through fake payments and overpayment scams. On the other hand, buyers can be scammed by offers of items that do not exist, or are worthless or counterfeit.

Case study 2: Fake PayPal emails

Jaiden wanted to sell his old laptop. He advertised it online for $500 and received an offer for the full asking price. The buyer wanted to use PayPal; Jaiden was happy with this as PayPal is a safe way to send and receive money online.

Jaiden received an email telling him his PayPal account had been credited $1000, so he contacted the buyer straight away to say they had transferred too much money. The buyer said they paid extra for postage and Jaiden could just send any leftover money back to them. Jaiden thought this made the buyer more trustworthy, and did not check his PayPal account. He posted the laptop to the buyer and then transferred the leftover money.

When he went to his account, he found there was no payment. He contacted PayPal and they told him that the email he received was a scam. The buyer blocked him on social media. He could not stop the courier. Jaiden lost his laptop, $60 in courier fees and the $440 he had 'refunded' to the buyer.

Protect yourself

- If you see something at a very low price, be cautious.
- Check out the seller:
  - Read independent reviews from people that have actually bought something from them.
  - Don't believe testimonials they've posted themselves.
  - Find out whether they have an established social media presence or a brand-new profile.
- Don't use unusual payment methods—you should be suspicious of payment requests for Bitcoin, cardless cash, eVouchers and gift cards.
- If you're unsure, check with someone you trust.

Women

The 'typical' female scam victim is aged 45 to 54, living on the east coast of Australia and using social networking sites to find friends or a partner. New South Wales women made the most reports, but the highest losses were from Queensland.

Scamwatch received 2167 reports of dating and romance scams from women in 2019, with $21.5 million in losses. Although males made 43 per cent of reports about these scams, women reported 75 per cent of the financial losses.

Scammers are increasingly using non-traditional apps to target unsuspecting victims. In 2019 Scamwatch saw an increase in reports of dating and romance scams originating on Google Hangouts, Words With Friends, Facebook and Instagram. This is concerning as people may not expect scammers to target them in these forums. Women lost $7.2 million to scams on these apps alone.

Protect yourself

- If you're interacting online with someone you've never met, consider the possibility that it's a scam.
- Don't send money to somebody you haven't met in person.
- Never give your personal information to anybody you haven't met in person, including financial details and intimate photos.

'I'm not a stupid woman and I would never have described myself as being gullible, but I was drawn into an elaborate web of lies and deceit and once in there it was impossible to escape.'
February 2019—$250 000 loss

Table 16: Women and scam type with highest losses

Age group	Losses for age category	Scam type with highest losses	Age group's percentage of total losses
Under 18	$86 721	Online shopping scams	0.1%
18–24 years	$2 134 252	Threats to life, arrest or other	3.6%
25–34 years	$6 093 404	Investment scams	10.6%
35–44 years	$8 554 690	Investment scams	14.8%
45–54 years	$15 333 216	Dating and romance scams	26.6%
55–64 years	$15 076 498	Dating and romance scams	26.1%
65+ years	$10 378 776	Investment scams	18.0%
No age provided	$5 964 811	Dating and romance scams	
Total	**$63 622 368**	**Dating and romance scams[33]**	**100.0%**

Men

The 'typical' male scam victim is 35 to 44 years old, living in New South Wales and investing in cryptocurrency scams.

This group lost a total of $17 million to scams in 2019, which constituted 24 per cent of the $72 million in losses for all men who provided an age. The next highest losses were to men aged 55 to 64, who reported losses of $14.7 million. Nearly $12 million of that was lost to investment scams, with 29 per cent of those losses coming from New South Wales. Almost one-fifth of these scams involved cryptocurrency.

> ***'I saw this ad on Facebook with reviews saying 'easy way to make money at low risk and great rewards every two weeks'... I don't know what to do because I saw a lot of people's reviews saying the same story of how they lost money'***
> February 2019—$310 000 loss

Table 17: Top five scams by loss for 35–44 year old males

Scam type	Losses	Number of reports	Percentage of total losses for age group
Investment scams	$11 926 482	518	69.6%
False billing scams	$1 735 434	674	10.1%
Hacking	$720 395	317	4.2%
Dating and romance scams	$696 365	216	4.1%
Identity theft	$439 350	856	2.6%

Protect yourself

- Don't invest more money than you can afford to lose.
- Avoid investment opportunities that promise no risk or high returns.
- Do your research, especially if investing in cryptocurrency.
- Don't be pressured into making hasty decisions.

33 Total losses to dating and romance scams by women was $21.5 million.

Older Australians

Remote access scams affect older Australians more than any other age group. The 'typical' scam victim is 65 or over, from New South Wales and being deceived by scam phone calls claiming to be from NBN Co.

In 2019 people aged 65 and over lost more than $2.5 million dollars to these scams. While they lost more money to other scams overall, older Australians were more likely than any other group to lose money to remote access scams.

Case study 3: Telstra remote access scam

When Geoff answered the phone he didn't expect to hear that there was a problem with his computer. But he had been talking to Telstra the day before and there were technicians in the neighbourhood. The caller told Geoff they needed to clean up his computer because hackers had tried to access it. The caller told Geoff what to type into his computer so that he could secure it remotely.

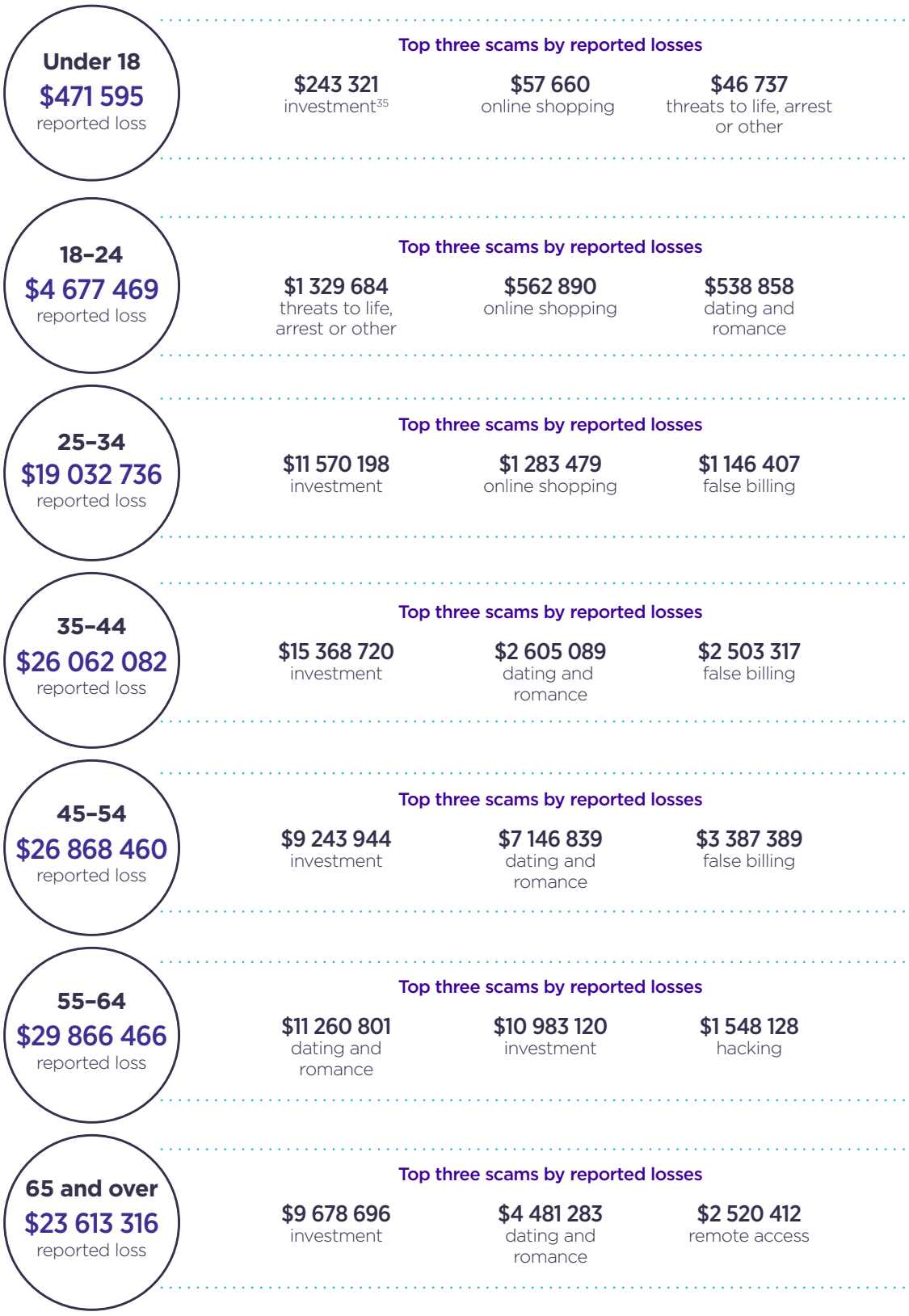
The caller said the hacker was probably trying to access Geoff's bank account, so he got Geoff to log into internet banking. The caller then did something that made Geoff's screen go blank and said he would fix it. However, while Geoff was distracted the caller was transferring money around and eventually transferred $2000 from Geoff's bank to another account. Geoff only realised when he was talking to his bank the next day.

Protect yourself

- Never give someone who contacts you out of the blue remote access to your computer.
- If you receive an unexpected call to fix your computer remotely, even from a trusted company, hang up the phone.
- If you feel rude suddenly hanging up, write down a polite but firm phrase you are comfortable using to end potential scam calls and keep it near the phone. For example, "I haven't asked you to call me and I'm hanging up now", or, "I am not interested and am hanging up now. Please do not call this number again".
- Maintain your computer's firewalls, passwords and antivirus protection. Make sure you research the best software for your computer and only buy from a reputable supplier.

4.4 Which scams are affecting your age group?

Figure 10: Top three scams by reported losses for age ranges[34]



34 Reports which did not provide an age are not included in this graphic.

35 This total includes one report with a loss of $200 000, which is unusual for this age group.

4.5 Indigenous communities

In 2019, Indigenous consumers reported 2767 scams with over $2.1 million in losses. While there were more reports than in 2018, losses were 30 per cent lower.

Investment scams incurred the highest financial losses for Indigenous communities, similarly to the rest of the population. Interestingly, for all scam types, the age group incurring the highest losses was younger for Indigenous Australians compared with non-Indigenous Australians. Indigenous people aged 35 to 44 incurred the highest losses of any age group; for non-Indigenous Australians, the highest losses were reported by people aged 55 to 64.

Figure 11: Top five scams by reported loss by Indigenous consumers

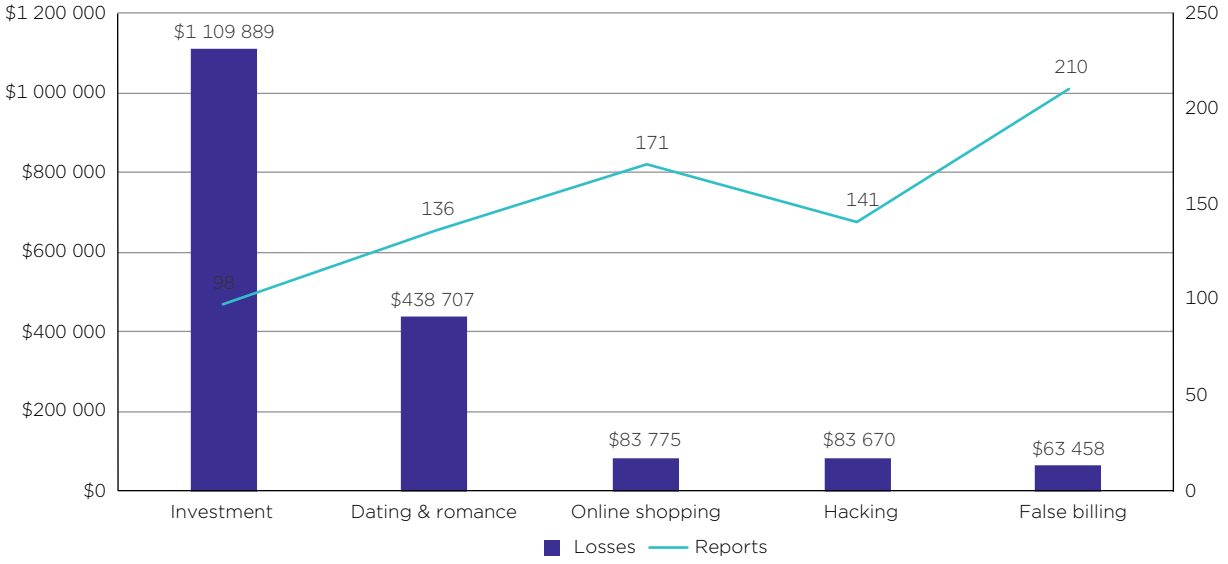


Table 18: Breakdown of age ranges in Indigenous reports

Age group	Reports	Reports with losses	Losses
Under 18	50	15 (30.0%)	$217 004
18–24	311	76 (24.4%)	$136 206
25–34	621	87 (14.0%)	$280 892
35–44	457	99 (21.7%)	$659 470
45–54	365	61 (16.7%)	$259 964
55–64	306	41 (13.4%)	$476 368
65 and over	182	16 (8.8%)	$12 653
Age not provided	475	39 (8.2%)	$65 801
Total	**2 767**	**434**	**$2 108 358**

Case study 4: Dating and romance scam from an Indigenous victim

Cheryl joined a dating platform. She got a message from a man interested in her quite quickly. Rodney, Cheryl's admirer, suggested they move off the platform to take their relationship further. Rodney told Cheryl he had plenty of money overseas from his late wife. He wanted to use it to come and see Cheryl.

Rodney said that he and Cheryl should split the cost of the flights as a sign they trusted each other. Cheryl sent the money to Rodney. Rodney introduced Cheryl to his elderly mother over the phone as a way of getting to know him better, and they spoke a few times. Rodney then asked Cheryl for money for his mum's hospital appointment, vowing to repay her once he had cashed a cheque. He even sent her a copy of the cheque for proof. Cheryl sent the money.

Cheryl hasn't heard from Rodney in a while; the last time was when he was at the airport ready to catch his flight to see her. Cheryl sent over $10 000 to Rodney in the course of the relationship, and he has not repaid any of it.

Indigenous people from the Australian Capital Territory represent around 1 per cent of all Indigenous Australians. However, they were the victims of nearly 5 per cent of scams reported by Indigenous people in 2019. Indigenous reports from New South Wales, South Australia and Victoria were all proportionally higher than their state's Indigenous population.

Worryingly, while Indigenous Victorians made up only 12.5 per cent of reports, they suffered the second highest Indigenous losses in the country at $344 153.

National Indigenous Consumer Strategy

The ACCC continued the National Indigenous Consumer Strategy (NICS) National Project (Too Good to be True) throughout 2019. Our outreach activities included both NICS-directed scam messaging, as well as more focused scam messaging based on advice received from individual communities, especially Palm Island.

The ACCC is part of the Palm Island Settlement Response Committee for the impending Palm Island Class Action settlement. We have been working with recipients to help them to identify scam conduct before they fall victim. For example, we spoke with a women's group on Palm Island about dating and romance scams. We educated the women on what these scams are, how to identify them and how to make informed decisions.

The ACCC is the current Chair for NICS. As the COVID-19 pandemic has resulted in the ACCC and other NICS regulatory office members suspending physical outreach visits to Indigenous communities, we have deferred the implementation of the 2020–2022 NICS Action Plan to assist members in re-prioritising resources due to COVID-19. NICS will extend its 2017–2019 Action Plan for the calendar year 2020 and will continue its broader suite of work to include scams messaging to Indigenous communities, albeit by way of a non-physical platform.

Your Rights Mob

The ACCC leverages social media to provide timely messaging to Indigenous consumers, including scams information, through our Your Rights Mob Facebook page. This platform also encourages and facilitates reporting and discussion among Indigenous consumers about scam conduct.

Table 19: Location of Indigenous people reporting to Scamwatch[36]

State	Reports	Losses	Percentage of total reports from Indigenous reporters	Percentage of Australian Indigenous population[37]
ACT	106	$71 378	4.6%	0.9%
NSW	794	$604 160	34.8%	33.3%
NT	138	$60 850	6.1%	9.5%
Qld	544	$332 843	23.9%	27.7%
SA	158	$28 536	6.9%	5.3%
Tas	58	$106 379	2.5%	3.6%
Vic	285	$344 153	12.5%	7.2%
WA	196	$79 102	8.6%	12.6%
Total	**2 279**	**$1 627 401**	**100%**	**3.3%**

4.6 Diverse communities

English as a second language

In 2019 people with English as a second language made 7777 reports, with $13.7 million in losses.

As with the broader population, communities where English was a second language reported the highest losses to investment scams, with dating and romance scams coming in second. People were more likely to lose money to online shopping scams than any other scam type, with 64 per cent experiencing a loss.

Table 20: Top 10 scams by loss for people with English as their second language

Scam category	Reports	Reports with losses	Losses
Investment scams	294	170 (57.8%)	$5 276 031
Dating and romance scams	356	103 (28.9%)	$2 685 141
Threats to life, arrest or other	689	102 (14.8%)	$1 723 501
False billing	418	120 (28.7%)	$623 930
Pyramid schemes	28	12 (42.9%)	$526 844
Remote access scams	305	33 (10.8%)	$500 046
Classified scams	254	112 (44.1%)	$397 231
Phishing	879	43 (4.9%)	$317 325
Unexpected prize and lottery scams	362	36 (9.9%)	$277 911
Online shopping scams	656	422 (64.3%)	$275 873

Scams affecting CALD communities

Particular scams target culturally and linguistically diverse (CALD) communities. In some cases, the scammers are part of the communities that they target.

36 Table only includes reports from Indigenous Australians who provided state/territory information.

37 Australian Bureau of Statistics Estimates of Aboriginal and Torres Strait Islander Australians 3238.0.55.001, June 2016. https://www.abs.gov.au/ausstats/abs@.nsf/mf/3238.0.55.001.

GOVERNMENT IMPERSONATION SCAMS

Scammers impersonate government agencies and other authorities to threaten you

Scammers call you impersonating a government department, police or overseas authorities

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

Chinese Authority scams caused the highest losses of all government impersonation scams in 2019

STATISTICS:

Over:
$4.3 million
reported lost

1172 reports of Chinese Authority scams **$2 million** lost in 2019

Reports to Scamwatch in 2019

PROTECT YOURSELF:

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

Chinese authority scams

Chinese authority scams emerged in 2018, specifically targeting Mandarin-speaking people in Australia. In 2019 reports of this scam dropped by 36 per cent, but losses increased by 40 per cent to over $2 million.

Victims include Chinese students, recent immigrants and longer term residents of Australia. Most scams were robocalls, with a spike in parcel delivery scams in 2019. The caller would ask the victim to call back urgently and tell them there was a package in their name containing contraband. The victim was then transferred to 'Chinese police' to negotiate the situation to avoid arrest or deportation, usually by transferring large sums of money. This scam continues to be a problem in 2020, and has adapted to the COVID-19 crisis to manipulate money from victims.

These robocall scams were also sent en masse to the broader Australian public. As non-Mandarin speakers could not understand the message, they did not respond.

> ***'The scammer claimed they are the police from Shanghai, and said that I am laundering money. I need to keep it secret or I will go to jail.'***
> March 2019—$10 000 loss

Sri Lankan flights scam

In 2019 Sri Lankan people in Australia were targeted by a scammer purportedly selling discounted flights and accommodation, losing $338 464. Many reports stated that the scammer was known to the victim's community, and that friends or family had introduced them to the scammer. Such 'affinity' scams are not unusual in close communities. The scam extended across Australia, indicating far-reaching contacts within this community.

Table 21: State/territory residence of reports for Sri Lankan flights scams

Reporter residence	Reports	Losses
NSW	20	$185 144
Vic	4	$66 180
Qld	3	$64 640
WA	2	$4 600
ACT	1	$4 900
Not provided	3	$13 000

▶ Case study 5: Sri Lankan flights and accommodation scam

Kasun's friends told him about a man they'd bought flight tickets from. The man told Kasun he could get tickets at a staff discount, so it made them cheaper. Kasun paid $8100 for tickets for him and his family to travel to Sri Lanka.

When it was getting close to the holiday Kasun realised he did not have tickets for the flights. He called the scammer, but could not get in contact with him. He contacted the travel agency the scammer was representing, but they told him the tickets had been issued to someone else.

Kasun was left without flights and without his money. Kasun heard that this had happened to many people in his community, including the person who introduced him to the scammer.

Other scams affecting CALD communities

AMES Australia provides support and services to new migrants to Australia. In 2019 AMES observed the following key scams affecting CALD communities:

- ATO impersonation scams: Scammers make calls that are intimidating and hard to identify as false, as the victim has limited experience with the Australian Government
- Wangiri scams: Scammers call from overseas numbers. It is not unusual for friends and family to call from overseas, and the victim will be keen to return the call
- charity scams: Known individuals elicit money from community members for a 'good cause' and then take off with the money.

4.7 The impact of scams

Financial loss is only one of the effects of scams. Victims also face emotional distress and lose time and energy to come to terms with, and extricate themselves from, a scam. Studies have shown that victims of scams share many of the same devastating outcomes as those who experience violent crime, including self-harm in some cases.[38] Other effects may include lack of self-confidence and problems with friends and family. Older victims of scams may experience reduced independence if family members limit their ability to access their money and make financial decisions for themselves.

The ACCC's research has found that almost 20 per cent of scam victims did not tell anyone what had happened.[39] Reasons included being too embarrassed and feeling shame about the experience. Some people also indicated the matter was private and they didn't want to tell people.

It is important that people talk about scams. Most people find out about scams through word of mouth, and many suspect they're falling prey to a scam long before they tell anyone. In 2019 Scamwatch heard from many scam targets who avoided becoming victims simply because they told someone about their experience, and that person advised them that it sounded like a scam. By reducing the stigma surrounding scams, we can help more people learn to identify and avoid them.

Scams are changing. They are more insidious, losses are higher and identity theft matters more. They take time, money and energy to resolve. Identity theft is becoming more common and it's estimated that, on average, victims spend 22 hours repairing the damage.[40] Scammers take out loans, phone contracts and credit cards in victims' names to obtain a financial benefit. The aftermath of such scams can be long lasting and cause financial devastation. On top of this is the ongoing stress experienced by victims.

Scamwatch reports help us find out about new scams and tell others, to prevent them falling victim too. We use reports to tweet warnings quickly, and inform the media about scams people need to be aware of. We rely heavily on reports to understand what's happening in Australia. People who report scams help us disrupt scammers, and reduce the likelihood that one in five people will fall victim to a scam in the next five years.

38 M Button, C Lewis and J Tapley, 'A better deal for fraud victims', Centre for Counter Fraud Studies, London, 2009.

39 Roy Morgan ACCC scam survey 2019

40 P Jorna, K Norman and RG Smith, *Identity crime and misuse in Australia: results of the 2018 online survey*. 2020. Statistical Report 19. Canberra: Australian Institute of Criminology http://aic.gov.au/publications/sr/sr19.

5. The businesses

Businesses made 5904 reports to Scamwatch, with losses of $5.3 million. While this was a 1 per cent increase in reports from 2018, losses dropped by 27 per cent. Businesses that sustain substantial losses from scams are likely to report the matter directly to police and/or their banks, which could explain the drop in reports to Scamwatch. For the 462 businesses that did lose money, the average loss was $11 398.

Businesses, especially small to medium-sized businesses, face all the same scam risks as individuals. However, several scams specifically target businesses. The most common of these are false billing and phishing scams. Business email compromise scams also continue to affect industry; while we generally classify them as a subset of false billing scams, business email compromise scams are reported across various scam categories.

Table 22: Top scam categories affecting businesses

Scam type	Number of reports	Reports with loss	Losses
False billing	1 264	193	$2 578 787
Investment scams	76	20	$1 183 488
Identity theft	299	23	$329 776
Hacking	320	16	$297 464
Phishing	795	19	$201 998

Scam reports from businesses were mostly from small or micro businesses, although many didn't report the business size. Medium businesses reported the highest losses, but micro businesses experienced the largest number of scams resulting in a financial loss.

Table 23: Breakdown of scams by business size

Business size	Number of reports	Reports with loss	Losses
Micro (0–4 staff)	1 699	155 (9.1%)	$1 359 177
Small (5–19 staff)	1 496	132 (8.8%)	$1 047 827
Medium (20–199 staff)	992	100 (10.1%)	$1 614 946
Large (over 200 staff)	425	28 (6.6%)	$232 330
Size of business not provided	1 292	47 (3.6%)	$1 011 624
Total	**5 904**	**462 (7.8%)**	**$ 5 265 904**

5.1 Business email compromise scams

> **Business email compromise scams are the most financially harmful scam affecting Australian businesses, with combined losses of over $132 million in 2019.**

In a business email compromise scam, a scammer impersonates a supplier business or senior staff member through email and requests that money be sent to a fraudulent account. Common scenarios include scammers impersonating:

- the supplier, by intercepting legitimate invoices and changing them to include fraudulent payment details before releasing to the intended recipient
- CEOs or other senior managers, requesting staff transfer funds to them for a variety of reasons. For example, they are travelling overseas and need funds for an unforeseen emergency, or they need to purchase gift cards as a surprise for an employee
- staff members, requesting a change to their ordinary payment account.

Scamwatch receives reports from businesses that have been impersonated in business email compromise scams, and other businesses or individuals who have paid a scammer in a business email

compromise scam. Businesses were more likely to report these scams to the police or their bank than to Scamwatch.

How do they work?

Scammers can find names of executives, senior managers, accountants and payroll officers online, and then quickly work out the format for that person's business email address. They can also hack into email accounts, including through information gathered in phishing scams.

If they gain access to a business email account, scammers can use their mailing lists to send large numbers of fake invoices that provide the scammer's payment details instead of the business's.

Scammers will also intercept emails and invoices legitimately issued by a business and change the beneficiary account numbers to their own. This way any money sent by the receiver of the invoice will go to the scammer's bank account (or a bank account controlled by the scammer) rather than the legitimate business.

'***Only realised it was a fraudulent account after a month when the supplier called me to ask where payment was.'***
November 2019—$174 000 loss

The ACCC is advocating for banks to check the name of accounts as well as BSBs and account numbers to help prevent these scams occurring. Similar measures have been implemented overseas with good results.[41]

Another variant involves no actual compromise of the target's email account. In this version, scammers create an email address that looks like the target's email on casual inspection.

A scammer impersonating 'lex.luthor@lexcorp.com" might register the domain 'lexcorp.com' (with an upper case 'i' instead of lower case 'l') then send their scam from 'lex.luthor@lexcorp.com' making it initially very hard to tell the difference.

Scammers often rely on urgency to pressure people into transferring funds quickly, before their story can be checked.

Case study 6: Business email compromise scam involving a property settlement

Emma received an email from the solicitor handling her recent property settlement. The email appeared to be legitimate, with the same format and signature block as previous emails. Emma's solicitor was requesting she transfer the shortfall amount into a trust account. The email contained lots of accurate information, including the property address, correct amount, and dates and timings. Emma made the transfer of $63 000. A couple of days later, Emma's solicitor told her he had not requested the money and did not know about the trust account she used. Emma checked back over her emails and noticed that the email addresses were almost identical—but the new email address did not end in '.au'. Emma contacted her bank but it was too late. The money had been transferred into a different account and then overseas.

41 The Netherlands introduced the IBAN-Name Check in 2017 for domestic payments—it helps bank customers protect themselves from fraud with account numbers and to avoid incorrect transfers. It covers 90 per cent of all online transactions. https://www.surepay.nl/en/services/confirmation-of-payee/. In the UK, Confirmation of Payee was introduced in October 2018 and will become law from 30 June 2020. https://thepaypers.com/digital-identity-security-online-fraud/uk-based-banks-to-launch-confirmation-of-payee-to-avoid-fraud--1242850.

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:
$5.3 million
Combined losses **$132 million**
(Reported to Scamwatch, other government agencies and the big four banks)

120% increase in losses over previous year

According to the FBI, global losses to BEC scams between 2016 and 2019 = **US$26 billion**

Reports to Scamwatch in 2019

PROTECT YOURSELF:

If you receive an email to change payment details, contact the vendor by alternative means to check the details

BEC in the building sector

In 2019, business email compromise scams targeted the building sector, with $367 984 in losses. Builders and other tradespeople make lucrative targets for impersonation as they often send multiple invoices for large amounts of money, which helps confuse the individuals paying for the services.

For example, Scamwatch received many reports of business email compromise scams from individuals who were renovating their houses. In some cases, the scammer had intercepted emails from the builder attaching an invoice before it reached the client; in others, the scammer had hacked the client's email account and set up rules to divert emails containing words such as 'invoice', 'bank account details' or 'payment due'. The scammer then removed the builder's payment details from the real invoice and inserted their own, before sending to the individual for payment.

5.2 False billing scams

False billing scams accounted for the highest reports and losses from businesses in 2019. Aside from business email compromise scams, fake invoices make up a large proportion of false billing scams. A common example involves scammers sending an invoice for payment for an advertisement in dubious magazines or journals. When the business queries the advertisement, they are told they agreed to it months ago and now have to pay the invoice. Generally the scammer continues to harass the business until they are paid.

Case study 7: False billing scam involving advertising in an online magazine

Andrew's small business received a fax from a company stating they had organised advertising. The fax said if Andrew wanted to stop the advertising, he should sign the form and return the fax. Andrew did as directed. However, the company then advised there would be a charge because the advertising was already in place for the year, and they would not cease the advertising until payment was made. Andrew was suspicious and decided to do nothing. His business began to receive several harassing calls a day, tying up the business line and preventing real customers from calling. Andrew's business had never advertised online and he suspected scammers had just created the 'ads' with pictures from his business website. After several days of constant phone calls Andrew paid the amount, even though he was pretty sure it was a scam.

Other scams affecting businesses

Businesses also suffered losses to general scams such as the NBN robocalls and Telstra remote access scams. In 2019, Scamwatch received multiple reports about scammers tying up business phone lines, preventing genuine customers from getting through.

Businesses may also be targeted by scammers using stolen credit cards. The scammer will order something from a business and pay with one credit card. They will call back later and make an excuse to cancel the order, requesting to be refunded to a different credit card. After refunding the money, the business learns the initial credit card was stolen and the legitimate owner is querying the charge with their bank. The business is left out of pocket.

Another variant involves a scammer advertising an item at a slightly lower price than legitimate retailers. Somebody then orders the item and sends money to the scammer. The scammer orders the item from a legitimate retailer using stolen credit card details, and enters the address of the person who ordered the item. When the credit card owner challenges the charge, the business loses twice: the item is gone, and the credit card payment needs to be refunded.

5.3 New payment methods and scams

Neosurf is an online payment method for buying, paying and playing games online. It was launched in 2004. Neosurf is a prepaid card that lets you shop or play online games without needing to provide your credit card details. Neosurf vouchers can be purchased online, or through a reseller or store.

Scamwatch received the first scam report involving Neosurf as a payment method in March 2019. There were 99 scam reports about it in 2019, with losses of $67 320. The majority of reports were about online shopping scams or classified scams.

Twelve reports came from businesses, with losses of $25 710. The scam was almost identical in each case. The business would receive a phone call from someone purporting to work at EPay (the service provider for Neosurf vouchers), stating there was an issue with Neosurf that had to be fixed before they could issue any more vouchers.

The scammer would then walk the business through the steps to resolve the issue. This involved printing vouchers from the system and reading the voucher numbers to the scammer. As soon as the business realised this was a scam and contacted EPay, they were told the voucher had already been used.

6. The failed attempts

In 2019 Scamwatch received 123 872 reports of attempted scams, where the reporter did not give money or personal information to a scammer. These reports are important, as they give insights into the red flags that help people recognise and avoid scams.

We've analysed the data to share the stories of these near misses, and provide information about how people can identify scams.

How to avoid a scam

- **Tell someone**—got a new online friend or love interest, job offer or investment opportunity? Sound it out with your friends or family. They may know about this type of scam and can alert you to it early. Most people find out about scams through word of mouth.
- **Trust your instincts**—sometimes we're unwilling to admit it—even to ourselves—but when you know, you know. Many scam reporters said they were suspicious of the scammer, and hid it from their friends and families because they didn't want to be told the truth or because they were embarrassed.
- **Research**—scammers are efficient and will use the exact same story to try to deceive many people. Paste some text into a search engine or do a reverse image search on a photo to see if others have reported it as a scam.
- **Check whether the story adds up**—does the person say they are educated, but have poor spelling or grammar? Does their description match their photo? These small inconsistencies can flag a big problem.
- **Ignore what's not applicable to you**—if you don't use that bank, it's unlikely there is an issue with your account. If you didn't enter the lottery, you won't have won it. If you didn't order anything, then there isn't an online delivery waiting for your confirmation.
- **Stop engaging**—it is important to immediately stop communicating with a person if you suspect they might be a scammer. If you continue, they will try to convince you to stay in the scam, or even try to lure you into a new one.

▶ Case study 8: Suspicious job interview

Rachel received a text message from Steve, who told her he found her resume on Ladders and invited her to an interview without providing any job details. The interview was held over Skype with Fred. Fred didn't appear by video; there was a still photo on screen while he texted questions to her. Despite being on alert, Rachel continued the interview. Fred asked two or three questions about Rachel's job history, but then began asking about her financial institutions. Rachel became suspicious so she asked about the position and duties, but Fred couldn't answer. Rachel terminated the interview and did not follow up.

Afterward, Rachel realised she never actually saw anyone's face nor spoke directly to anyone before or during the interview. Fred's comments in the interview didn't sound as though he understood the industry. Rachel suspected Steve and Fred were the same person and the job was really a scam. Rachel decided she would now only look for jobs that included the business name, deeply research all potential job opportunities before applying and make sure she speaks to a person during the process instead of relying on texts or emails.

Case study 9: Outsmarting a dating and romance scammer

Alice met Chris on the pen pal app Slowly, and they had been chatting for about a week. She knew that Chris was from Canada and was working on an oil rig near Hong Kong, which meant he couldn't video call her. Within the week Chris started professing his love, which Alice thought was a little odd. Chris then had to travel for work, and told Alice he was afraid that pirates would steal his money. Chris offered to give Alice 20 per cent of his cash if she helped him send the money through a UN courier.

Chris told Alice that he would come to Australia to marry her when his contract was over. She was shocked; she'd already told him she didn't want to get married. Suspicious, Alice said she would not help Chris, and that she thought what he suggested might be fraud.

Alice began to have doubts about everything Chris told her. He'd forgotten details of earlier conversations, and she realised that his descriptions of himself didn't match the photos he had sent. Alice did a reverse image search and found his photo was actually of a man in the US, whose image had been used for several other scams. Alice decided this was a scam too and stopped communicating with Chris.

6.1 Scam myths

Scams are not the same as they used to be, and it's timely to dispel some common myths:

- *Scam victims are naive:* Scammers are professional tricksters and use human psychology against victims. Anyone can be targeted successfully by scammers despite their level of education or business acumen. Some scams are conducted by organised criminals who are very experienced in fooling people.
- *Scam victims are greedy:* Many people who fall victim to scams believe they are helping others. Dating and romance scams had the second highest losses of all scam types in 2019, and this scam usually relies on victims sending money to their 'loved one' to provide assistance. Often victims are acting from their heart and scammers take advantage of this.
- *Only older people fall for scams:* Anyone can fall for a scam. People 24 to 35 years old reported sending money more frequently than other age groups. People 55 to 64 years old lost the most money, followed by 45 to 54 year olds.
- *Scams are easy to spot:* This may have been true years ago when poor spelling or grammar was a clear warning sign, but technology has made scams harder, and sometimes impossible, to identify. For example, last year phone porting scams spiked, and there was no warning sign for the victim until it was too late.
- *You are only scammed if you lose money:* In the 21st century your personal information is just as important as your money. In fact, your personal information can be used to steal your money, or take loans or credit cards out in your name. If you have given personal details to a scammer, you have been scammed.
- *There is no way to protect yourself from a scam:* While it's true that scams can happen to anybody, you can protect yourself using some common sense tactics:
  - be aware scammers are out there and be vigilant in looking out for scams
  - research opportunities, read independent reviews, sign up for Scamwatch's free radar emails and talk to your friends and family before you make any big decisions
  - scammers will often use unusual communication methods or encrypted communication means, so be cautious if someone wants to move your communication from a monitored website to a more anonymous one
  - never give money or personal data to people you have never met, even if you have been chatting online for several months.

7. The fight against scams

The ACCC, other regulators, law enforcement agencies and businesses continuously fight to prevent scams from affecting Australians.

The ACCC's goal is to make Australia a harder target for scammers. We want to prevent people from falling victim to scams in the first place, and suffering the financial loss and emotional distress that comes with them. As such, we are active in scams disruption with many other organisations all working together to prevent scammers affecting our country.

7.1 ACCC activity

Enforcement

Scams are a considerable challenge for law enforcement agencies as perpetrators often frustrate traditional regulatory approaches by setting up schemes that are difficult to trace, based overseas and across multiple jurisdictions. Additionally, even when law enforcement agencies are able to take enforcement action against perpetrators, these actions are difficult, drawn out and resource intensive. A successful court judgment against a perpetrator is often not the end of these agencies' enforcement work.

The ACCC's action in relation to Mr Richard Otton, the sole director of We Buy Houses Pty Ltd (WBH) is an illustrative example. On 15 November 2018, following legal action by the ACCC, the Federal Court imposed penalties of $12 million against WBH and $6 million against Mr Otton for making false or misleading representations in promoting a number of wealth creation strategies involving real estate. The penalty awarded against Mr Otton is the highest ever awarded against an individual under the Australian Consumer Law (ACL), and the penalty against WBH was the highest ACL penalty for a company at that time. The Court also ordered that WBH and Mr Otton pay the ACCC's legal costs.

After the decision, the ACCC had to pursue freezing orders to ensure Mr Otton didn't dissipate his assets rather than paying the penalty and costs ordered by the Court. The matter was finalised in 2020.

Scams Intermediaries project

Since 2018 the ACCC has been working with a range of private sector 'intermediaries' to minimise consumer losses to scams.

Intermediaries include digital platforms, where scammers make contact with victims, and financial service providers such as banks and money remitters, through which money is sent to scammers.

In 2018 the ACCC ran a successful pilot project, sharing relevant scam reports with participating intermediaries for six months. Feedback from participants confirmed that these reports improved their own ongoing scam prevention efforts.

Following this initial success, in March 2019 the ACCC began establishing automated solutions for ongoing sharing of scam reports (where consent is provided).

By December 2019, the ACCC had established automated solutions for sharing scam reports with intermediaries. We inform intermediaries of scams daily, which has disrupted some scams.

Scam Watchlist project

In 2019 the ACCC proactively engaged with several private sector organisations about scam trends affecting their platforms or services. Following discussions with these organisations it became apparent that some were not aware of the true impact of scams affecting their customers, because customers do not always report scams directly to them.

Recognising that the organisations were in the best position to disrupt scams for their customers, we began a six-month trial of sharing relevant intelligence through 'scam watchlists'.[42]

As a result of this trial, participating organisations have reported that they:

- are able to input better data into fraud detection software, making it easier to identify and remove scam accounts from their business
- can use current data to predict future scam activity, and target scam prevention and awareness activities to customers most at risk
- better understand the financial impact of scams on their customers, thus placing more importance on disrupting scams
- developed materials to assist frontline staff in helping customers
- improved scams messaging on their websites, and
- removed scam pages and profiles.

We hope to expand this trial in 2020 to encourage and help other organisations to improve their scams disruption activities.

Digital Platforms Inquiry

In July 2019, the ACCC released the final report of the Digital Platforms Inquiry. This report outlined key issues regarding the impact of private data and emerging technologies in proliferating scams on digital platforms.

The report found that the rise of digital platforms has enabled the growth of online scams, resulting in significant losses for consumers and small businesses. The ease with which scammers use digital platforms to conduct scams, particularly dating and romance scams, investment scams and advertisements containing false representations, is especially concerning. Further, the extensive data collected by digital platforms may include data that identifies (or infers) an individual's vulnerabilities. This can place vulnerable consumers at risk of being targeted by scammers.

The report found that governments have a role to closely monitor and update regulatory and legislative frameworks to protect society and individuals from harm. In addition, it found that Google and Facebook needed to do more to take down scam ads and similar content and provide redress, where appropriate, for consumers that have experienced harm as a result. In the Australian Government's response to the *Digital Platforms Inquiry final report* (December 2019) it indicated that it supported, in principle, the need for improved dispute resolution by digital platforms. The government's response confirmed that in 2020 it will develop a pilot external dispute resolution scheme, which will inform whether to establish a digital platforms ombudsman to resolve complaints and disputes between digital platforms and individual consumers and small businesses using their services.

7.2 Australian Communications and Media Authority

In December 2018 the ACMA established the Scam Technology Project to fight phone scams. The project included the ACCC and the Australian Cyber Security Centre along with other government agencies, such as the ATO, and telecommunications providers. In late November 2019 the ACMA released its *Combating scams* report, which recommended a three-point action plan. These initiatives aimed to reduce common phone scams, including scams where the calling line identification has been overstamped or 'spoofed' and Wangiri scams. The third action point was trialling a Do Not Originate list with the ATO to prevent scammers from spoofing legitimate ATO phone numbers. More information can be found at www.paulfletcher.com.au/media-releases/joint-media-release-stopping-ato-phone-call-scams.

As part of the project, the ACCC has been providing scam telephone numbers to Telstra so it can investigate and find ways of blocking the numbers. In September 2019, Telstra announced it had blocked 2.9 million scam calls in one month alone. The ACCC will be expanding this project to share data with other telecommunications carriers in 2020.

42 The data was anonymised to protect the confidentiality of reporters.

7.3 Law enforcement and consumer protection

Last year saw some important results for law enforcement agencies. On the Gold Coast, Queensland Police charged five people for being part of a syndicate operating a cryptocurrency investment scam.[43] The scam operated from 2017 to 2019, with losses exceeding $2.7 million from 100 investors.

Separately, the Australian Federal Police and the Australian Securities and Investments Commission disrupted an identity theft syndicate that purchased stolen credentials from dark net marketplaces. The scammers used this information to create fake identities that mimicked real Australian identities to establish bank accounts.[44]

WA ScamNet received 2461 scam reports in 2019 with reported losses of $13.6 million. It removed 34 scam websites and 24 scam social media pages during the year. WA Scamnet was also able to assist six victims to recover $7000 in funds lost to scammers.

Australian Border Force busts Queensland boiler room scam

In May 2019 the Australian Border Force (ABF) prevented 35 Taiwanese nationals from entering Australia, after ABF officers at Brisbane Airport identified their intended involvement in 'boiler room' scams.

Boiler room scams often involve foreign nationals brought to Australia on student or tourist visas, who are forced to live and work in substandard conditions and carry out phone scams. These scams generally involve callers attempting to fleece large amounts of money from unsuspecting victims. The scams harm Australians and the foreign nationals forced to carry them out.[45]

7.4 Banking sector

In 2019, the big four banks saved nearly $230 million from being sent to scammers. This included amounts that were detected early and thus not processed, and amounts that were recovered from financial institutions after being sent.

All reputable banks should have dedicated teams to investigate potential scam and fraud transactions, and many do. They should also invest in scams awareness materials for staff and customers.

Once a person has sent money to a scammer it is difficult to recover the funds. This is particularly so if the funds are sent offshore. With new payment methods and speedier payment transfers, scammers may have already moved money to different bank accounts by the time a victim has realised they are dealing with a scammer. Therefore, it is important people understand they may be dealing with a scammer as quickly as possible to reduce the financial impact of the scam.

7.5 Scams Awareness Network

The SAN 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 disrupt scams and raise awareness about them.

The ACCC's Deputy Chair, Delia Rickard, is the Chair of SAN, and we also provide secretariat services. Each month, members share scams intelligence, research and upcoming awareness campaigns.

---

43 T Crockford 'More than 100 lose $2.7 million in Gold Coast cryptocurrency scams', Brisbane Times, 8 August 2019: https://www.brisbanetimes.com.au/national/queensland/more-than-100-lose-2-7-million-in-gold-coast-cryptocurrency-scam-20190808-p52f0m.html.

44 'Australian Federal Police Online fraud syndicate dismantled after allegedly siphoning millions from shares and superannuation accounts' media release, 17 September 2019: https://www.afp.gov.au/news-media/media-releases/online-fraud-syndicate-dismantled-after-allegedly-siphoning-millions.

45 D Murray, 'Australian Border Force stops 35 Taiwanese over 'boiler room scams', May 14, 2019, https://www.theaustralian.com.au/nation/australian-border-force-stops-35-taiwanese-over-boiler-room-scams/news-story/8f7b3baa0bbffb6efde8577272d725cf.

Scams Awareness Week

SCAMS AWARENESS WEEK

Every year, SAN organises and delivers Scams Awareness Week. The week promotes awareness around a particular theme to help Australians recognise and avoid scams.

In 2019 the week ran from 12 to 16 August with the theme 'Too smart to be scammed?' It aimed to draw attention to the large number of scams that exist, remind people that new scams continue to emerge, and challenge people's ideas that they could identify a modern scam.

As part of this campaign, the ACCC produced three vox pop videos of people in Melbourne trying to spot a scam. The videos were well received, and one set an ACCC record for the highest number of views (69 000). We also released quizzes for people to test their own ability to spot and understand particular scams.

Scams Awareness Week 2019 received good media coverage. Our media release generated over 350 media items during the week, and Deputy Chair Delia Rickard participated in 18 official media engagements. The vox pop videos were viewed on the ACCC's channels 118 792 times. A number of SAN partners shared the videos on their Facebook pages, reaching a total of 187 176 users. The quiz was promoted by news outlets including news.com.au and the Yahoo Finance website. In total, Scams Awareness Week media items had an estimated potential reach of 10.4 million.

8. The future of scams

Calling the last 10 years 'the decade of scams' is not an overstatement. Reports and losses have increased exponentially since 2009 and scams are affecting more and more people, businesses and vulnerable communities.

New technologies have not only enabled scammers to access more targets, but to act more quickly and convincingly. Since 2009 scammers have moved from relatively unsophisticated scams such as 'Nigerian prince' email frauds to professional robocalls and complicated remote access scams.

As technology evolves, we can expect scams to continue to adapt and become more difficult to detect. Scams are a whole-of-community problem, and the ACCC expects industry and businesses, as well as governments, to implement scam disruption and prevention measures to ensure scammers don't take advantage of their innovations.

8.1 What is on the horizon?

It is hard to predict the new ways scams will evolve over the coming years. However, the past provides a good indication of patterns and trends that we can expect to continue:

- **Scammers will continue to use previously successful scam techniques albeit with modern twists**. While the methods have changed over time, classic scams such as dating and romance and investment scams have remained constant.
- **Digital identity scams will increase**. Identity theft scams have increased significantly over the last two years, and identity theft has become a common secondary issue to most other scams.
- **Emerging technologies will pose new risks**. Artificial intelligence and deepfakes are examples of new technologies that are already being used to add credibility to existing scams. As these types of technologies mature and new ones emerge, we can expect scams to become even harder to detect.

8.2 Concluding comments

The impact of scams is getting worse. They are more complex and harder to detect. The 11-year trend of significantly increasing losses requires urgent action to prevent it continuing. Australians lose large amounts of money to scams, which would be better spent improving lives and the overall economy.

Scams are a pervasive threat to our society and we all have a role to play in defeating them. It is not enough for consumer regulators and law enforcement agencies to pursue scammers. We also need the continued efforts of governments, financial institutions, businesses, digital platforms, and telecommunications and internet providers if we are to make a meaningful difference

By raising public awareness about scams, and implementing scams disruption measures as ordinary business practice, we can all work together to make Australia a harder target for scammers.

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

Reports by losses

Scam types	Reports	Reports with loss	Losses	Percentage increase or decrease in losses from 2018
Investment scams	5 005	2 128	$61 813 401	▲59.1%
Dating and romance scams	3 948	1 380	$28 606 215	▲16.1%
False billing	11 255	1 881	$10 110 756	▲83.4%
Hacking	8 321	509	$5 139 414	▲64.3%
Online shopping scams	9 953	6 027	$4 845 452	▲47.8%
Remote access scams	9 019	682	$4 836 812	▲1.6%
Identity theft	11 373	562	$4 311 066	▲192.8%
Threats to life, arrest or other	13 375	414	$4 250 689	▲27.3%
Classified scams	4 958	1 528	$2 816 076	▲19.1%
Inheritance scams	2 920	67	$2 622 355	▲20.7%
Unexpected prize and lottery scams	9 456	471	$2 385 669	▼-13.1%
Jobs and employment scams	2 505	433	$1 741 881	▲14.2%
Pyramid schemes	596	171	$1 669 618	▲175.0%
Phishing	25 168	513	$1 517 864	▲62.6%
Betting and sports investment scams	503	132	$1 205 001	▼-54.2%
Overpayment scams	1 794	452	$1 114 880	▲50.6%
Nigerian scams	661	152	$1 068 638	▼-22.5%
Psychic and clairvoyant	194	73	$452 811	▲136.2%
Scratchie scams	760	22	$419 336	▼-11.0%
Fake charity scams	1 167	165	$411 588	▲94.9%
Travel prize scams	728	56	$360 151	▲137.3%
Rebate scams	1 520	49	$220 648	▼-63.1%
Mobile premium services	2 107	188	$188 778	▲123.2%
Health and medical products	858	239	$179 639	▼-34.6%
Ransomware and malware	4 511	52	$156 569	▲3.6%
Other scams	35 142	1 438	$462 065	▼-88.9%
Total	**167 797**	**19 783**	**$142 907 372**	**▲33.6%**

Reports by numbers

Scam type	Reports	Reports with loss	Reported losses	Change in reports since 2018
Phishing	25 168	513 (2.0%)	$1 517 864	▲3.6%
Threats to life, arrest or other	13 375	414 (3.1%)	$4 250 689	▼–31.3%
Identity theft	11 373	562 (4.9%)	$4 311 066	▼–11.1%
False billing	11 255	1 881 (16.7%)	$10 110 756	▲2.4%
Online shopping scams	9 953	6 027 (60.6%)	$4 845 452	▲2.7%
Unexpected prize and lottery scams	9 456	471 (5.0%)	$2 385 669	▼–5.9%
Remote access scams	9 019	682 (7.6%)	$4 836 812	▼–20.5%
Hacking	8 321	509 (6.1%)	$5 139 414	▼–3.5%
Investment scams	5 005	2 128 (42.5%)	$61 813 401	▲42.7%
Classified scams	4 958	1 528 (30.8%)	$2 816 076	▼–0.2%
Ransomware and malware	4 511	52 (1.2%)	$156 569	▲3.6%
Dating and romance scams	3 948	1 380 (35.0%)	$28 606 215	▼–0.8%
Inheritance scams	2 920	67 (2.3%)	$2 622 355	▲3.3%
Jobs and employment scams	2 505	433 (17.3%)	$1 741 881	▼–11.8%
Mobile premium services	2 107	188 (8.9%)	$188 778	▲8.5%
Overpayment scams	1 794	452 (25.2%)	$1 114 880	▼–7.0%
Rebate scams	1 520	49 (3.2%)	$220 648	▼–60.0%
Fake charity scams	1 167	165 (14.1%)	$411 588	▲24.0%
Health and medical products	858	239 (27.9%)	$179 639	▼–17.3%
Scratchie scams	760	22 (2.9%)	$419 336	▼–24.5%
Travel prize scams	728	56 (7.7%)	$360 151	▼–28.3%
Nigerian scams	661	150 (22.7%)	$1 066 838	▼–24.7%
Pyramid schemes	596	171 (28.7%)	$1 669 618	▲84.0%
Betting and sports investment scams	503	132 (26.2%)	$1 205 001	▲84.2%
Psychic and clairvoyant	194	73 (27.6%)	$452 811	N/A
Other scams	35 142	1 438 (4.1%)	$462 065	▲6.7%
Total	**167 797**	**19 783**	**$142 905 572**	**▼–5.40%**

Indigenous reports

Scam type	Reports	Reports with loss	Losses	Change in losses since 2018
Investment scams	98	57 (58.2%)	$1 109 889	▼–7.4%
Dating and romance scams	136	42 (30.9%)	$438 707	▼–51.5%
Online shopping scams	171	102 (59.6%)	$83 775	▲168.0%
Hacking	141	18 (12.8%)	$83 670	▲268.0%
False billing	210	37 (17.6%)	$63 458	▼–3.5%
Classified scams	81	34 (42.0%)	$61 859	▼–34.6%
Unexpected prize and lottery scams	159	15 (9.4%)	$41 405	▼–36.7%
Psychic and clairvoyant	10	5 (50.0%)	$37 880	N/A
Threats to life, arrest or other	178	6 (3.4%)	$30 665	▲2 966.5%
Nigerian scams	33	10 (30.3%)	$29 292	▼–46.7%
Ransomware and malware	59	1 (1.7%)	$19 950	▲256.3%
Jobs and employment scams	42	10 (23.8%)	$15 888	▼–72.9%
Identity theft	219	15 (6.8%)	$15 749	▲38.3%
Overpayment scams	28	7 (25%)	$9 489	▲68.6%
Mobile premium services	31	4 (12.9%)	$8 678	▲144 533.3%
Fake charity scams	37	4 (10.8%)	$7 900	▼–41.2%
Phishing	258	9 (3.5%)	$6 400	▼–90.7%
Pyramid schemes	17	7 (41.2%)	$6 400	▼–81.5%
Health and medical products	16	5 (31.3%)	$6 134	▼–22.7%
Betting and sports investment scams	3	1 (33.3%)	$5 000	▼–27.4%
Inheritance scams	50	1 (2.0%)	$5 000	▼–80.2%
Remote access scams	89	6 (6.7%)	$4 586	▼–85.7%
Travel prize scams	11	1 (9.1%)	$148	▼–99.3%
Rebate scams	17	0	$-	▼–100.0%
Scratchie scams	7	0	$-	N/A
Other scams	666	37 (5.6%)	$16 436	▼–93.7%
Total	**2767**	**434 (15.7%)**	**$2 108 358**	**▼–29.9%**

Appendix 2: Scam reported by state and territory

Australian Capital Territory

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2018
Dating and romance scams	$1 144 096	68	20 (29.4%)	▲166.1%
Threats to life, arrest or other	$374 457	517	16 (3.1%)	▲986.5%
Investment scams	$370 202	118	35 (29.7%)	▼-61.6%
Scratchie scams	$250 000	39	1 (2.6%)	▲4 025.4%
Remote access scams	$190 296	218	22 (10.1%)	▲23.1%
False billing	$89 892	363	44 (12.1%)	▲215.8%
Online shopping scams	$65 300	245	153 (62.4%)	▼-10.5%
Hacking	$43 254	204	15 (7.4%)	▼-54.4%
Classified scams	$42 725	161	47 (29.2%)	▲3.1%
Overpayment scams	$41 122	54	13 (24.1%)	▲2 522.6%
Phishing	$33 489	929	20 (2.2%)	▲102.9%
Jobs and employment scams	$31 166	46	5 (10.9%)	▲224.9%
Identity theft	$19 375	336	10 (3.0%)	▼-56.7%
Mobile premium services	$15 947	55	7 (12.7%)	▲1373.8%
Pyramid schemes	$14 163	16	8 (50.0%)	▼-6.6%
Betting and sports investment scams	$7 060	12	2 (16.7%)	▼-99.6%
Nigerian scams	$4 500	9	2 (22.2%)	N/A
Psychic and clairvoyant	$4 500	7	3 (42.9%)	▲52.5%
Fake charity scams	$2 725	34	1 (2.9%)	▲263.3%
Inheritance scams	$2 715	70	1 (1.4%)	▼-81.9%
Unexpected prize and lottery scams	$1 741	270	8 (3.0%)	▼-36.2%
Travel prize scams	$1 466	21	2 (9.5%)	N/A
Ransomware and malware	$900	134	2 (1.5%)	▼-75.3%
Rebate scams	$650	46	1 (2.2%)	▼-78.3%
Health and medical products	$597	19	1 (5.3%)	▼-82.7%
Other scams	$9 695	1 073	34 (3.2%)	▼-85.8%
Total	**$2 762 033**	**5 064**	**473 (9.3%)**	**▼-25.7%**

New South Wales

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2018
Investment scams	$12 259 739	1 177	422 (35.9%)	▲29.2%
Dating and romance scams	$6 935 567	762	277 (36.4%)	▲19.4%
False billing	$2 239 474	3 160	521 (16.5%)	▲40.2%
Hacking	$1 893 880	2 507	155 (6.2%)	▲61.9%
Identity theft	$1 838 974	3 353	170 (5.1%)	▲305.9%
Remote access scams	$1 566 828	2 759	201 (7.3%)	▲11.9%
Online shopping scams	$1 009 953	2 754	1 676 (60.9%)	▲37.1%
Inheritance scams	$926 530	714	17 (2.4%)	▲396.8%
Pyramid schemes	$771 106	107	42 (39.3%)	▲293.2%
Classified scams	$744 131	1 374	419 (30.5%)	▲6.0%
Threats to life, arrest or other	$596 070	3 946	99 (2.5%)	▼-43.0%
Unexpected prize and lottery scams	$453 007	2 534	130 (5.1%)	▲34.0%
Phishing	$319 161	6 996	129 (1.8%)	▲51.6%
Jobs and employment scams	$319 034	562	100 (17.8%)	▲30.2%
Psychic and clairvoyant	$288 675	49	22 (44.9%)	▲136.2%
Betting and sports investment scams	$246 530	110	25 (22.7%)	▼-49.8%
Nigerian scams	$196 914	132	35 (26.5%)	▼-29.8%
Overpayment scams	$122 867	473	115 (24.3%)	▼-58.8%
Fake charity scams	$102 797	280	41 (14.6%)	▼-6.7%
Mobile premium services	$61 745	615	58 (9.4%)	▲181.5%
Rebate scams	$59 077	432	14 (3.2%)	▲380.5%
Ransomware and malware	$52 826	1 268	15 (1.2%)	▼-7.8%
Health and medical products	$47 543	226	78 (34.5%)	▲16.8%
Travel prize scams	$32 548	187	20 (10.7%)	▼-61.5%
Scratchie scams	$14 158	140	3 (2.1%)	▼-88.7%
Other scams	$123 030	9 444	395 (4.2%)	▼-87.6%
Total	**$33 222 164**	**46 061**	**5 179 (11.2%)**	**▲25.8%**

Northern Territory

Scam category	Reported losses	Reports	Reports with loss	Percentage change since 2018
Dating and romance scams	$1 008 904	120	45 (37.5%)	▲91.3%
Investment scams	$637 846	43	26 (60.5%)	▼–74.6%
Threats to life, arrest or other	$124 958	158	10 (6.3%)	▲188.7%
Unexpected prize and lottery scams	$89 200	128	13 (10.2%)	▲143.9%
Online shopping scams	$73 551	120	73 (60.8%)	▲321.7%
Identity theft	$68 128	121	5 (4.1%)	▼–12.9%
Overpayment scams	$50 034	20	10 (50.0%)	▲484.0%
Ransomware and malware	$48 427	65	4 (6.2%)	▲497.2%
Remote access scams	$36 456	57	4 (7.0%)	▲84.8%
False billing	$34 228	125	13 (10.4%)	▼–31.7%
Jobs and employment scams	$30 334	39	10 (25.6%)	▲125.0%
Hacking	$25 528	98	7 (7.1%)	▲215.9%
Nigerian scams	$25 367	21	8 (38.1%)	▼–7.6%
Pyramid schemes	$24 000	4	2 (50.0%)	▲557.2%
Classified scams	$22 776	56	17 (30.4%)	▼–64.4%
Mobile premium services	$8 428	23	5 (21.7%)	▲1 231.4%
Betting and sports investment scams	$1 650	6	2 (33.3%)	▼–79.4%
Health and medical products	$1 367	11	4 (36.4%)	▼–72.2%
Psychic and clairvoyant	$1 186	9	5 (55.6%)	▲13 077.8%
Phishing	$1 073	197	5 (2.5%)	▼–75.4%
Travel prize scams	$1 000	11	1 (9.1%)	N/A
Scratchie scams	$992	5	1 (20.0%)	N/A
Rebate scams	$604	13	2 (15.4%)	▲1 913.3%
Fake charity scams	$250	15	1 (6.7%)	N/A
Inheritance scams	$200	47	1 (2.1%)	▼–99.9%
Other scams	$7 276	308	23 (7.5%)	▼–70.0%
Total	**$2 323 763**	**1820**	**297 (16.3%)**	**▼–37.2%**

Queensland

Scam category	Reported losses	Reports	Reports with loss	Percentage change in losses since 2018
Investment scams	$10 610 828	876	302 (34.5%)	▲52.9%
Dating and romance scams	$6 862 069	550	338 (61.5%)	▲55.7%
False billing	$1 722 109	2 277	343 (15.1%)	▲72.3%
Hacking	$1 412 439	1 678	94 (5.6%)	▲258.3%
Inheritance scams	$1 104 240	537	5 (0.9%)	▲285.3%
Online shopping scams	$633 156	1 727	1 030 (59.6%)	▲15.0%
Identity theft	$600 707	2 193	85 (3.9%)	▲198.9%
Pyramid schemes	$599 999	102	40 (39.2%)	▲1 170.2%
Threats to life, arrest or other	$534 007	2 640	70 (2.7%)	▼-10.5%
Remote access scams	$527 557	1 719	121 (7.0%)	▼-39.5%
Jobs and employment scams	$464 633	424	79 (18.6%)	▲6.1%
Classified scams	$427 935	1 070	256 (23.9%)	▼-28.8%
Unexpected prize and lottery scams	$414 835	1 769	86 (5.0%)	▲48.3%
Overpayment scams	$285 212	344	66 (19.2%)	▲185.2%
Betting and sports investment scams	$269 005	131	15 (11.5%)	▲146.3%
Phishing	$237 106	4 705	91 (2.0%)	▲69.3%
Nigerian scams	$175 682	122	22 (18.0%)	▼-23.9%
Fake charity scams	$141 793	243	27 (11.1%)	▲195.7%
Scratchie scams	$99 795	198	7 (3.5%)	▼-10.7%
Other scams	$99 548	7 728	284 (3.7%)	▼-88.1%
Ransomware and malware	$32 928	959	13 (1.4%)	▲21.0%
Mobile premium services	$20 831	408	31 (7.6%)	▲69.3%
Rebate scams	$19 701	297	18 (6.1%)	▼-64.5%
Health and medical products	$7 595	163	27 (16.6%)	▼-60.3%
Travel prize scams	$2 512	166	5 (3.0%)	▼-55.5%
Psychic and clairvoyant	$910	16	3 (18.8%)	▼-49.3%
Total	**$27 307 132**	**33 042**	**3 458 (10.5%)**	**▲48.0%**

South Australia

Scam category	Reported losses	Reports	Reports with loss	Percentage change in losses since 2018
Investment scams	$2 645 207	286	103 (36.0%)	▲25.8%
False billing	$461 827	836	125 (15.0%)	▲7.9%
Dating and romance scams	$392 718	176	119 (67.6%)	▼-69.2%
Unexpected prize and lottery scams	$365 397	746	37 (5.0%)	▲321.4%
Remote access scams	$328 154	697	51 (7.3%)	▲72.3%
Threats to life, arrest or other	$307 549	999	21 (2.1%)	▼-8.2%
Online shopping scams	$230 985	632	381 (61.2%)	▲1.6%
Identity theft	$228 997	837	49 (5.9%)	▲287.5%
Hacking	$167 272	628	31 (4.9%)	▲179.2%
Classified scams	$166 368	344	117 (34.0%)	▲106.2%
Nigerian scams	$160 180	32	9 (28.1%)	▲107.2%
Phishing	$84 315	1 770	34 (20.0%)	▼-53.9%
Pyramid schemes	$43 885	20	4 (20.0%)	▼-66.7%
Scratchie scams	$40 833	132	3 (2.3%)	▲118.9%
Overpayment scams	$26 968	116	20 (17.2%)	▼-39.6%
Rebate scams	$23 800	104	4 (3.8%)	▲49.1%
Jobs and employment scams	$23 317	123	27 (22.0%)	▲323.9%
Fake charity scams	$13 578	77	8 (10.4%)	▲2 076.0%
Health and medical products	$9 258	88	20 (22.7%)	▲199.6%
Ransomware and malware	$6 703	394	6 (1.5%)	▲1 076.0%
Psychic and clairvoyant	$2 835	10	4 (40.0%)	▼-21.4%
Mobile premium services	$2 799	124	11 (8.9%)	▼-70.3%
Travel prize scams	$1 553	75	3 (4.0%)	▼-13.7%
Betting and sports investment scams	$680	10	2 (20.0%)	▼-94.7%
Inheritance scams	$200	216	1 (0.5%)	▼-99.8%
Other scams	$29 416	2 995	87 (2.9%)	▼-88.8%
Total	**$5 764 794**	**12 467**	**1 277 (10.2%)**	**▲0.5%**

Tasmania

Scam category	Reported losses	Reports	Reports with loss	Percentage change since 2018
Investment scams	$1 164 631	75	32 (42.7%)	▲208.5%
Dating and romance scams	$351 329	52	22 (42.3%)	▲191.0%
False billing	$97 731	263	38 (14.4%)	▲317.4%
Remote access scams	$72 604	203	10 (4.9%)	▲1.1%
Online shopping scams	$52 000	198	129 (65.2%)	▲49.6%
Identity theft	$47 859	217	8 (3.7%)	▲552.4%
Threats to life, arrest or other	$35 150	208	6 (2.9%)	▲328.7%
Classified scams	$30 481	116	44 (37.9%)	▲280.6%
Hacking	$25 565	200	9 (4.5%)	▲15.2%
Phishing	$18 675	534	13 (2.4%)	▼-34.9%
Unexpected prize and lottery scams	$17 826	178	10 (5.6%)	▼-67.1%
Inheritance scams	$10 000	67	1 (1.5%)	▲159.7%
Health and medical products	$3 319	27	12 (44.4%)	▲606.2%
Overpayment scams	$2 332	27	6 (22.2%)	▲191.5%
Travel prize scams	$2 000	8	1 (12.5%)	▲700.0%
Nigerian scams	$1 500	7	1 (14.3%)	▼-25.4%
Mobile premium services	$1 208	27	2 (7.4%)	▼-43.9%
Betting and sports investment scams	$878	6	3 (50.0%)	▼-98.3%
Pyramid schemes	$700	1	1 (100.0%)	▼-80.0%
Fake charity scams	$285	23	3 (13.0%)	▲235.3%
Jobs and employment scams	$0	44	0 (0.0%)	N/A
Ransomware and malware	$0	89	0 (0.0%)	N/A
Rebate scams	$0	20	0 (0.0%)	N/A
Scratchie scams	$0	5	0 (0.0%)	N/A
Psychic and clairvoyant	$0	0	0 (0.0%)	N/A
Other scams	$10 482	675	24 (3.6%)	▼-92.8%
Total	**$1 946 555**	**3 270**	**375 (11.5%)**	**▲98.6%**

Victoria

Scam category	Reports with losses	Reports	Reports with loss	Percentage change in loss since 2018
Investment scams	$8 269 183	876	320 (36.5%)	▲28.2%
Dating and romance scams	$2 931 063	580	227 (39.1%)	▼–29.5%
False billing	$2 514 538	2 384	439 (18.4%)	▲193.9%
Threats to life, arrest or other	$1 735 939	3 053	132 (4.3%)	▲91.3%
Hacking	$1 154 722	1 904	126 (6.6%)	▲49.9%
Remote access scams	$1 145 589	2 224	172 (7.7%)	▼–19.5%
Online shopping scams	$1 034 916	2 233	1 335 (59.8%)	▲87.7%
Classified scams	$797 415	1 050	357 (34.0%)	▲81.6%
Phishing	$650 417	5 718	127 (2.2%)	▲155.6%
Identity theft	$624 203	2 634	131 (5.0%)	▲96.7%
Unexpected prize and lottery scams	$438 718	2 259	98 (4.3%)	▼–70.8%
Betting and sports investment scams	$317 389	75	12 (16.0%)	▲96.1%
Overpayment scams	$277 570	389	109 (28.0%)	▲152.5%
Nigerian scams	$230 242	93	19 (20.4%)	▼–9.5%
Jobs and employment scams	$210 405	444	79 (17.8%)	▲39.5%
Pyramid schemes	$71 280	69	16 (23.2%)	▼–40.3%
Fake charity scams	$63 190	246	38 (14.4%)	▲80.8%
Travel prize scams	$61 608	168	13 (7.7%)	▲94.1%
Rebate scams	$48 245	381	9 (2.4%)	▼–90.3%
Mobile premium services	$33 413	556	35 (6.3%)	▲29.5%
Psychic and clairvoyant	$28 820	33	13 (39.4%)	▼–25.0%
Health and medical products	$15 004	157	46 (29.3%)	▼–90.4%
Inheritance scams	$13 600	522	5 (1.0%)	▼–93.2%
Scratchie scams	$13 156	198	4 (2.0%)	▼–93.7%
Ransomware and malware	$11 776	992	6 (0.6%)	▼–74.5%
Other scams	$101 639	7 501	312 (4.2%)	▼–89.9%
Total	**$22 794 040**	**36 739**	**4 180 (11.4%**	**▲9.9%**

Western Australia

Scam category	Reported losses	Reports	Reports with loss	Percentage change in losses since 2018
Investment scams	$7 325 528	468	197 (42.1%)	▲50.8%
Dating and romance scams	$2 525 289	281	113 (40.2%)	▲25.1%
False billing	$510 771	1 323	176 (13.3%)	▼–41.2%
Threats to life, arrest or other	$363 854	1 378	35 (2.5%)	▲145.1%
Online shopping scams	$360 647	828	494 (59.7%)	▲30.9%
Remote access scams	$359 220	814	67 (8.2%)	▼–10.6%
Hacking	$352 599	792	46 (5.8%)	▼–21.3%
Identity theft	$331 783	1 144	52 (4.5%)	▲46.0%
Classified scams	$248 912	522	183 (26.4%)	▲74.8%
Unexpected prize and lottery scams	$244 874	917	42 (4.6%)	▼–6.9%
Jobs and employment scams	$111 105	274	26 (9.5%)	▲145.9%
Inheritance scams	$109 940	279	3 (1.1%)	▼–86.9%
Phishing	$94 197	3 278	42 (1.3%)	▲27.6%
Overpayment scams	$82 899	172	37 (21.5%)	▼–27.8%
Pyramid schemes	$79 100	40	16 (40.0%)	▲100.4%
Betting and sports investment scams	$56 291	45	11 (24.4%)	▲81.9%
Mobile premium services	$32 463	215	26 (12.1%)	▲293.0%
Fake charity scams	$29 190	106	16 (15.1%)	▲338.0%
Nigerian scams	$28 348	45	9 (20.0%)	▼–79.3%
Travel prize scams	$5 397	58	5 (8.6%)	▼–79.4%
Health and medical products	$5 127	86	19 (22.1%)	▲2.1%
Rebate scams	$3 800	168	1 (0.6%)	▼–74.6%
Scratchie scams	$402	8	3 (37.5%)	N/A
Ransomware and malware	$0	462	0 (0.0%)	N/A
Psychic and clairvoyant	$0	7	0 (0.0%)	N/A
Other scams	$46 921	3 668	145 (4.0%)	▼–86.1%
Total	**$13 308 657**	**17 378**	**1 909 (11.0%)**	**▲17.1%**

Appendix 3: Scam reports from businesses

Scam category	Reported losses	Reports	Reports with loss	Change in losses since 2018
False billing	$2 578 787	1 264	193 (15.3%)	▼-24.4%
Investment scams	$1 183 488	76	20 (26.0%)	▼-35.6%
Identity theft	$329 776	299	23 (7.7%)	▲496.7%
Hacking	$297 464	320	16 (5.0%)	▼-63.2%
Phishing	$201 998	795	19 (2.4%)	▼-16.5%
Online shopping scams	$198 284	188	52 (27.7%)	▲33.7%
Classified scams	$145 405	217	43 (19.8%)	▼-31.1%
Remote access scams	$104 516	344	10 (2.9%)	▲67.0%
Overpayment scams	$82 520	137	8 (5.8%)	▲16.3%
Jobs and employment scams	$45 590	83	9 (10.8%)	▲409.5%
Ransomware and malware	$32 199	186	4 (2.2%)	▲4347.4%
Fake charity scams	$16 675	98	10 (10.2%)	▼-28.1%
Health and medical products	$11 733	39	5 (12.8%)	▼-45.4%
Mobile premium services	$10 017	40	3 (7.5%)	▲202.1%
Threats to life, arrest or other	$9 117	211	2 (0.9%)	▲264.7%
Nigerian scams	$0	13	0	N/A
Inheritance scams	$0	61	0	N/A
Betting and sports investment scams	$0	2	0	N/A
Dating and romance scams	$0	11	0	N/A
Pyramid schemes	$0	1	0	N/A
Rebate scams	$0	21	0	N/A
Scratchie scams	$0	1	0	N/A
Travel prize scams	$0	2	0	N/A
Unexpected prize and lottery scams	$0	21	0	N/A
Other scams	$18 335	1 474	44 (3.0%)	▼-93.2%
Total	**$5 265 904**	**5 904**	**462 (7.8%)**	**▼-27.6%**


ACCC
AUSTRALIAN COMPETITION
& CONSUMER COMMISSION