ACCC
AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

Targeting scams

Report of the ACCC on scams activity 2020

June 2021

accc.gov.au

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

© Commonwealth of Australia 2021

This work is copyright. In addition to any use permitted under the *Copyright Act 1968*, all material contained within this work is provided under a Creative Commons Attribution 3.0 Australia licence, with the exception of:

- the Commonwealth Coat of Arms
- the ACCC and AER logos
- any illustration, diagram, photograph or graphic over which the Australian Competition and Consumer Commission does not hold copyright, but which may be part of or contained within this publication.

The details of the relevant licence conditions are available on the Creative Commons website, as is the full legal code for the CC BY 3.0 AU licence.

Requests and inquiries concerning reproduction and rights should be addressed to the Director, Content and Digital Services, ACCC, GPO Box 3131, Canberra ACT 2601.

Important notice

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

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

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

ACCC 06/21_21-30 www.accc.gov.au

Foreword

This report marks 12 years of the ACCC's annual Targeting Scams report. It provides insight into scam activity in 2020 – a year in which Australia faced a bushfire crisis and, along with the rest of the world, an unprecedented and disruptive pandemic (COVID-19).

Scammers unfortunately took advantage of the global environment, which led to higher than usual financial and personal information loss. However, alongside the stories of resilience and innovation in the community during the bushfires and the pandemic, we also saw increased collaboration across government, law enforcement and the private sector in response to the complex challenges that arose in the fraud and scam landscape. This unprecedented collaboration and focus provide optimism that if built on, can increase our resilience to make Australia a harder target for fraud and scam activity.

Scam losses and reports climb during the bushfires and COVID-19 pandemic

Australians lost over **$850 million** to scams and made 444,164 scam reports in total to Scamwatch, ReportCyber,[1] other government agencies, banks and payment platforms in 2020. Based on this combined data, the scams causing the most financial harm to Australians in 2020 were:

- $328 million lost to investment scams
- $131 million lost to romance scams
- $128 million lost to business email compromise (payment redirection scams).

Scamwatch.gov.au remains the primary government website where Australians report scams. Roughly 48% (216,087) of all scam reports were made to the ACCC's Scamwatch service, which is the highest number of reports since it commenced. Our previous research[2] shows that there are low levels of reporting to government, and that of all scam victims, around 13% report to Scamwatch. Consequently, the true amount lost to scams is likely to be considerably higher than that reported.

Whilst losses reported to Scamwatch increased 23% compared to the previous year, we had expected that the increase might be much higher due to the unprecedented nature of 2020. Globally, government and the private sector identified significant increases in scam and fraud activity during the pandemic.

Scammers were quick to take advantage of crises in Australia. Scammers set up fake charity scams in response to the bushfires and took advantage of pandemic related incentive schemes available in Australia. Levels of phishing activity increased to unprecedented levels as scammers sought personal information from Australian consumers and businesses to fraudulently access government programs.

The top 3 categories of reports to Scamwatch were phishing, threats to life, arrest or other (threat based scams) and identity theft. Reports in these 3 categories often involved the impersonation of government agencies to obtain personal information or demand money.

Phishing activity thrived during the pandemic. Over 44,000 reports were received, representing a 75% increase. Reports of threat based scams, which typically involve scammers threatening victims with arrest, deportation, legal action or excessive 'fees' unless money they claim is owed is paid, increased by 140% to just over 32,000 reports. There was a corresponding 178% increase in losses to these scams of $11.8 million. Similarly, identity theft reports increased by 84% to over 20,000 reports. A number of government taskforces and law enforcement noted the increase in crimes aimed at stealing personal information and connected this to conduct aimed at fraudulently accessing COVID-19 related initiatives such as early access to superannuation.

It is not surprising that in 2020, 25% of all scam reports involved the loss of personal information, up from 16% in 2019. Loss of personal information was even higher among Indigenous consumers, where 36% of all scam reports involved the loss of personal information. The increasing value of personal information at a time when face to face transactions were not possible was a significant driver of scam activity in 2020.

[1] ReportCyber is the reporting portal run by the Australian Cyber Security Centre at cyber.gov.au (previously ACORN).

[2] Roy Morgan ACCC scam survey 2019.

For the first time, Victorians had the highest reported losses to Scamwatch, with losses of $49,096,516 (an increase of 115% from 2019 losses). We believe this is likely attributable to the long lockdown periods the population experienced in 2020, which created opportunities for scammers as people were forced into unusual economic and social situations that had the potential to increase their susceptibility to scams.

While the ACCC, other government agencies and increasingly, the private sector, continue to take action to prevent and disrupt scams and to educate the public, we need to increase our efforts on all fronts to reduce the ongoing impact of scams in Australia. We also need to continue to focus on educating the public about the ways in which the government will legitimately make contact with them so they can avoid falling victim to these scams in future.

Increasing losses to investment scams

In 2020, combined financial loss to investment scams was a record $328 million.[3] For the banks, Scamwatch and ASIC it was the category with the highest losses. Scamwatch reports increased by 63% to 7,295 and losses rose slightly to $66 million. Almost 34% of people who reported an investment scam lost money, with an average loss of $26,713.

It appears to be increasingly difficult for people to identify legitimate investment opportunities from scams. Scammers no longer just rely on professional looking websites. They now have the ability to contact people through phone, apps, social media and other means. We saw more fraudulent celebrity endorsements of investment opportunities advertised across digital platforms as well as scammers posing as romance interests to 'bait' people into scam investments.

Romance baiting was a new type of scam that emerged in 2020 to target sections of the population which in the past have not typically suffered high losses to investment scams. Victims are contacted on a dating app, typically moved off the app and then lured into an investment scam, often involving cryptocurrency. People aged 25 to 34 years lost the most money ($7.3 million) to romance baiting in 2020.

Unsurprisingly, trends to perpetrate scams via less traditional payment methods continued in 2020. Whilst the highest reported losses are still experienced via bank transfers, we received reports of over $50 million in losses via Bitcoin or 'other payments'. These include cryptocurrencies such as Ethereum, charges to phone bills, Neosurf vouchers and digital payment apps such as Zelle or Skrill.

Ongoing collaboration and disruption is crucial

It can be very difficult to repair the damage inflicted by scams after they have occurred. Often funds and personal information cannot be recovered and it is typically extremely difficult for law enforcement and government agencies to identify and prosecute scammers, particularly as most are located overseas. Scams can also have significant impacts on mental health and relationships.

Thankfully it's not all bad news. Over the year there was an impressive amount of work to identify clever solutions which over the longer term will prevent or disrupt scams. In 2020, the ACCC was pleased to work closely with the ACMA and the telecommunications industry on a range of initiatives to address scams occurring over the telecommunications network. As a result, we have seen decreases in mobile porting fraud, Wangiri scams and made it harder for scammers to successfully use number 'spoofing' to trick people into believing they are from a government agency. We are keen to monitor the results from the new Reducing Scam Calls Code and hope to see a reduction in scam calls being carried over Australian networks in the coming year.

The ACCC has also had success in working with the Department of Home Affairs on a solution to improve outcomes for victims of identity compromise in Australia.

It is also pleasing to see more government investment in agencies like the Australian Cyber Security Centre and the Department of Home Affairs to deal with cyber security as well as government funding for important victim support services like IDCARE.

[3] Note: This was the first year that the ACCC included ASIC investment scams data showing losses of over $185 million.

On the theme of collaboration, I would like to thank all of the government agencies and businesses that provided data for this report and to welcome all of those that provided their data for the first time this year.[4] This is crucial as it helps us to more completely understand the extent of scam activity in Australia.

The figures in this report show there is still a lot of work to be done. The ACCC will continue to share scam reports with law enforcement and we are hopeful that the increased focus of government and law enforcement will result in more actions against scammers and better outcomes for victims.

We need to continue to collaborate more, share information and look for unique solutions utilising the combined knowledge and skills of law enforcement, government and the private sector, including platforms, to minimise future harm.

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

[4] Those that provided data for the first time for the Targeting scams 2020 report are: the Australian Securities and Investments Commission, Bendigo and Adelaide Bank, Suncorp-Metway Limited, Macquarie Group, the Bank of Queensland, MoneyGram and Western Union.

Contents

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 about how to recognise, avoid and report scams. We also share intelligence and work with government and the private sector to disrupt and prevent scams.

The ACCC outlines its approach to scams each year in its Compliance and Enforcement Policy, which contains a commitment to analyse and share Scamwatch data to identify trends, monitor financial losses and inform our scam prevention strategies. We undertake an annual review of our strategic approach to scams and consider whether there are any new initiatives we may be able to take to minimise harm caused by scams. Information about the activities we carried out in the fight against scams in 2020 is set out throughout this report.

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 risk of scams. We also prioritise targeted activities in response to emerging issues affecting vulnerable and disadvantaged consumers.

The ACCC focuses on scams disruption and prevention to minimise harm to Australians. As 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.

Notes on data in this report

The data in this report is from the calendar year 1 January to 31 December 2020.

All details in this report are based on reports made to Scamwatch, except where specified. References to combined reports or losses include data from Scamwatch, ReportCyber, other government agencies and financial institutions.

This year, the ACCC obtained data from other government agencies[5], 8 banks[6] and 2 remittance service providers 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 a fraction of the total losses suffered by Australians.

Scam victims often report their experience to more than one organisation, for example, Scamwatch and their bank. We have made all reasonable efforts to avoid counting reports or losses multiple times but we acknowledge some multiple counting of reports or losses may remain.[7]

Banks and payment platforms

Scam victims are more likely to report financial losses to their bank than anywhere else. In 2019, we obtained scam data from the big 4 banks to inform the Targeting Scams report for the first time. In 2020, we expanded this by obtaining and including data from an additional 4 banks and 2 remittance service providers.

We thank all of the contributing organisations for their participation and cooperation in the production of this report. The Australia and New Zealand Banking Group (ANZ), Commonwealth Bank of Australia (Commonwealth Bank), National Australia Bank (NAB), Westpac Banking Corporation (Westpac), Bendigo and Adelaide Bank, Suncorp-Metway Limited (Suncorp), Macquarie Bank Limited (Macquarie), Bank of Queensland Limited (BOQ), MoneyGram International (MoneyGram) and The Western Union Company (Western Union) all contributed data to this report.

ReportCyber

The Australian Cyber Security Centre (ACSC) is based within the Australian Signals Directorate (ASD). The ACSC's aim is to help make Australia the most secure place to connect online.

The ACSC provides advice and information about how to protect yourself and your business online through its website: cyber.gov.au.

On 1 July 2019, the ACSC launched the ReportCyber online reporting portal as a place to report cyber-dependent crimes (cyber.gov.au). The ACSC portal triages reports and refers some to the appropriate law enforcement jurisdiction for investigation. This report contains data extracted from ReportCyber for the period 1 January – 31 December 2020.

[5] Australian Communications and Media Authority, Australian Cyber Security Centre (ReportCyber), Australian Securities and Investments Commission, Australian Taxation Office, Services Australia and WA ScamNet, NT Office of Fair Trading and New South Wales Police.

[6] Australia and New Zealand Banking Group (ANZ), Commonwealth Bank of Australia (Commonwealth Bank), National Australia Bank (NAB), Westpac Banking Corporation (Westpac), Bendigo and Adelaide Bank, Suncorp-Metway Limited (Suncorp), Macquarie Bank Limited (Macquarie), Bank of Queensland Limited (BOQ).

[7] We note that the ACCC did not have the opportunity to deconflict or analyse data provided by ASIC. ASIC data is therefore included as provided by reporters.

Targeting scams 2020

Losses

$851 million

2020 combined financial losses to scams as reported to Scamwatch, ReportCyber (ACSC), ASIC, other government agencies and 10 financial institutions (ANZ, Commonwealth Bank, NAB, Westpac, BoQ, Bendigo and Adelaide Bank, Macquarie Bank, Suncorp, Western Union and MoneyGram)

$176 million

Amount reported lost to Scamwatch

216,087

reports to Scamwatch

2019
$143 m
2020
$176 m

▲ **23%** since 2019

Average loss: $7,677

Top 3 scams causing the most financial harm to Australians in 2020

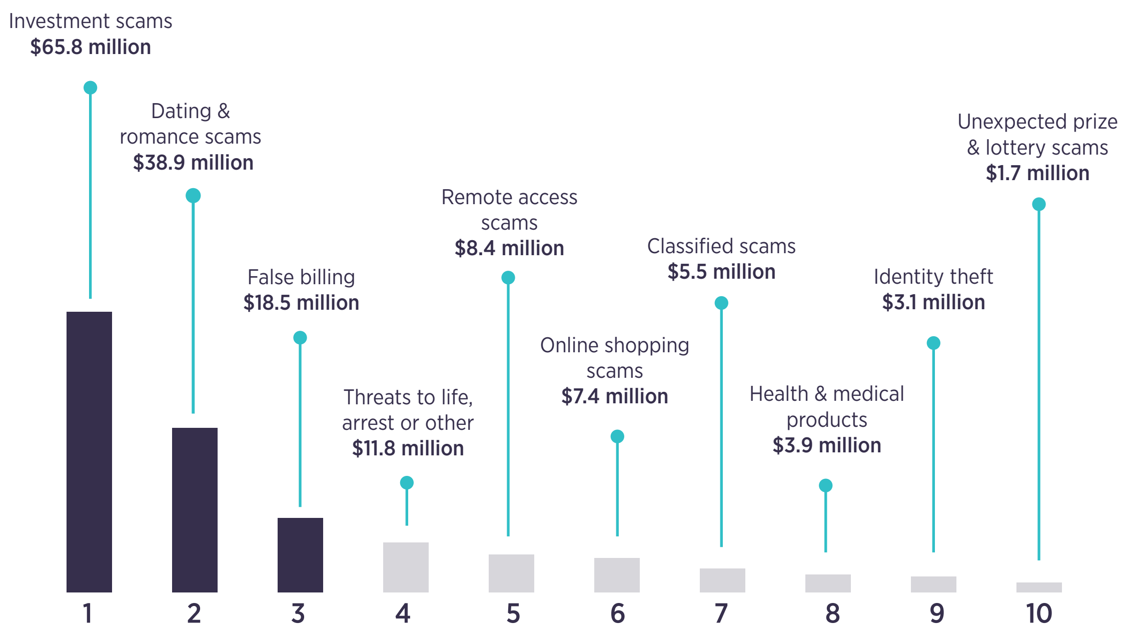
As reported to Scamwatch, ReportCyber, ASIC, other government agencies and 10 financial institutions (as above).

$328 million
lost to
investment scams

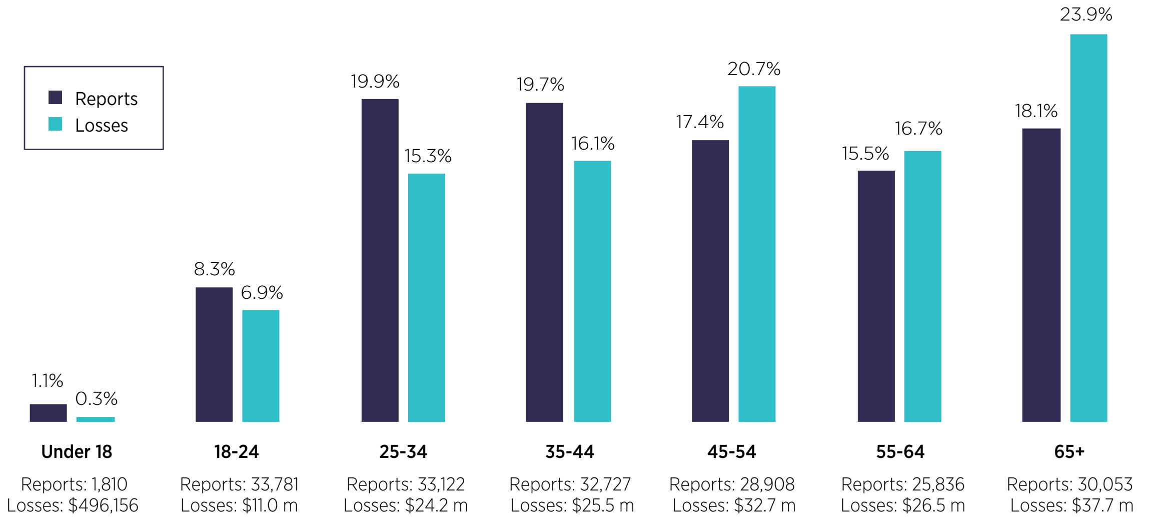
$131 million
lost to
romance scams

$128 million
lost to business
email compromise
(payment redirection scams)

Top scams by loss as reported to Scamwatch



Age



Note: Only Scamwatch reports where age was provided are included (n=166,237 $158,005,406). There were 49,850 reports that did not include an age category with losses of $17,678,685.

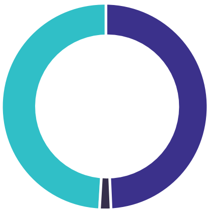
Gender

Male

$88 million

103,057 reports

Investment scams caused the highest losses – **$44.7 million**



Female

$87.4 million

108,995 reports

Dating and romance scams caused the highest losses – **$28.1 million**

Non-specified gender

$318,409

The highest losses were split between investment scams and dating and romance scams – **$69,514**

Top contact methods by reports

47.7%
Phone
103,153 reports
$48.2 million reported lost

22%
Email
47,503 reports
$35.2 million reported lost

15%
Text message
32,337 reports
$3.1 million reported lost

6.3%
Internet
13,636 reports
$26.7 million reported lost

4.5%
Social networking/ online forums
9,687 reports
$27.1 million reported lost

1. Executive summary

1.1 Key statistics 2020

- Scamwatch, ReportCyber, other government agencies, banks and payment platforms received a combined total of over 444,164 reports, with reported losses of over **$850 million** in 2020.
- Investment scams caused the most financial loss, with combined losses of **$328 million**. This was followed by romance scams with **$131 million** lost, and business email compromise with **$128 million** lost.
- Scamwatch received 216,087 scam reports in 2020, a 29% increase from the 167,797 reports received in 2019.
- Financial losses reported to Scamwatch totalled nearly **$176 million** in 2020. This is an increase of around 23% compared to the **$143 million** in losses reported in 2019.
- Investment scams and romance scams continued to cause the most financial loss reported to Scamwatch. **$66 million** was reported lost to investment scams and **$40 million** to romance scams.
- Scamwatch received the most reports about phishing scams (44,000). This was a 75% increase on the number of these reports in 2019 and was attributed to a rise in government impersonation scams during the COVID-19 pandemic.

1.2 The scams

COVID-19 scams

- The COVID-19 environment led to an increase in losses and reports for several categories.
- Compared with 2019, online shopping scam reported losses increased more than 52% to **$7.4 million**, remote access scam reported losses increased more than 74% to **$8.4 million,** threat based scam reported losses increased more than 178% to **$11.8 million** and classified scam reported losses increased more than 96% to **$5.5 million**.
- Health and medical scam reported losses increased more than 2,000% compared with 2019 as a result of the pandemic, reaching over **$3.9 million**.

Government impersonation scams

- In 2020, there were over 24,000 reports about government impersonation scams made to the ACCC, with losses of **$1.9 million**.
- Scammers often impersonate government agencies to seek a financial benefit or personally identifiable information from people.
- The most common government agencies impersonated in 2020 were the Australian Taxation Office, the Department of Home Affairs and Services Australia.

Superannuation scams

- In 2020, Scamwatch received over 1,500 reports of scams relating to superannuation, with over **$6.4 million** in losses.[8]
- In March 2020, the government announced new measures under its COVID-19 economic support package, allowing more individuals under 65 suffering financial hardship to access up to $10,000 of their superannuation in 2019–20 and a further $10,000 in 2020–21.

[8] Note: Not all of the losses related to COVID-19 specific scams.

- As soon as the announcement was made, Scamwatch saw an increase in phishing scams aimed at eliciting personal information, specifically superannuation details of peopled aged between 18 and 55 years.

Puppy scams

- Reported losses to puppy scams increased from $375,510 in 2019, to over **$2.2 million** in 2020.
- Puppy (and other pet scams) are not new. However, in 2020 reports quadrupled and losses to puppy scams more than quintupled from those reported in 2019. Reporters made 2,252 reports about puppy scams in 2020, compared with 498 in 2019.

Vehicle sale scams

- In 2020, the ACCC saw a 220% increase in reports and a 322% increase in reported losses to scams related to buying vehicles including cars, caravans and campervans, with reported losses of **$1,035,401**.
- Scammers targeted both people buying and selling vehicles and used legitimate websites such as Facebook Marketplace (facebook.com/marketplace), Gumtree (gumtree.com.au), Car Sales (carsales.com.au) and Autotrader (autotrader.com.au) to make contact with potential victims.

Bushfire scams

- The ACCC opened a hotline for people to report bushfire related scams, which received more than 1,000 calls between its opening on 6 January 2020 and closure on 27 March 2020.
- Scamwatch also received over 330 bushfire related Scamwatch reports through the website.
- Most bushfire scam related web reports concerned fake charity scams. The ACCC was able to shut down several fake bushfire charity and fundraising webpages on crowd-funding platforms and social media.

Romance baiting

- In 2020, people reporting to Scamwatch lost **$15.4 million** (from 414 reports) to scams involving romance baiting. This is where victims meet scammers on dating apps and are lured into investing in a cryptocurrency investment scam. This was by far the most common romance baiting scam type, with 57% of these scams luring victims into cryptocurrency investment scams.
- Younger people aged between 25 and 34 years lost the most money to scams using this technique (**$7.3 million**).

Chinese authority scams

- Scamwatch received 2,082 reports with reported losses of **$7,044,098** to Chinese authority scams in 2020. This was a 77% increase in the number of reports and a 250% increase in the amount reported lost compared with 2019.
- Most Chinese authority scams start as robocalls. These may impersonate the Chinese Embassy in Australia or, more commonly, a courier company.
- These scams used the fear associated with the pandemic to coerce people into paying money. Scamwatch received several reports of scammers pretending to be the Chinese Centre for Disease Control and Prevention or the Beijing Centre of Epidemic Prevention.

Celebrity endorsement scams

- Celebrity endorsement scams caused reported losses of over **$1.8 million** in 2020, an increase from the $1 million reported in 2019. Given the scale of individual losses reported in the media, we note that the actual losses to these scams were likely to be much higher.[9]
- A celebrity endorsement scam is usually where a scammer uses the image, name and personal characteristics of a well-known person to sell a product. The product might be health related – and with COVID-19 there were a few scams taking advantage of health concerns. Or, the scam could be an investment strategy, such as encouraging people to invest in cryptocurrencies.
- Celebrity endorsement scams were not new in 2020; however, the celebrities used by scammers changed. In 2020, with investment scams in particular, scammers moved away from using the likeness of individual celebrities and began using fake news articles impersonating well-known media sites, such as ABC News, The Project and News.com.au as a way to lure people into scams.

1.3 The people

- For the first time in over 5 years, men and women lost almost the same amount to scams. Men lost **$88 million** and women lost approximately **$87 million**.[10]
- Similar to previous years, men reported the highest losses to investment scams (**$44.6 million**), while women reported the highest losses to romance scams (**$28 million**).
- People aged 65 years and over reported higher losses than any other age group, with almost **$38 million** lost.
- Young people aged 25 to 34 years made the most reports to Scamwatch (33,000).
- One third of the 3,445 scams reported by Indigenous Australians involved the loss of personal information but overall losses decreased 4% to **$2 million**.
- For the first time, Victoria experienced the highest losses of all the states and territories, with reported losses to Scamwatch of **$49,096,516**. This was almost double the losses from 2019. We think it is likely that this is because Victorians were in lockdown for the longest period, which may have made people more susceptible to the scams described in chapter 3 of this report.
- NSW and Queensland experienced increasing losses and reports, while other states had less financial loss.
- Scamwatch received over 11,700 reports from people whose first language was not English, with losses of around **$22 million**. This was a large increase in terms of both reports and losses for this section of the Australian community.
- People with disability reported 7,543 scams, with losses of about **$10 million**. Romance scams caused almost half (**$5 million**) of this loss.

1.4 The businesses

- Scam losses reported by businesses increased by 260% in 2020, to **$18 million**[11] from $5 million in 2019. This was due to scams resulting in particularly high losses.
- Businesses made the most reports about false billing and phishing scams. These scams typically involve a request for payment for a service or item that wasn't ordered or a scammer diverting money by impersonating the intended recipient of a payment.

[9] For example, see Bitcoinwww.abc.net.au/news/2020-07-10/warning-over-Bitcoin-scam-using-celebrities-to-promote-product/12441920; and Bitcoinwww.theguardian.com/technology/2020/dec/14/scam-Bitcoin-ads-using-unauthorised-celebrity-images-fool-tens-of-thousands-of-australians, which both contain stories of individuals losing over $80,000.

[10] Reporters who did not identify as either male or female, or who chose not to disclose their gender, reported losses of $318,409.

[11] This total figure was impacted by a single report with a reported loss of $8 million.

- While combined losses to business email compromise scams decreased overall, Scamwatch received around 1,300 reports in 2020, with over **$14 million** in losses, compared to approximately 900 reports and $5 million in losses in 2019.

1.5 The payment and contact methods

- Bank transfer remained the most common payment method used in scams, with just over **$97 million** lost (a 40% increase).
- Bitcoin was the second highest payment method, with **$26.5 million** lost.
- Phone continued to be the most commonly reported contact method, with 103,153 reports and **$48.2 million** in financial loss (an increase of 48% above 2019).
- Contact by email and social networking continued to cause large losses, with **$35.2 million** lost for email across 47,503 reports and **$27.1 million** lost for social networking/online forums in 9,687 reports.
- Social media[12] remained the most common way that romance scammers find their victims, with **$14.3 million** lost.
- **$21.6 million** was reported lost to scams over mobile apps. This was an increase of 213% above 2019.
- Despite an increase in reports, losses to internet based scams decreased from **$31.6 million** in 2019 to **$27.6 million** in 2020.

1.6 The fight against scams

- In 2020, Scamwatch had 114,752 subscribers to its email alert service, with 14 alerts and 18 media releases issued.
- The Scamwatch website had 9 million page views, and the ACCC's *Little Black Book of Scams* was downloaded 12,714 times. We also distributed 54,684 physical copies of the book (in addition, some banks print their own copies to give to customers).
- The Scamwatch Twitter account grew by around 1,000 followers to 28,755. The account posted 247 tweets and 74 retweets alerting Australians to current scams in 2020.
- We responded to hundreds of media requests and kept 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.
- We set up a dedicated bushfire scams hotline between January and March 2020 and published warnings about these scams in the media and on our Scamwatch and Twitter accounts.
- In response to the COVID-19 pandemic, we increased our monitoring of Scamwatch reports to quickly identify high risk scams and take action to disrupt them, such as contacting the Australian Cyber Security Centre to arrange takedowns and issuing public warnings and information.
- Scams Awareness Week ran in August 2020 with the tag line 'Be yourself. Don't let a scammer be you'. The campaign was headed by the ACCC as Chair of the SAN and focused on educating people on how to protect their personal details. A podcast series entitled 'This is not your life' was released as part of the campaign.
- We continued sharing scam intelligence with the private sector, including platforms. By sharing targeted scams intelligence with these businesses, we were able to help them build front-end scams disruption measures to prevent further harm to Australians.
- We continued to share Scamwatch reports with government partners and law enforcement.
- During COVID-19, the ACCC was a key source of information about scams in its role on various taskforces and forums including the Criminal Justice and Law Enforcement Forum and the COVID-19 Counter Fraud Taskforce.

[12] We note that the field selected in response to 'How were you contacted by the scammer' on the Scamwatch report form is 'Social networking/Online forums'.

- We continued our involvement with the Australian Communications and Media Authority's (ACMA) Scam Technology Project. In 2020, both the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 and the Reducing Scam Calls Code were introduced. The Minister for Communications, Urban Infrastructure, Cities and the Arts recently announced that Australian telecommunications providers had blocked 55 million calls as a result of this work.[13]
- The ACCC also played an active role in the Scam Telecommunications Action Taskforce by providing data to assist telecommunications service providers to meet their obligations under the Reducing Scam Calls Code.
- In 2020, the 10 banks/financial institutions that provided data for this report saved nearly $208 million from being sent to scammers. In addition to that amount being prevented or recovered from scammers, these financial institutions also refunded almost $49 million to customers who were the victims of scams.

[13] www.minister.infrastructure.gov.au/fletcher/media-release/millions-scam-calls-stopped#:~:text=The%20Morrison%20Government%20is%20serious,to%20comply%20with%20the%20code.

2. Scam activity in 2020

2.1 Combined data – the bigger picture

Research commissioned by the ACCC in 2019 tells us that Scamwatch is just one of many places people report scams, and only a third of people who respond to a scam go on to report that scam to a government agency.[14]

To better understand the impact of scam activity in Australia, the ACCC obtained scam data from 10 financial institutions as well as ReportCyber, the Australian Taxation Office (ATO), Services Australia, the Australian Securities and Investments Commission (ASIC), WA ScamNet and the Australian Communications and Media Authority (ACMA). The combined losses reported to Scamwatch and these other organisations in 2020 was just over $850 million across 444,164 reports. Scamwatch received the largest number of reports.

Table 2.1: Losses reported to all agencies and banks

Agency/organisation	Reports	Losses
Scamwatch	216,087	$175,684,091
ReportCyber	58,120	$338,695,650
Banks/financial institutions	59,751	$345,521,544
ATO	96,220	$2,400,000
Services Australia	11,689	N/A
WA ScamNet	3489	$11,812,023
ACMA	14,475	N/A
ASIC	2,352	$186,690,976[15]
Adjustments for possible duplications*	-20,930	-$209,405,861
Total	**441,253**	**$851,398,423**

*Note: These totals have been adjusted to take account of duplications where the same incident has been reported to multiple agencies.

Scams reported to financial institutions and money remitters

ANZ, Commonwealth Bank, NAB, Westpac, Bendigo and Adelaide Bank, Macquarie Bank, BOQ, Suncorp-Metway Limited, Western Union and MoneyGram provided high level anonymised data about the reports and losses their customers experienced in 2020.

Overall, the above financial institutions received and detected 59,751 cases with around $345 million in losses. The top 5 scams reported to banks were investment scams, business email compromise scams (BEC), remote access scams, romance scams and buying and selling scams. The most common ways people paid money to scammers were bank transfers and Bitcoin.

[14] Roy Morgan ACCC scam survey research 2019.

[15] ASIC's reported losses were distributed between a number of categories including investment scams, fake credit/loan scams, money transfer schemes and fake/debt invoice scams.

Table 2.2: Highest scam losses reported to banks and government

Scam type	Scamwatch	ReportCyber*	Bank losses	ASIC	Total[16]
Investment scams	$65,820,313	$6,806,439*	$89,339,207	$185,394,786[17]	$328,091,449
Dating and romance scams	$38,916,120	$27,871,737	$92,486,588	N/A	$131,976,234
BEC scams	$14,115,692	$75,704,868	$73,901,297	N/A	$128,415,400
Shopping scams	$12,914,146	$55,239,943	$10,523,027	N/A	$62,147,260

*Note: The investment scam figure provided for ReportCyber in table 2.2. is only for a period of 2 weeks in December 2020. Prior to this period, ReportCyber did not have an investment scam category for the purpose of reporting. Therefore, we expect that the actual losses to investment scams are likely to be considerably higher than those set out in the table above.

Losses reported to business email compromise was the only category in the top 4 that decreased in 2020.

2.2 Scamwatch statistics in 2020

The ACCC received 216,087 scam reports in 2020, with reported losses of nearly $176 million. Reports increased by 29% compared to 2019, and financial losses increased by 23%.

Table 2.3: Scam category by losses in 2020

Scam category	Reports 2020	Reports with loss 2020	Reported losses 2020	2019 losses	Change in losses since 2019
Investment scams	7,295	2,464	$65,820,313	$61,813,401	6.5%
Dating & romance scams	3,708	1,289	$38,916,120	$28,606,215	36.0%
False billing	13,120	1,799	$18,464,903	$10,110,756	82.6%
Threats to life, arrest or other	32,215	558	$11,833,508	$4,255,389	178.1%
Remote access scams	8,473	667	$8,441,632	$4,836,812	74.5%
Online shopping scams	15,306	8,349	$7,384,733	$4,845,452	52.4%
Classified scams	7,928	2,497	$5,529,413	$2,816,076	96.4%
Health & medical products	1,459	382	$3,915,689	$179,639	2,079.8%
Identity theft	20,939	673	$3,072,287	$4,311,066	-28.7%
Unexpected prize & lottery scams	4,543	298	$1,706,253	$2,385,669	-28.5%
Phishing	44,079	696	$1,689,406	$1,517,864	11.3%
Inheritance scams	1,676	59	$1,434,544	$2,622,355	-45.3%
Hacking	8,691	425	$1,419,353	$5,139,414	-72.4%
Jobs & employment scams	2,933	290	$1,268,582	$1,727,381	-26.6%
Betting & sports investment scams	448	150	$985,926	$1,205,001	-18.2%
Nigerian scams	577	92	$896,115	$1,066,838	-16.0%
Overpayment scams	1,658	358	$701,729	$1,114,880	-37.1%
Rebate scams	1,827	91	$701,250	$220,648	217.8%
Pyramid schemes	406	85	$286,107	$1,669,618	-82.9%
Scratchie scams	143	14	$243,348	$419,336	-42.0%
Psychic & clairvoyant	230	90	$230,273	$452,811	-49.1%
Mobile premium services	1,523	148	$141,549	$188,778	-25.0%
Fake charity scams	1,425	139	$133,214	$411,588	-67.6%
Ransomware & malware	3,885	42	$74,076	$156,569	-52.7%
Travel prize scams	151	17	$11,754	$360,151	-96.7%

[16] These totals have been adjusted to take account of duplications where the same loss has been reported to multiple agencies.

[17] Whilst ASIC does not have reported losses listed in any other categories in table 2.2, it also received reports of losses of $857,195 to fake credit/loans, $289,750 to money transfer schemes and $149,245 to fake debt/invoice scams.

Other scams	31,449	1,213	$382,014	$462,065	-17.3%
Total	**216,087**	**22,885**	**$175,684,091**	**$142,895,772**	**22.9%**

Scamwatch categories with the highest losses in 2020

The 3 scams with the highest reported losses in 2020 were investment scams, dating and romance scams and false billing.

Losses to investment scams increased from $62 million in 2019 to $66 million in 2020. Reports of investment scams increased by 63% over 2020, with 7,295 reports received compared to 5,005 in 2019. Almost 34% of people who reported an investment scam lost money, with an average loss of $26,713.

Almost $39 million was reported lost to dating and romance scams in 2020, a 36% increase from 2019.

Losses to false billing scams, which typically involve a request for payment for a service or item that wasn't ordered or a scammer diverting money by impersonating the intended recipient of a payment[18], increased by roughly 87% in 2020 to $18 million.

The most reported scam categories in 2020

The 3 most reported scams of 2020 were phishing, identity theft and threat based scams.[19]

Scamwatch received over 44,000 reports of phishing scams in 2020, with almost $1.7 million in losses reported. Many of these were government and other impersonation scams. As phishing scams frequently involve personal information theft, there are often ongoing financial losses inflicted on victims and therefore it is difficult to capture the full extent of losses to these scams.

Scamwatch received over 32,000 reports about threats to life, arrest or other, with almost $12 million in losses in 2020. This represented an increase in losses of 178%. Many of these targeted young people in the Chinese community.

Almost 21,000 reports of identity theft were received, which represents an increase of 84% compared to 2019. Identity crime was a key theme of Scams Awareness Week 2020. Common methods of identity theft reported included phishing, hacking, remote access scams, malware and ransomware scams, and fake online profiles.

Payment methods

In 2020, the highest reported losses were via bank transfers, Bitcoin and other payments. The 'other payments' category includes cryptocurrencies aside from Bitcoin such as Ethereum, as well as charges to phone bills, Neosurf vouchers, digital payment apps such as Zelle or Skrill and even goods and items sent but not paid for by scammers.

As banks move towards more real time payments, there is a greater need for real time solutions that can identify and halt scam transactions via bank transfers. In addition, the ACCC notes that better processes could be developed to alert customers when an account number does not match a name.

The ACCC considers that initiatives similar to the UK's Confirmation of Payee[20] could assist to reduce some of the losses occurring by bank transfer and has advocated for the adoption of a similar system in our recent submission to the Review of the Australian Payments System. In order for name matching on bank transfers to be effectively implemented in Australia, there would need to be an overlay of the functionality that checks name against account number onto the traditional banking system.

[18] For a more detailed explanation of these scams, please refer to the Glossary section of this report.

[19] We note that the field selected in response to the 'What type of scam is it' question on the Scamwatch report form is 'threats to life, arrest or other'.

[20] www.ukfinance.org.uk/confirmation-of-payee. The ACCC advocated for similar initiatives in a submission to ASIC's Review of the ePayments Code.

We believe this would be particularly useful in disrupting payment redirection scams[21] and would also provide limited protections for consumers from other types of fraud such as romance scams or online shopping scams where scammers are impersonating a specific individual.

Bitcoin and other payment methods are now common ways for scammers to receive money. The perceived anonymity of unregulated cryptocurrencies can impede the ability to recover funds or identify scammers. It is likely that we will see increased use of Bitcoin and other cryptocurrencies in the years to come.

Table 2.4: Payment methods, reports and losses by highest loss

Payment method	2020 Reports	Reported losses 2020
Bank	8,215	$97,656,013
Bitcoin	1,985	$26,653,070
Other payment method	2,680	$24,178,938
Cash	1,278	$8,571,992
Credit Card	6,267,	$8,108,346
Money Transfer Services*	499	$3,612,110
Paypal	2,761	$1,639,662
Other gift cards	844	$1,630,080
iTunes gift card	428	$853,190
Australia Post Load & Go prepaid debit	98	$243,055
Google Wallet	68	$100,958
UKASH	5	$6,751
Payment method not provided/NA	190,959	$2,429,926

*Note: Including World Remit, MoneyGram, Western Union

We note that 'Other gift cards' in the table above includes cards such as Google Play, Steam and Amazon gift cards.

Data from banks & money remitters

ANZ, Commonwealth Bank, NAB, Westpac, Bendigo and Adelaide bank, Macquarie Bank, BOQ and Suncorp-Metway Limited, as well as Western Union and MoneyGram, provided high level anonymised data about the reports and losses their customers experienced in 2020.

Overall, these financial institutions received a combined total of 59,751 reports, with $345 million in reported losses. The most common scams were generally also the most financially harmful. Investment scams, business email compromise scams, remote access and romance scams were some of the most commonly reported scams to banks and payment providers and also caused substantial losses to customers across the financial institutions.

Table 2.5: Aggregate bank reports and losses

Category	Number/losses
Scams reported by customers	17,274
Scams detected by bank/financial institution	39,835
Total scams cases	59,751[22]
Scam reports with a loss	18,775
Losses	$345,521,544[23]

[21] Please refer to the Glossary for the definition of these scams.

[22] This total includes reports where the financial institution did not capture if the case was reported by a customer or detected through other means.

[23] One financial institution provided all losses in $USD. For the purposes of this report, we used a historic currency exchange converter to convert to $AUD as of 31 December 2020: www.x-rates.com/historical/?from=USD&amount=62230033&date=2020-12-31.

Table 2.6: Top 6 scams in terms of reports to banks

Scam type	Reports	Losses
Investment scams	1,862	$89,339,207
BEC	1,900	$73,901,297
Remote access scams	5,315	$28,364,543
Romance scams	1,531	$27,871,737
Buying and selling scams	991	$10,523,027
Threats/immigration/extortion scams	312	$4,728,841

▶ **In 2020, 10 banks/financial institutions saved nearly $208 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, that is, where a financial institution was able to recall a payment from an account that was suspended or halted as suspected as being involved in a scam. In addition to that amount being prevented or recovered from scammers, financial institutions also refunded almost $49 million to customers who were victims of scams.**

All reputable banks should have dedicated teams to investigate potential scam and fraud transactions, and many do. They should also invest in scams awareness activities for staff and customers. This is important as 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 faster 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.

Contact methods

Phone continues to be the most common way scammers target victims and the most successful in terms of the amount of financial loss. Both reports and losses to scams conducted over the phone increased by 48% compared to 2019. Losses to phone based scams increased to just over $48 million.

Phone, email and text messages were the top 3 ways scammers made contact with people in 2020. Phone based scam reports made to Scamwatch peaked in October 2020 with about 17,000 reports that month.

2020 also saw an increase of 213% in losses to scammers using mobile apps when compared to 2019. There was also an increase in losses to scams conducted via email (24% increase from 2019) and social networking/online forums (22% increase from 2019). Again, this may be attributable to the COVID-19 pandemic as people spent more time on their devices due to lockdowns.

Table 2.7: Contact methods, reports and losses by highest loss

Contact mode	2020 Reports	Reported losses 2020
Phone	103,153	$48,240,921
Email	47,503	$35,231,831
Social networking/Online forums	9,687	$27,128,296
Internet	13,636	$26,712,164
Mobile apps	4,348	$21,677,361
In person	1,814	$11,218,706
Text message	32,337	$3,091,790
Mail	2,625	$2,267,222
Fax	109	$52,428
Not provided	875	$63,372

Scam reports made to the ACMA

The ACMA manages the spam intelligence database and receives complaints about scams (mainly phone scams). The ACMA received 14,475 scam reports in 2020, the vast majority (80%) of which were about scams conducted by phone. Of these, the most common scam was the NBN Co robocall scam, with 2,690 reports. This was also the most common scam reported to the ACMA in 2019, but with significantly more reports (4,548) in 2020.

The top 5 scam categories reported to the ACMA were scams impersonating NBN Co, a scam related to Amazon, computer virus and tech support scams, Telstra related scams and Chinese authority robocalls.

The response to increasing phone scam activity

In December 2018, the ACMA established the Scam Technology Project to tackle phone scams. Since its inception, the ACCC's Scamwatch team has been a key partner in the project alongside the Australian Cyber Security Centre, other government agencies, such as the ATO, and telecommunications providers. In late November 2019, the ACMA released the Combating Scams Action plan.[24]

The plan proposed initiatives aimed at reducing common phone scams, including scams where the calling line identification has been over stamped or spoofed, and Wangiri scams.[25] The third action point was trialling a Do Not Originate list with the ATO to prevent scammers from spoofing legitimate ATO phone numbers.

2020 saw the implementation of these initiatives culminate with 2 milestones: the introduction of the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 and the registration of the Reducing Scam Calls Industry Code.

The Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 was introduced to improve identity verification requirements and reduce the ability for scammers to commit mobile porting scams and fraud.

Each month, under the ACCC's Intelligence Sharing Project, we share Scamwatch reports of phone porting (changing ownership of a mobile number between telecommunications service providers) and sim-swapping (changing the currently active sim card for a mobile number with the same telecommunications service provider) with the ACMA.

Under the Reducing Scam Calls Industry Code, telecommunications providers are required to:

- monitor and detect scam call traffic on their networks
- share scam call data with other telecommunications providers
- verify, trace and block scam calls
- refer scam calls and/or perpetrators to authorities
- provide advice and information to customers.

[24] A publicly available summary of the Combating Scams Action Plan is available at www.acma.gov.au/sites/default/files/2020-10/Combating-Scams-summary-report.pdf.

[25] Please refer to the Glossary section of this report for a definition of Wangiri scams.

Since 2019, the ACCC has been providing scam telephone numbers to Telstra so it can investigate and find ways of blocking and tracing the calls. In August 2020, we sought feedback from Telstra on how this data was being used. Telstra reported that from mid-May 2020 to the beginning of August 2020, as a direct result of ACCC data sharing:

- 600,000 attempted scam calls (from 10 different numbers) were blocked by Telstra
- 4.2 million potential scam calls (from 102 different numbers) were identified but the numbers used to make the calls were engaged or disconnected when investigation was attempted. Telstra noted the numbers were theoretically usable for trace back processes. This was before the Reducing Scam Calls Code placed obligations for further investigation onto the providers, and so no further investigation occurred.

In 2020, we expanded our data sharing to a further 4 telecommunications providers.

To assist businesses in meeting their obligations under this Code, the ACCC now provides regular reports of telephone numbers that have been reported to Scamwatch as relating to a scam call on at least 2 occasions to a number of Communications Alliance members. We also share telephone numbers contained in scam reports relating to COVID-19 that appear more than once, including those reported to us by other agencies.

The Minister for Communications, Urban Infrastructure, Cities and the Arts recently announced that telecommunications providers had blocked 55 million calls. These blocked scam calls were described as being Wangiri scams (11 million) or from made-up or spoofed numbers (44 million).[26]

The ACCC will continue its work with the ACMA and telecommunications service providers to find solutions to scams utilising telecommunications networks and hopes to expand its data sharing arrangements in 2021.

▶ Case study 2.1: Phone porting – a good news story

In 2020, the ACCC focused attention on scams targeting personal information and other forms of identity crime.

The number of reports made to Scamwatch about identity theft in 2020 increased by 84% (20,939 reports) from the 11,373 reports made in 2019. However, losses to identity theft scams dropped from $4.3 million in 2019, to $3.1 million in 2020. The change in losses is due in part to new rules introduced by the ACMA in April 2020.[27] The new rules commenced on 30 April 2020 and require all mobile carriage service providers to use additional identity verification before a mobile number is ported from one provider to another.

The changes also appear to have impacted the losses associated with identity theft reported to the ACCC. In 2019, losses of $1.1 million were due to phone porting scams reported to Scamwatch. In 2020, the losses associated with phone porting scams decreased to just over $540,000.

Social media scams

For several years Scamwatch has highlighted the increasing reports and losses about scams on social media.

Scams using social media are diverse. The most common scams take place on popular platforms such as Facebook (including Facebook Marketplace and Messenger), Instagram and online dating sites. The Scamwatch reporting form has 3 contact modes where social media platforms may be selected: internet, mobile apps and social networking/online forums. People reported a variety of platforms to Scamwatch in terms of where they first met the scammer or engaged with the scammer.

[26] www.minister.infrastructure.gov.au/fletcher/media-release/millions-scam-calls-stopped.

[27] 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.

We analysed reports where the contact method was social networking/online forums. Reports using this contact method increased from 8,194 reports in 2019 to 9,687 reports in 2020 (an increase of over 18%). Losses have also increased for this contact mode, from $22 million in 2019, to $27 million in 2020 (an increase of over 22%).

The most common types of scam reported as occurring on social media sites in 2020 included:

- fraudulent fundraising pages (primarily related to bushfires)
- advertisements of fraudulent products or services
- contacts from scammers informing recipients they had won non-existent lotteries or grants. In some cases scammers impersonated the friends of the victim
- fake news articles
- Bitcoin investment scams
- romance scams.

Overall social media scam use

- In general, the platforms most commonly selected in social networking/online forums remain Facebook and Instagram. Both platforms saw moderate increases in the number of reports between 2019 and 2020. In 2020, we received 4,973 reports (51.3% of all reports in the category) providing this contact method and listing Facebook as the platform on which the scammer made contact. We received 1,522 reports listing Instagram (15.7% of all reports in this category) in the same way.
- The ACCC continues to share scam reports occurring on Facebook with the platform (where the reporter consents to do so) on a daily basis, expecting that it will take action to warn users and remove scammers from its platform.
- Losses are not instructive in this subcategory. This section's analysis only considers scam reports that list the contact mode as social networking/online forum, whereas many reports will consider Facebook to be a website or a mobile application. Further, the current reporting form only allows for listing of a single platform in each report. This means some scams are captured imperfectly; romance scams beginning on Tinder then moving to WhatsApp will only be listed under one of the platforms.
- However, the noted increases and ongoing high numbers of reports on the specified platforms accurately reflect significant usage of these platforms by scammers.

Increase in scammers using WhatsApp and Tinder

WhatsApp

- In 2019, WhatsApp was not provided as a pre-populated dropdown menu option for the social networking/online forums category. However, an examination of reports where the user selected the 'other' or 'blank' subcategories of social networking/online forum contacts in 2019 uncovered 104 reports where WhatsApp was the contact mode.
- We added WhatsApp as an option in the reporting form in 2020. We received 347 reports selecting WhatsApp from the drop down menu, and found an additional 50 reports from the 'blank' subcategory where WhatsApp was the platform on which the contact occurred (a combined 272% increase in reports).
- Generally, WhatsApp continues to be a secondary platform in scams. Scammers often attempt to perpetrate romance scams or investment scams by making contact in a different way (for example, via a dating app), then encouraging potential victims to continue their communication on the encrypted WhatsApp platform. The increase between 2019 and 2020 largely concerned reports of this sort, but 2020 saw a handful of dedicated spam campaigns unique to the platform. One example offered grocery vouchers for major Australian stores if users filled in personal information including details of their superannuation account(s).

Tinder

- Scam reports listing the contact mode as social networking/online forum and identifying the platform as Tinder increased from 73 in 2019 to 174 in 2020. This 138% increase in reporting was primarily in relation to romance scams, but also included investment scams where scammers encouraged victims to invest in cryptocurrencies.

The ACCC is continuing to address social media platforms through its work on digital platforms. The Final Report of the Digital Platforms Inquiry was published in June 2019 and contains recommendations of relevance to scams on social media platforms.[28] Of particular relevance are:

Recommendation 22: Digital platforms to comply with internal dispute resolution requirements

- The development of minimum internal dispute resolution standards by the ACMA to apply to digital platforms.
- The standards should, among other things, set out requirements for the visibility, accessibility, responsiveness, objectivity, confidentiality and collection of information of digital platforms' internal dispute resolution processes. They should also set out the processes for continual improvement, accountability, charges and resources.
- All digital platforms that supply services in Australia, and have over one million monthly active users in Australia, will be required to comply with the standards.
- Once published, relevant digital platforms will have 6 months to comply with the standards.
- Breaches of the standards would be dealt with by the ACMA, which will be vested with appropriate investigative and information gathering powers and the capacity to impose sufficiently large sanctions for breaches to act as an effective deterrent.

Recommendation 23: Establishment of an ombudsman scheme to resolve complaints and disputes with digital platform providers

- The establishment of an independent ombudsman scheme to resolve complaints and disputes between consumers and digital platforms, and businesses and digital platforms.
- The ACMA and the relevant ombudsman will determine the nature of complaints and disputes that would be subject to the scheme.
- At a minimum, it should cover complaints or disputes from businesses relating to the purchase or performance of advertising services and complaints or disputes from consumers, including in relation to scams and the removal of scam content.

[28] www.accc.gov.au/system/files/Digital platforms inquiry - final report.pdf.

3. The impact of the COVID-19 pandemic

It is well recognised that the pandemic was (and continues to be) more than just a health and economic crisis. 2020 was a year of unprecedented challenges. The pandemic disrupted governments, economies, health systems and individual movement throughout the world. It inevitably influenced the nature of crime and fraud by creating new opportunities for criminals to exploit vulnerabilities in individuals and in business and government communications and processes. Scammers were quick to take advantage of the change and uncertainty that dominated most people's lives throughout the year.

3.1 Changing scam activity

As parts of Australia went into lockdown, people were required to make drastic changes to the way they lived and worked. In Victoria, restrictions continued for much of the year. This meant more people were online more often, relying on internet based and app services they may not have used before to connect socially, to work remotely and to shop or obtain services such as (tele) healthcare. Many Australians also lost their source of income either temporarily or permanently and many businesses were unable to continue operating. People who had not expected to need government services were forced to access programs such as JobSeeker or JobKeeper or apply for early access to their superannuation or access small business grants.

Unfortunately, scammers identified the opportunity to take advantage of these changes and early in the pandemic there was an increase in phishing activity aimed at obtaining personal information. The increase in phishing scams in the context of increased government communication made it harder for the general public to identify what was real and what was fake, which often led to scammers accessing valuable personal information.

Scamwatch monitored scam activity closely during the pandemic and received over 5,400 scam reports directly mentioning COVID-19, with over $6 million in reported losses between February and December 2020.

However, the COVID-19 environment saw increases in reports and losses across many scam categories as well as decreases in others. Key trends are outlined further below.

Government impersonation scams

In 2020, over 24,080 government impersonation scams were reported to the ACCC, with losses of almost $2 million.

Government impersonation scams generally rely on fear, intimidation and the desire people have to comply with authority, to deceive people into parting with their money.

Government agencies commonly impersonated in scams in 2020

- Australian Tax Office (ATO): Contact was generally made over the phone. The scammer asked for payment of an outstanding tax debt and threatened arrest or legal action.
- ATO: Scammers sent text messages saying the recipients were eligible for tax refunds and provided a URL to click on to complete a security check to claim the refund. The URL was https://ato.-gov.au.taxreturn.link/claim. Note the '-' before gov.au, which identifies that this is not a legitimate government URL. There was no refund available; rather, the link was designed to capture personal information that scammers could then use to impersonate the victim to access government benefits or incentives.
- Department of Home Affairs: Contact was made by phone, often via a robocall advising that the recipient was under investigation and to press 1 to speak to an investigator. These scams sought immediate payment of money.

- Department of Home Affairs or the Australian Federal Police: Contact was made via phone advising the recipient of problems with their immigration papers or visa status and threatening deportation unless fees were paid.
- Services Australia: In this phishing campaign, which was designed to obtain information to access superannuation, scammers sent emails offering a subsidy grant and requesting personal identification information to claim the grant.
- Fake government organisations: Scammers also invented government agencies, such as the 'Commonwealth Grants Department'. Scammers phoned victims advising they were entitled to a rebate for paying their bills on time. The scammers sought credit card or bank details and personal information from victims.

In response to these scams, the ACCC monitored scam reports and quickly reported instances of impersonation to agencies such as Services Australia, the ATO, the Department of Home Affairs and other government agencies impersonated by scammers so that warnings could be delivered promptly to the public. Scamwatch reports were also shared with relevant government and law enforcement agencies where consent was provided.

Throughout 2020 the ACCC issued media releases[29] and tweets warning consumers about scams emerging or increasing in response to COVID-19. For example, in November 2020 we published a media release about threat based scams, and throughout 2020 Scamwatch tweeted about government impersonation scams with real examples and screenshots as provided in scam reports.[30]

Australian Taxation Office reports

Many scams impersonate the ATO and are reported to the ATO. In 2020, the ATO received 96,220 scam reports. Of those, 457 victims lost money, totalling nearly $2.4 million. This was a decrease in reports (10%) as well as a decrease in the number of reporters who lost money to scammers (28%) from 2019. However, there was a 12% increase in the overall amount reportedly lost to scammers in 2020.

People aged 25 to 34 years continued losing the most money to tax scams. The ATO also observed a number of concerning new scam trends in 2020:

- Scammers took advantage of the bushfire crisis from January to March 2020 by targeting victims offering a bonus on their 2020 tax returns.
- There was a sharp rise in COVID-19 myGov text message phishing scam campaigns in April as stimulus packages (JobKeeper and Early Release of Super) were announced late March. These campaigns saw large volumes of text message and email phishing scams linked to fake myGov log on websites. These scams looked as though they had been sent from a myGov or ATO email address or phone and some appeared in clients' legitimate ATO or myGov text message threads. These scam campaigns sought to harvest people's personal information including myGov login credentials, banking details, driver licences, passports and credit cards. One scam campaign went even further, asking victims to take a photo of themselves holding their documents to verify authenticity.
- Scam report volumes more than doubled in May. The fake tax debt phone scam made a significant resurgence, possibly due to the easing of global COVID-19 restrictions. Under this scam, scammers pretending to be from the ATO contacted members of the community, telling them that they had a tax debt and that if they did not pay it straight away, they would be arrested. This scam remained one of the ATO's highest reported scams until the end of 2020.

[29] Refer to Appendix 4 for a complete list of the media releases the ACCC issued in 2020 which related to scams.

[30] Scamwatch only shares this information when consent is provided to share anonymously.

Case study 3.1: WA ScamNet assists in returning funds to ATO impersonation scam victim

Victims of an ATO impersonation scam received cold calls from random numbers stating that the caller was from the ATO. The caller stated there were frauds being committed under the victim's name and threatened them with a warrant for their arrest. The victim was then asked where their nearest police station was and told that someone from the station would call them soon to discuss the issue.

The victims then received a call from what appeared to be the number of their local police station. The caller represented themselves as a police officer, stated they were investigating an issue with their linked bank accounts and that it appeared they were in the midst of illegal activity.

In one instance, following this series of phone calls, a victim went to 2 stores to purchase Google Play cards. At the first store she purchased $600 worth of cards and then at the second store, a total of $1,000 worth of cards. At the second store staff questioned why she was buying the cards. The victim was on the phone to the scammers whilst she was buying the cards. The staff member took the phone and told the scammers to leave the victim alone. The victim left the store but then went back afterwards seeking a refund but was refused by both stores. She had not scratched the cards or given the codes to the scammers.

The victim reported the scam to WA ScamNet. WA ScamNet contacted the relevant stores to discuss the scam and seek a remedy for the victim, given that the cards had not been used. After liaising with the stores, WA ScamNet was able to attain a full refund for the victim.

The retailer affected sent information to all their stores on the process for assisting victims of these scams and providing refunds where possible, especially where gift cards have not been redeemed.

WA ScamNet also updated their website with information about this scam, sent out social media alerts and issued a media release to warn consumers.

Superannuation scams

In 2020, Scamwatch received 1,530 reports of scams related to superannuation, with $6.4 million in losses reported. Many of these reports related to COVID-19 and the attempts by scammers to obtain personal information and access superannuation.

Australia's superannuation schemes are one of the country's largest sources of wealth, totalling $3 trillion at December 2020.[31] Australians aged between 55 and 60 years or over can access their super (depending on their preservation age).[32]

In March 2020, the government announced new measures under its COVID-19 economic support package, allowing more individuals under 65 years experiencing financial hardship to access up to $10,000 of their superannuation in 2019-20 and a further $10,000 in 2020–21. The new measure commenced in mid-April and applied to people who had been made unemployed or who had their income reduced by 20% or more.

As soon as the announcement was made, scammers began exploiting the new measures, which resulted in people losing money from their superannuation. Typically scammers first gained access to personal information through phishing scams or data breaches. They then used the information to impersonate the victim to withdraw their super.

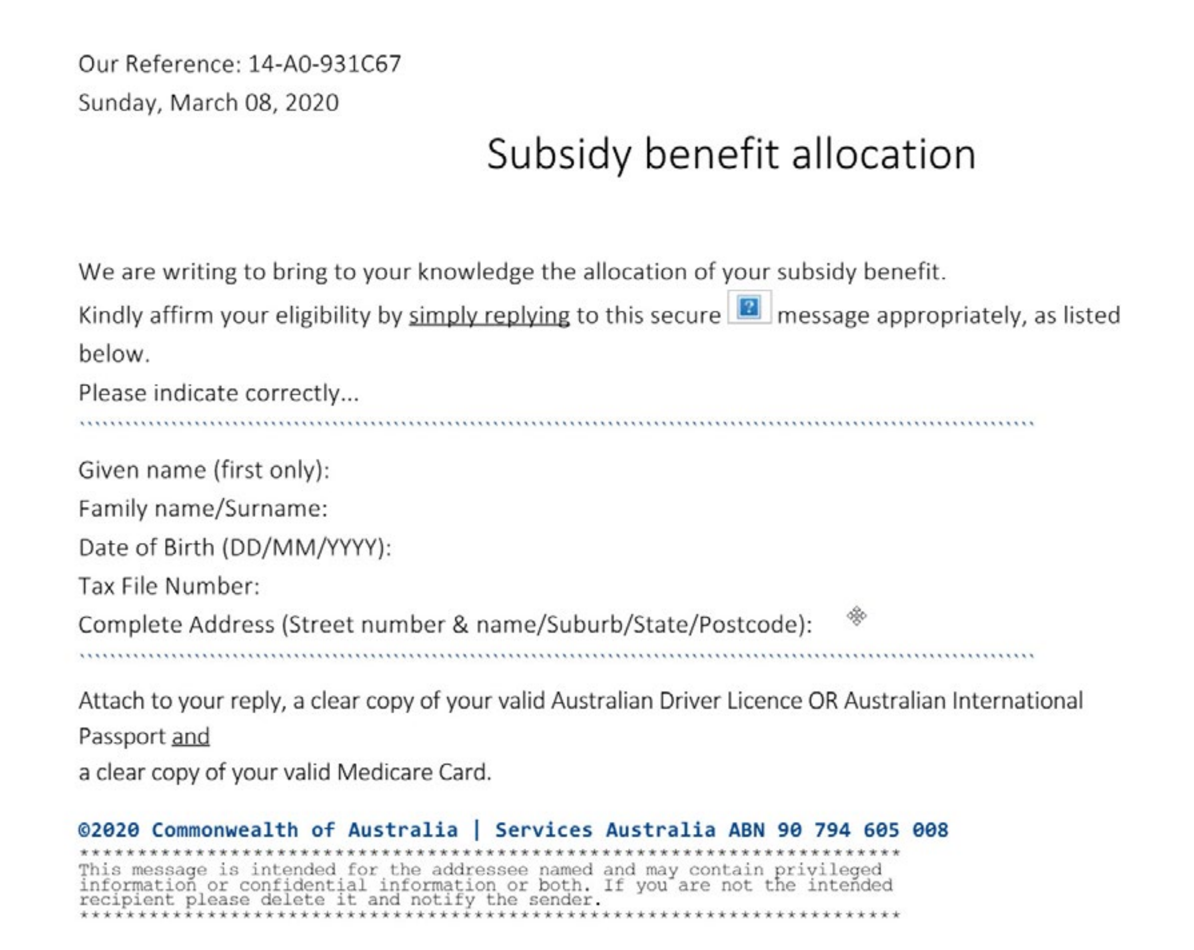
Scammers used multiple methods to seek people's superannuation details, or to make money from the scheme.

- In early March, Scamwatch received the first COVID-19 superannuation scam reports of cold callers offering unnecessary superannuation related services and charging a fee. Scammers claimed to be from the National Review Team, Advisory Committee, Superannuation Compliance, and National Superannuation Board.

[31] www.superannuation.asn.au/resources/superannuation-statistics.
[32] When you can access your super | Australian Taxation Office (ato.gov.au).

- In late March, Scamwatch received reports of other phishing scams such as fake grocery shopping vouchers designed to steal victims' superannuation details.
- Scammers also impersonated government agencies such as Services Australia with phishing emails designed to capture personal information and superannuation details (see examples below).
- In April, Scamwatch received reports about scammers withdrawing up to $10,000 from people's superannuation by accessing their myGov account or creating fake myGov accounts and linking to genuine accounts.

▶ Case study 3.2: Example of a government impersonation phishing scam



Our Reference: 14-A0-931C67

Sunday, March 08, 2020

Subsidy benefit allocation

We are writing to bring to your knowledge the allocation of your subsidy benefit.

Kindly affirm your eligibility by simply replying to this secure message appropriately, as listed below.

Please indicate correctly...

Given name (first only):

Family name/Surname:

Date of Birth (DD/MM/YYYY):

Tax File Number:

Complete Address (Street number & name/Suburb/State/Postcode):

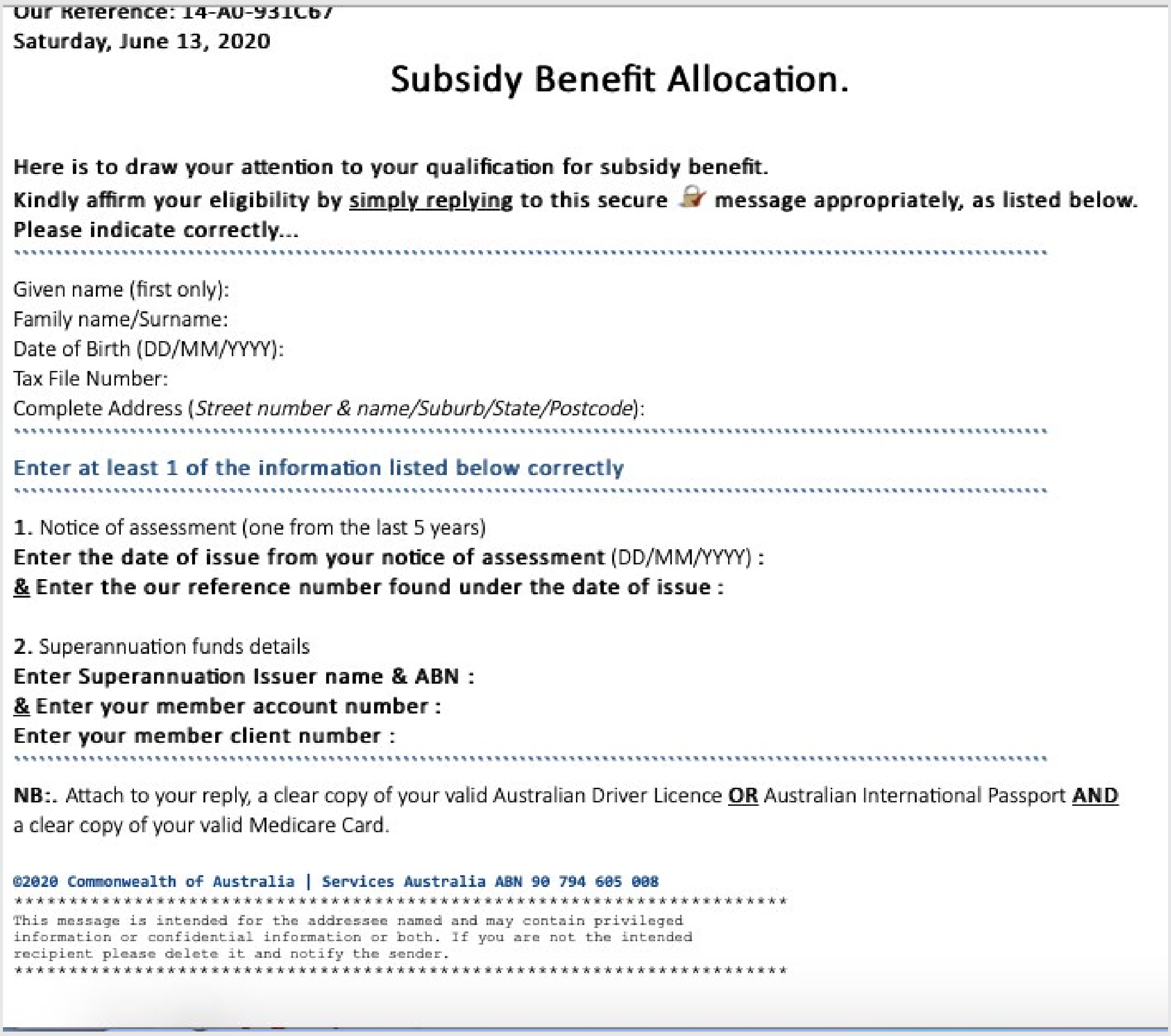
Attach to your reply, a clear copy of your valid Australian Driver Licence OR Australian International Passport and

a clear copy of your valid Medicare Card.

©2020 Commonwealth of Australia | Services Australia ABN 90 794 605 008

```
*****************************************************************************
This message is intended for the addressee named and may contain privileged
information or confidential information or both. If you are not the intended
recipient please delete it and notify the sender.
*****************************************************************************
```

Case study 3.3: Second example – with superannuation details requested



Our Reference: 14-AU-931C67
Saturday, June 13, 2020

Subsidy Benefit Allocation.

Here is to draw your attention to your qualification for subsidy benefit.
Kindly affirm your eligibility by simply replying to this secure 🔒 message appropriately, as listed below.
Please indicate correctly...

Given name (first only):
Family name/Surname:
Date of Birth (DD/MM/YYYY):
Tax File Number:
Complete Address (*Street number & name/Suburb/State/Postcode*):

Enter at least 1 of the information listed below correctly

1. Notice of assessment (one from the last 5 years)
Enter the date of issue from your notice of assessment (DD/MM/YYYY) **:**
& Enter the our reference number found under the date of issue :

2. Superannuation funds details
Enter Superannuation Issuer name & ABN :
& Enter your member account number :
Enter your member client number :

NB:. Attach to your reply, a clear copy of your valid Australian Driver Licence **OR** Australian International Passport **AND** a clear copy of your valid Medicare Card.

©2020 Commonwealth of Australia | Services Australia ABN 90 794 605 008

This message is intended for the addressee named and may contain privileged
information or confidential information or both. If you are not the intended
recipient please delete it and notify the sender.

The ACCC quickly identified high risks associated with this activity. The ACCC worked with government and law enforcement to share information, identify vulnerabilities and reduce the risks with the following initiatives:

- Driving collaborative meetings and discourse with a range of government agencies (including the ATO and the Australian Prudential Regulation Authority (APRA)) and super funds to identify technical vulnerabilities in the early release of super claims process.
- Issuing warnings to the community, initially via a media release launched on 6 April 2020, followed by a Thai translation of the release on 17 April.[33]
- On 8 April 2020, launching a COVID-19 Scamwatch webpage containing warnings around superannuation scams.
- On 28 May 2020, publishing a Superannuation early-access scams factsheet on the ACCC and Scamwatch websites, to inform consumers about these scams and guide potential victims on steps they can take to protect themselves from further damage.
- Circulating this publication to key stakeholders including: AUSTRAC (Fintel Alliance), ASIC, Australian Federal Police (AFP), Services Australia, APRA, ATO, a number of banks, the Consumer

[33] The Thai translation was commissioned in response to reports indicating scammers were targeting the Thai community in Australia in the early version of the cold call phishing scams.

Consultative Committee (CCC) and the Scams Awareness Network (SAN). The ACCC encouraged all stakeholders to share the factsheet with their wider networks.

- Where scammers targeted specific superannuation accounts, the ACCC passed sharable reports to APRA, ASIC, the Australian Criminal Intelligence Commission (ACIC) and the ATO.
- Proactively contacting and providing guidance to Scamwatch reporters who had received unexpected text messages informing them that their superannuation withdrawal had been successful.

Whilst initially losses to these scams were high, overall they were relatively low when considering the wealth in Australian super funds and what could potentially have been lost. This outcome may be a reflection of the ACCC's and other government agencies' collaborative efforts and proactive actions in response to the emergence of these scams.

▶ Case study 3.4: ATO – Early Release of Super scams

The ATO observed a range of scam campaigns aimed at taking advantage of public fear regarding COVID-19 and the urgency created by the variety of economic stimulus packages offered by the government, including Early Release of Super and JobKeeper.

The predominant Early Release of Super scam reported to the ATO was a pending Early Release of Super notification text message. The text message advised clients that their Early Release of Super request had been approved by the ATO and a payment was about to be made. However, if the client did not request this payment, they were directed to either call a number, reply to the text message or click a link to stop the payment.

Upon investigation by the ATO, these scams were either a text message crafted to appear to originate from either the ATO or myGov aimed at harvesting personal information or launching malware; a legitimate text message from a super fund to an old mobile number no longer used by the client and received by an unrelated party who thought it was a scam; or a small number of legitimate text messages issued by a super fund in response to a fraudulent attempt to access Early Release of Super but perceived by the client as a scam.

Phishing scams

Reports of phishing scams to Scamwatch increased by 75% in 2020 to 44,078 reports, compared with 25,170 in 2019. Phishing scams usually impersonate either a private sector or government entity.

Many phishing reports report an attempted scam that, if explored further, may have been a more specific type of scam better captured by another category, such as a suspicious call that would have led to a remote access scam. In 2020, more than 60% of phishing scam reports did not list a scammer name. These reports are usually a suspicion about a contact the reporter thinks is 'off' in some way. The reports are valuable and often contain phone numbers, email addresses or informative narratives.

The most commonly impersonated entities for phishing scams in 2020 were the same as those in 2019: Telstra, NBN Co, government organisations, the big 4 banks and package delivery companies.

Amazon

In 2020, we saw a large increase in the number of phishing scams involving impersonations of Amazon. Phishing reports mentioning the company rose 600% from 127 in 2019 to 897 in 2020. These reports were concentrated in the final quarter of 2020 and have continued into 2021.

This spike is a result of a new phone scam claiming that there is either a fraudulent purchase being made on a person's Amazon account, or that their free Amazon Prime trial is running out and they are about to begin subscription payments. In both cases, the recipient is told that it is too late to cancel the payment, but they can receive a refund (if they grant the caller access to their computer).

During the course of this remote access, the scammer impresses upon the victim the importance of entering the correct refund amount into an electronic form they show the victim. The scammer then alters the amount the victim writes into the form by adding additional numbers. For example, the victim may write $300.00. The scammer adds 2 additional 0s so that it reads $30,000.00.

The scammer then accuses the victim of having changed the value and appeals for sympathy by claiming they will lose their job and/or threatens the victim with legal repercussions unless the money is paid back. In Australia, the scammer then requests the victim sends the balance of the refund to a bank account or cryptocurrency exchange.

These scams are likely better categorised as remote access scams, but reporting numbers for phishing were buoyed by victims who realised Amazon was being impersonated prior to seeing the end result of the scam.

More financial institutions

We saw increased reporting of phishing impersonations of financial institutions outside of NAB, Commonwealth Bank, ANZ and Westpac.

Phishing reports about text messages impersonating Bendigo and Adelaide Bank increased from just 3 reports in 2019, to more than 172 reports in 2020. Reports of scammers impersonating the Bank of Queensland in 3 phishing text messages in 2019 compared with 414 in 2020. This trend was common across a number of other institutions.

Email phishing

Email phishing in 2020 most commonly impersonated PayPal, followed by Netflix. The PayPal scams varied, but the increase in reporting of scammers impersonating Netflix was largely attributable to emails claiming that the recipient's subscription payment details had either been declined, were about to expire, or had just expired and needed updating.

The most significant change in phishing scams was the Department of Home Affairs, mentioned 28 times in the phishing category in 2019, but 2,432 times in 2020. The scams responsible for this spike are discussed in the next section.

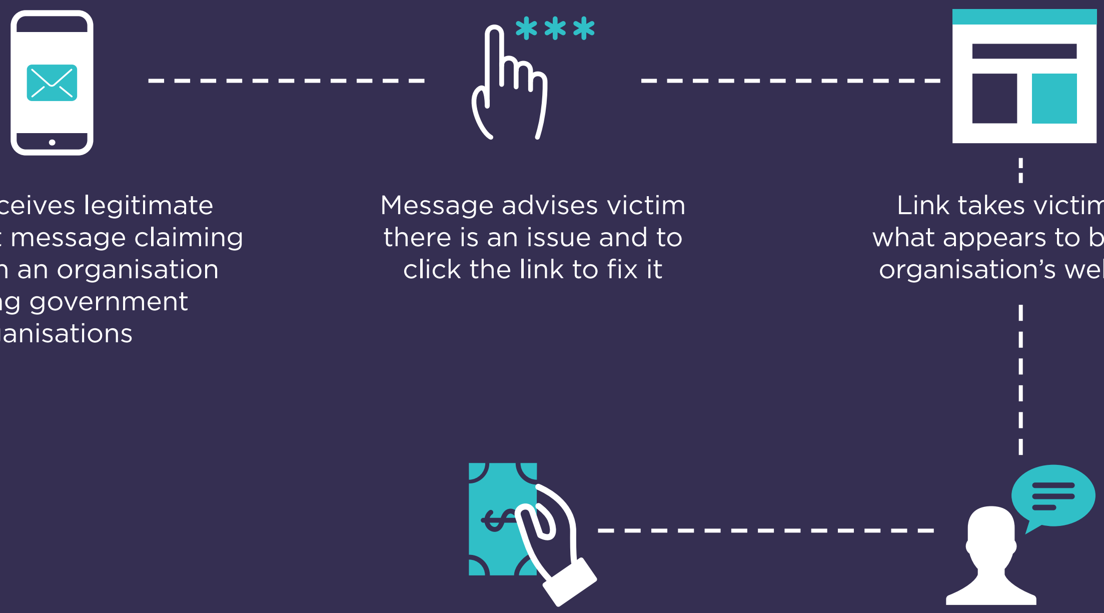
NBN Co takes action to combat phishing scams

For a number of years, NBN Co has been one of the entities most often impersonated in phishing scams. To coincide with Scams Awareness Week, in August 2020 NBN Co launched a community education campaign to raise awareness on the evolving nature of scams and to provide tips on how the community can stay safe. As part of this campaign, NBN Co held free information sessions across the country to talk directly to the public about scams.

The ACCC and NBN Co work closely as part of the watchlist project (see page 71 for more information) to investigate ongoing opportunities to collaborate in raising awareness and disrupting these scams.

PHISHING SCAMS

Scammers send you links to realistic looking websites to steal your personal information and then money



Victim receives legitimate looking text message claiming to be from an organisation including government organisations

Message advises victim there is an issue and to click the link to fix it

Link takes victim to what appears to be the organisation's website

Victim provides personal information e.g. banking information, date of birth, tax file number etc. to verify their identity

Scammers sell or use this information to impersonate the victim, usually attempting to obtain money in the victim's name

STATISTICS

Reports:

44,079

Reports to Scamwatch in 2020

A **75%** increase from the **25,168 reports** in 2019

PROTECT YOURSELF

Never click on any links or open attachments in emails claiming to be from your bank, the government or another trusted organisation asking you to update or verify your details

Puppy scams

In 2020, Scamwatch received 2,252 reports about puppy scams, with losses of over $2 million. These report numbers and losses were a substantial increase from the 498 puppy scam reports in 2019, with losses of $375,510.

The COVID-19 pandemic changed how people lived their lives. Shops, schools, gyms, restaurants and pubs all closed for a period of time. People were told to work from home where they could, and in some cases people were only allowed outside for exercise or grocery shopping. While at home many people took the opportunity to take on a pet for companionship or because it was now more convenient.

This increased demand for puppies led to increases in prices and more scam activity. Scammers set up fake websites, classifieds or social media ads pretending to sell sought-after dog breeds, taking advantage of the fact that buyers could not travel to meet the puppy in person. Scammers capitalised on the surge of interest in pets, and with state borders turning into hard borders, they were often able to scam people twice: once for payment for the puppy and the second time for transport costs for shipping the animal.

While many puppy scams do not specifically mention COVID-19 as a factor in the purchase or scam, the spike in reports in 2020 correlates to the beginning of the pandemic and social distancing/self-isolation measures.

Scammers also used excuses around COVID-19 social distancing measures, temporary business closures and quarantine periods to:

- request more money for coronavirus treatment or higher transportation costs for the puppy
- claim that puppies cannot be visited prior to sale due to social distancing restrictions
- legitimise delivery delays of the animal.

▶ Case study 3.5: Puppy scam

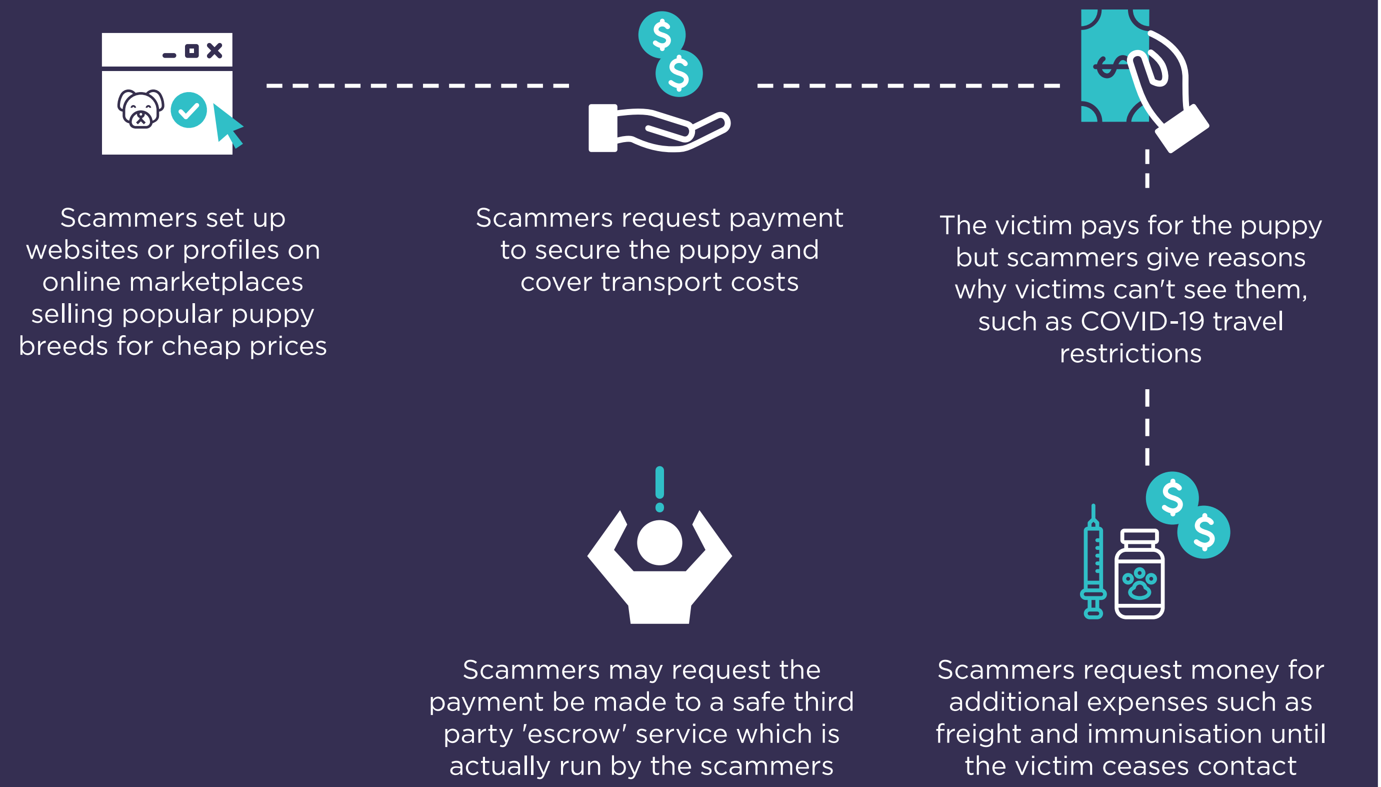
Sarah reported losing $10,350 to a puppy scam after attempting to buy a French Bulldog online. Sarah found the puppy on a fake website and paid $2,150 for the puppy and an additional $350 for shipping. The scammer said the puppy needed a temperature controlled crate for transport that would cost $7,500, but said this would be reimbursed once the puppy had arrived and the crate was returned to the sender. Two hours before the puppy was due to arrive at its new home, the scammer requested a further $2,500, claiming that the dog would not be able to transfer through the airport without COVID-19 insurance. At this point, Sarah realised she was being scammed. She tried to call the seller, only to realise they were not legitimate and her money was gone.

In response to puppy scams, the ACCC:

- published a media release in May 2020 warning about puppy scams
- worked with law enforcement and other government agencies to take down known puppy scam websites
- provided data (where consent was provided by reporters) to law enforcement to aid with investigations into puppy scammers
- highlighted common puppy scams on the Scamwatch Twitter page (twitter.com/Scamwatch_gov) including screenshots of fake websites used in puppy scams.

PUPPY SCAMS

Scammers ask for payments for non-existent puppies they've advertised online



Scammers set up websites or profiles on online marketplaces selling popular puppy breeds for cheap prices

Scammers request payment to secure the puppy and cover transport costs

The victim pays for the puppy but scammers give reasons why victims can't see them, such as COVID-19 travel restrictions

Scammers request money for additional expenses such as freight and immunisation until the victim ceases contact

Scammers may request the payment be made to a safe third party 'escrow' service which is actually run by the scammers

STATISTICS

Losses:
$2.2 million

Reports:
2,200+

Reports to Scamwatch in 2020

Reports quadrupled and losses were **6 times higher** than those reported in 2019

PROTECT YOURSELF

The safest option is to only buy or adopt a pet you can meet in person

If buying online, research the seller by running a search using the exact wording in the ad

Vehicle sale scams

In 2020, the ACCC received 1,067 reports about vehicle sales scams (cars, caravans and campervans) with reported losses of $1,035,401. This was a large increase both in terms of reports (220% increase) and losses (322% increase) compared to 2019. The average loss per report that included a loss was $6,637.

Scammers used websites including Facebook Marketplace (facebook.com/marketplace), Gumtree (gumtree.com.au), Car Sales (carsales.com.au) and Autotrader (autotrader.com.au), posing as either buyers or sellers.

When acting as a seller, the scammer will contact the buyer via email with an elaborate story, often about working for the military in a remote location, typically Tasmania, Western Australia or the Northern Territory. The scammer will provide fake documents to prove their identity and may use an email address that looks real (for example, @royalairforce-gov.com) but which is not, in fact, a real Australian Defence Force email address. The scammer will offer military transport to move the vehicle to where ever the buyer is located and suggest an escrow service for the protection of both the buyer and the seller. An escrow service is a third party that holds the money until both parties have fulfilled their obligations. However, in the case of vehicle scams there is no service and the money is just sent directly to the scammer.

To address these scams, the ACCC has developed relationships with reputable private sector platforms that are used by scammers to perpetrate scams. This can involve sharing reports where consent is provided, so the platform is aware that scams are taking place on their platform and can take steps to disrupt them, for example, by removing or blocking scammers.

The ACCC was part of government COVID-19 taskforces aimed at disrupting scams and shared (where appropriate) reports of vehicle scams. During 2020, some vehicle scams used the COVID-19 pandemic as an excuse as to why people could not view vehicles in person and these were shared with the relevant taskforces.

In November 2020, the ACCC published a media release about online shopping scams. Vehicle scams were the third most reported shopping scam and the second (after puppy scams) in terms of financial losses.

Identity theft

Identity theft was one of the top 3 most reported scams to Scamwatch in 2020, with reports of these scams increasing by 84%, from 11,373 reports in 2019 to 20,939 reports in 2020.

Despite the rise in reports, reported losses to these scams fell by 28.7%, from $4,311,066 in reported losses in 2019 to $3,072,287 in 2020. The full impact of an identity theft may not be known for some time, so losses in this category are always under reported.

Scammers used a range of scam techniques to steal people's identities including phishing, hacking, remote access scams, malware and ransomware scams and fake online profiles.

The ACCC has focused on disrupting identity theft as it can cause ongoing harm to its victims. Once a scammer has managed to assume an identity, it can be used to inflict further financial and personal information loss on victims.

To address these scams, the ACCC:

- continued our involvement with the ACMA Scam Technology Project. In 2020, both the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 and the Reducing Scam Calls Code were introduced. It is believed these Industry Standards have already had a signifcant impact in reducing harm caused by identity compromise
- focused 2020 Scams Awareness Week on how to avoid a scammer stealing your identity (further details provided below)

- worked with the Department of Home Affairs and state and territory driver licence authorities on a solution to improve outcomes for consumers when their driving licence information is stolen (further details provided below).

3.2 COVID-19 cooperation

The whole-of-government response to COVID-19 resulted in increased collaboration and information sharing between departments and agencies. Similarly, cooperation between government and the private sector led to the amplification of warnings to the community and increased disruption of scams.

In response to the emergence of scams related to COVID-19, the ACCC undertook increased monitoring of scam reports to support awareness raising and disruption activities. Since the pandemic began, we have reviewed COVID-19 scam reports daily to identify high risk scams and take action where appropriate and have maintained a public facing webpage on COVID-19 scams based on this information. As a result of this focus, the ACCC has been able to take swift action to confirm whether something is a scam, inform other relevant agencies or private sector organisations, provide useful intelligence to law enforcement and raise public awareness.

ACCC works with ACSC to identify and remove malicious websites

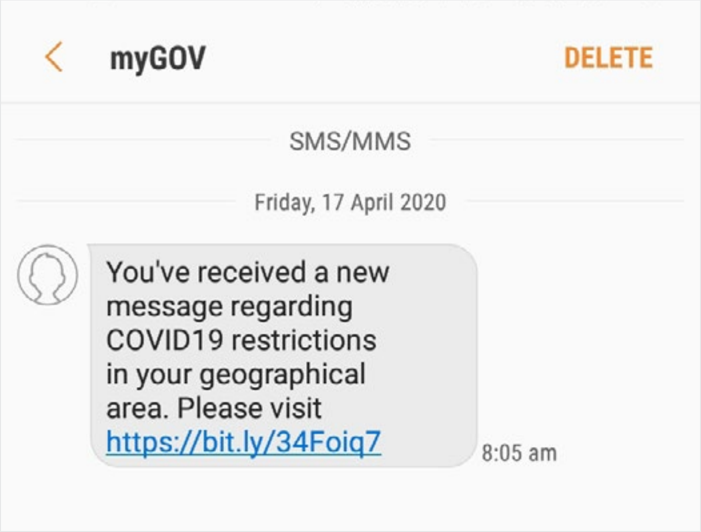
Scamwatch and a wide range of government agencies worked together to share intelligence, prevent and disrupt scams. For example, inter-agency cooperation protected consumers from government impersonation scams. Scamwatch started to receive a large number of reports of COVID-19 government impersonation related scams, involving text messages containing malicious links to fake websites. The ACCC worked with the Australian Cyber Security Centre (ACSC) and the agencies being impersonated to send out warnings to consumers and facilitate the take-down of the fake websites.

The first COVID-19 government impersonation text message scam was received and reported to Scamwatch on 16 March 2020. We published a warning in relation to the message and spoke with the ACSC to have the website it linked to removed as quickly as possible.

Case study 3.6: ACCC acts on first government impersonations during the pandemic

The text message pictured below was sent to an undetermined number of Australians on 16 March 2020. Scamwatch received 11 reports of this specific text but this certainly does not reflect the true scale of how many people were targeted. The timing was concurrent with announcements in relation to economic relief, border restriction information and other public announcements of key state and territory initiatives.[34]

If the website https://covid19-info.online was visited from an iPhone or computer, the website redirected the user to the Department of Health's official coronavirus information page. If the website was visited from an Android phone, the website instead presented a screen prompting the user to update their Adobe Flash Player. Clicking the download button to do so, downloaded a file (UpdatedFlashPlayer_11_5_1.apk) that was in fact a virus to the user's phone.



You've received a new message regarding COVID19 restrictions in your geographical area. Please visit https://bit.ly/34Foiq7

8:05 am

Due to the ACCC's increased monitoring, we were able to quickly notify the ACSC and issue a warning about clicking on the link in this message. The ACCC and ACSC worked together throughout 2020 on several waves of similar malicious text messages and linked websites.

In 2019–2020 the ACCC disrupted 31 websites, including puppy scam websites, celebrity endorsement investment scams and fake charity pages. The combined efforts of the ACCC, ACIC, AFP and Services Australia enabled the ACSC to disrupt over 150 malicious themed websites.

Services Australia joins other agencies to combat text scams

From April 2020, Services Australia saw a significant increase in both scam reports and website traffic as the COVID-19 pandemic emerged. In 2020, the agency's Scams and Identity Theft Helpdesk received 11,553 reports of scam and identity theft incidents, with 1,028 victims reporting a financial loss, a significant increase from the 4,790 reports received in 2019.

There was a significant increase in traffic to the scams awareness material on Service Australia's website. The information most sought related to 'how to identify a scam' and 'examples of scams'. The agency developed a Scams Alert webpage to facilitate almost real time updates on emerging and prevalent scams.

Services Australia made significant progress in blocking text message scams in 2020. The agency worked with Telstra and other key stakeholders, such as the ACMA and the ACSC, on the Cleaner Pipes initiative. This initiative prevents scammers sending scam text messages that impersonate the agency or myGov for mutual Telstra and agency customers.

[34] www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp2021/Chronologies/COVID-19StateTerritoryGovernmentAnnouncements.

Although the Cleaner Pipes initiative has blocked most malicious Telstra SMS accounts impersonating the agency's sender ID, Services Australia continues to see myGov phishing scams via text and email. These typically direct individuals to a fake myGov site built to capture credentials, financial information and personal identity information.

During 2020, Services Australia also referred 148 impersonation scams for investigation, monitoring or as part of a disruption effort. These included scams via phone, text, email and platforms such as Facebook including:

- 119 scams related to myGov
- 17 scams that impersonated Services Australia programs, platforms or services that attempted to leverage an emergency relating to the COVID-19 pandemic or bushfire relief.

The cooperation shown between government agencies throughout the pandemic serves as a case study in how working together can help prevent scams and these partnerships will allow for better outcomes in the future.

ACCC works with other agencies to raise awareness about online safety

During the pandemic, the ACCC met fortnightly to discuss communication strategies with other agencies and develop a shared understanding of the scams and online safety issues facing Australians.

The ACCC worked with the Office of the Australian Information Commissioner (OAIC), the eSafety Commission and the ACSC to produce a short guide about online safety and security and where to report. Be safe Be alert online was published in September 2020. Communication strategies and education are important ways communities can build resistance to scams. Government and the private sector continue to work together on a daily basis to warn the public about scam activity.

Without this cooperation, the losses reported to scams in Australia may have been significantly higher during 2020.

Collaboration to combat anticipated COVID-19 vaccination scams

With the announcement of the COVID-19 vaccination rollout in late 2020, government agencies anticipated an influx of reports of vaccine related scams and other fraud. The ACCC and a number of other agencies shared the Department of Health's warnings and advice about vaccine scams on their websites and social media platforms to ensure this messaging reached as many consumers as possible. As of 30 April 2021, the number of reports of vaccine scams has been low, which may be a reflection of these ongoing collaborative efforts.

ACCC works with Department of Home Affairs to reduce impacts of identity compromise

Impacts of identity theft can continue to occur for many years and are not limited to financial loss. Identity theft may also results in mental health challenges including trauma, grief, emotional and physiological distress.

Driver licences are commonly used for identity verification and a stolen licence (whether virtual, physical or just the driver licence information) presents a high risk of exploitation by criminals, who use licence details to steal a person's identity. Driver licences have been described as the 'golden ticket' to commit fraud by IDCARE, Australia's national identity theft victims support service. It is the most commonly used identity document in fraud.

In 2020, the ACCC continued to advocate for enhanced security measures around identity verification and driver licences. The aim of this work, undertaken via engagement with the Department of Home Affairs and state and territory authorities, is to minimise the impact of identity theft in Australia. We note that it also follows the guiding principles of the National Identity Security Strategy.

Scams Awareness Network focuses on identity crime in COVID-19

The ACCC leads the Scams Awareness Network (SAN), which 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.[35] The ACCC's Deputy Chair, Delia Rickard, is Chair of the SAN, and we also provide secretariat services. Each month, members share scams intelligence, research and upcoming awareness campaigns.

Every year, the SAN organises and delivers Scams Awareness Week. The week promotes awareness around a particular theme to help Australians recognise and avoid scams. The 2020 Scams Awareness Week ran from 17 to 21 August and focused on identity theft under the tagline, 'Be yourself. Don't let a scammer be you'. This topic was chosen as the ACCC observed a significant increase in scams targeting personal information at the start of the COVID-19 pandemic.

The aim of the campaign was to educate consumers about how to spot and avoid identity theft scams, such as the theft of banking or superannuation details or passwords, which can be used for scammers' financial gain.

The main communication tool for the campaign was a series of 5 podcasts entitled 'This is Not Your Life' produced by Julian Morrow, the creator of ABC TV's consumer education series The Checkout. The series provided advice on how to avoid a scammer from stealing your identity and featured cameos from ACCC Chair Rod Sims, eSafety Commissioner Julie Inman Grant and IDCARE's founder Professor David Lacey. During the campaign week, the podcasts were downloaded almost 10,000 times.

In addition to the podcasts, the ACCC developed a campaign landing page containing updated information about scams and identity theft and links to campaign resources. The page was viewed 235,000 times during the campaign week. We also developed a campaign toolkit that was distributed to the SAN and partners to help them support and promote the campaign.

Despite media focus on the COVID-19 pandemic throughout 2020, Scams Awareness Week gained strong media traction. The campaign generated 920 media items in 2020 (up 162% from the 2019 campaign), with a potential audience reach of 17.1 million. Deputy Chair Delia Rickard also participated in over 20 official media engagements across the week.

[35] A list of current SAN members is available at: www.scamwatch.gov.au/about-scamwatch/scams-awareness-network.

4. Other notable scam trends

4.1 Investment scams

Investment scams continue to be a significant problem in Australia as evidenced by the combined losses of $328 million reported in 2020. Investment scammers are increasingly taking advantage of the many ways to advertise or contact victims including via social media.

▶ Case study 4.1: Investment scams on Instagram

John became friends with Dexter on Instagram, who after a while started discussing Bitcoin. Dexter said he could show John how to trade. John purchased Bitcoins and then commenced trading on ABCcoinsTrade. Like many, he started small and then invested more. Every time he approached withdrawal, John was advised to make further payments until he realised he had been scammed and that Dexter was most likely running the trading site.

John was able to identify that Dexter had set up multiple accounts under different names on different platforms for the purpose of luring people into investment scams.

John then met Harris on Instagram and told him what happened. Harris then suggested a second Bitcoin site he said could help to get the money back. John agreed only to be faced with the same issue – it was the same scammer operating out of a garage.

Investment scams are difficult to investigate and prosecute, with many scammers based overseas. However, there has been some success in recent times through the combined efforts of the Victoria Police E-Crime Squad and ASIC. In October 2020, ASIC published a media release reporting that a Melbourne based man was arrested in relation to a number of investment scams.[36] This scammer was connected to more than 40 false business names registered between May 2019 and October 2020. He obtained a large number of international passports and opened bank accounts in Australia. He used a number of websites and advertisements and obtained at least $370,000 from victims. ASIC's investigation prevented any further investments in the scheme.

ACCC information for victims of investment scams

The ACCC encourages the public to report scams via the Scamwatch website, either when they have fallen victim to a scam or where they have seen something they believe is a scam.

Currently, when people report a scam to Scamwatch they receive an automated acknowledgement reply message containing standard information that is not tailored to the scam they are reporting.

In 2020, the ACCC commenced a pilot project to provide more tailored responses to people reporting an investment scam and victims of investment scams. We undertook a benchmarking study that showed that 62% of people who reported an investment scam to Scamwatch would have liked more information at the time they lodged their report, including the immediate steps they could take to protect themselves. The study also highlighted that the most common reasons people reported to Scamwatch are:

- to tell someone so other people can avoid the scam (90% of reporters)
- to find out if anyone could stop or punish the scammer (85% of reporters)
- to find support and information about where to get help (60%).

We then developed resources for victims and reporters of investment scams that were more tailored to their needs. These included information to direct them to report to their bank and to services such as

[36] asic.gov.au/about-asic/news-centre/find-a-media-release/2020-releases/20-244mr-man-arrested-following-suspected-financial-investment-scam/.

IDCARE; to provide information about how to avoid investment scams in the future; and to encourage them to share their experience with others.

In early 2021, the ACCC sent this dedicated investment scam information to investment scams reporters and victims and is now measuring its impact to determine if it assisted people to protect themselves; warn others; or helped them to reach the support and services they needed.

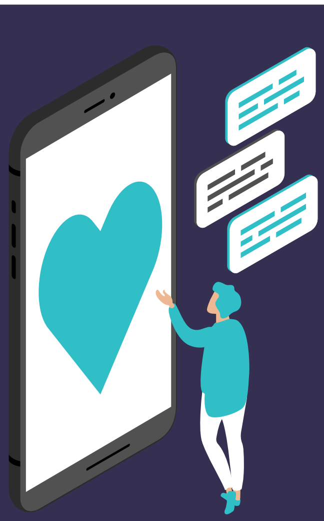
4.2 Romance baiting

In 2020, Scamwatch identified and monitored a new scam it named 'romance baiting' that led to over $15 million in financial loss (across 414 reports). In this scam, contact is made in the form of a romance interest, often on a dating app and after some initial grooming (baiting) the target is lured into an investment scam.

Younger people aged 25 to 34 years lost the most money to this scam, with over $7 million in losses reported in 2020. The most common contact method was via apps such as Tinder, TanTan, Badoo and Coffee meets Bagel. Other features of the scam include the following:

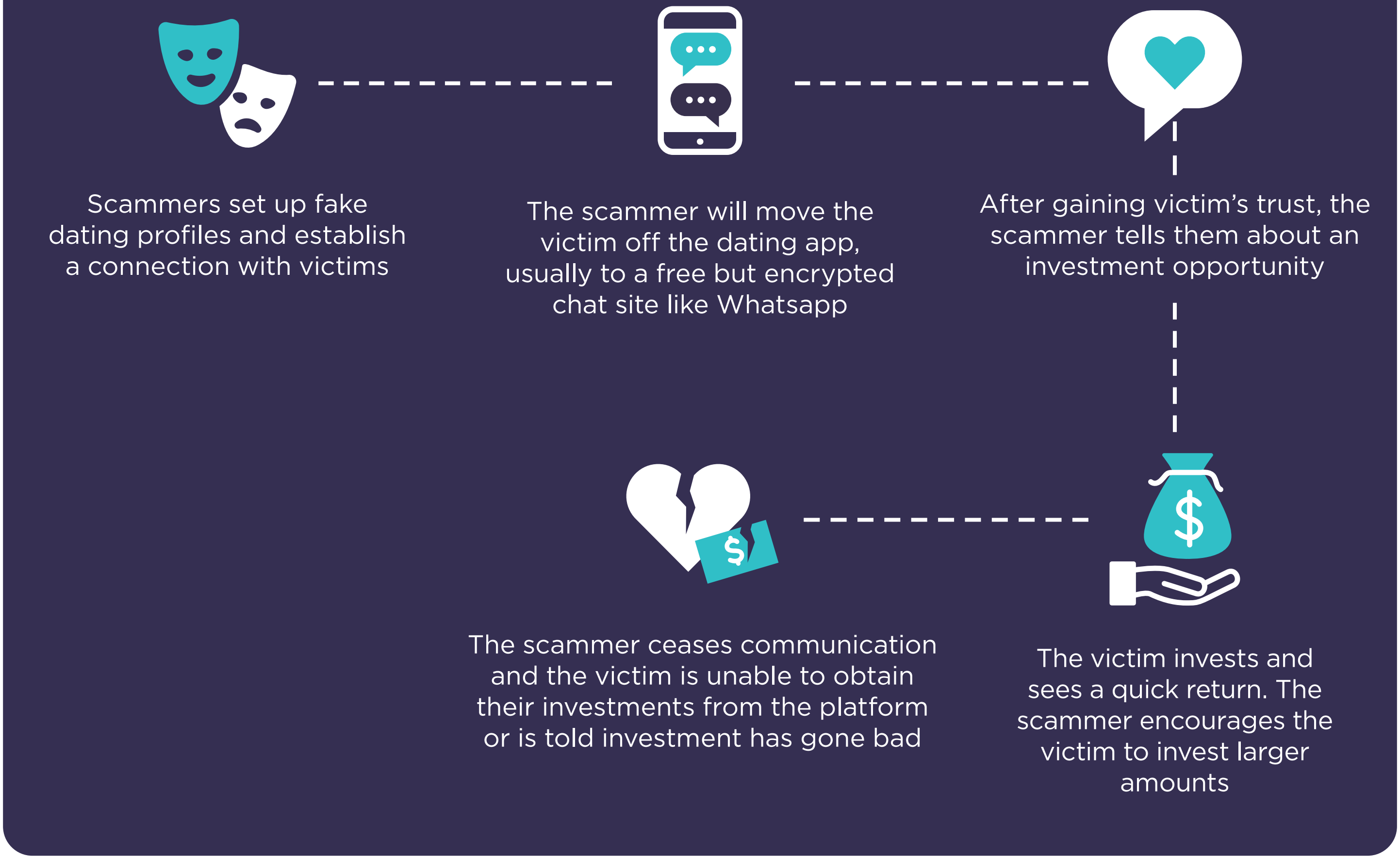
- After only a couple of messages, the scammer asks the victim to head to a free but encrypted chat site, such as Google Hangouts, WeChat, Line or commonly WhatsApp.
- A couple of weeks is spent developing the relationship so the victim has feelings for the scammer – this is sometimes referred to as love bombing and is a common tactic used with romance scams.
- After a little while, the scammer begins asking about the victim's finances.
- The scammer begins to mention that they are making money through different investments, most commonly cryptocurrencies, but sometimes through online gambling or investing in stocks or gold.
- The scammer offers to show the victim how to invest. Then the scammer pressures the person to transfer a small amount of money to see how easy it is.
- The scam ends when the victim has no more money to give. Often, they are told they have to top up their accounts to access their money or keep their accounts at a certain level or their account will be frozen and their money lost for good.

The ACCC is working with ASIC to share intelligence (where consent is provided to share reports) about romance baiting scams. Scamwatch continues to warn the public about these scams.



ROMANCE BAITING SCAMS

Scammers meet victims on dating apps and lure them into investment scams, often involving cryptocurrencies



Scammers set up fake dating profiles and establish a connection with victims

The scammer will move the victim off the dating app, usually to a free but encrypted chat site like Whatsapp

After gaining victim's trust, the scammer tells them about an investment opportunity

The victim invests and sees a quick return. The scammer encourages the victim to invest larger amounts

The scammer ceases communication and the victim is unable to obtain their investments from the platform or is told investment has gone bad

STATISTICS

Losses: **$15.5 million**

Reports: **400+**

Scammers used dating apps such as Tinder

Reports to Scamwatch in 2020

PROTECT YOURSELF

Don't take financial advice from someone you met through online dating

If you start to feel pressured by someone, stop communicating with them

4.3 Celebrity endorsement scams

In 2020, celebrity endorsement scams resulted in losses of almost $2 million, an increase of $800,000 from 2019.

A celebrity endorsement scam involves a scammer using the image, name and personal characteristics of a well-known person without their permission to sell a product. The product may be health related, or an investment strategy.

Celebrity endorsement scams are not new; however, the celebrities used by scammers are always changing. In 2020, scammers began using fake news articles about celebrities impersonating well-known media sites, such as ABC News, The Project, and News.com.au as a way to lure people into scams.

There are 2 main types of celebrity endorsement scams, firstly, scams that purport to sell a product using a celebrity's image, and secondly, scams that offer investments, usually in cryptocurrency schemes.

Celebrity endorsement investment scams

People might see an ad pop up on social media or even YouTube that piques their interest in investing. As with other investment scams, victims are offered an opportunity to make high returns quickly. They trade in cryptocurrencies and often communicate with the scammers on modern platforms such as Discord and Telegram. But suddenly, victims find that the trading platform is closed, the scammers cannot be contacted and that their money has disappeared. 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 them from notifying others that the company is illegitimate.

▶ Case study 4.2: ASIC warns of fake Bitcoin endorsements

In July 2020, ASIC warned the public about celebrities such as Kochie, Celeste Barber and Waleed Aly being used in celebrity endorsement scams involving cryptocurrency trading schemes. Fake celebrity endorsements were used on fake websites posing as crypto trading robots. These bots automatically traded crypto coins (i.e. Bitcoin, Ethereum etc.) on the user's behalf, often accessing their bank account. The websites were advertised on popular social media platforms.

The ACCC expects digital platforms to monitor and remove celebrity endorsement scams. Where consent is provided, Scamwatch reports are shared with social media platforms. In addition, the ACCC shares investment scam reports with ASIC and continues to raise awareness about these scams on Scamwatch, Twitter and via the media.

▶ Case study 4.3: UK National Cyber Security Centre removes 300,000 malicious links in celebrity endorsement investment scams[37]

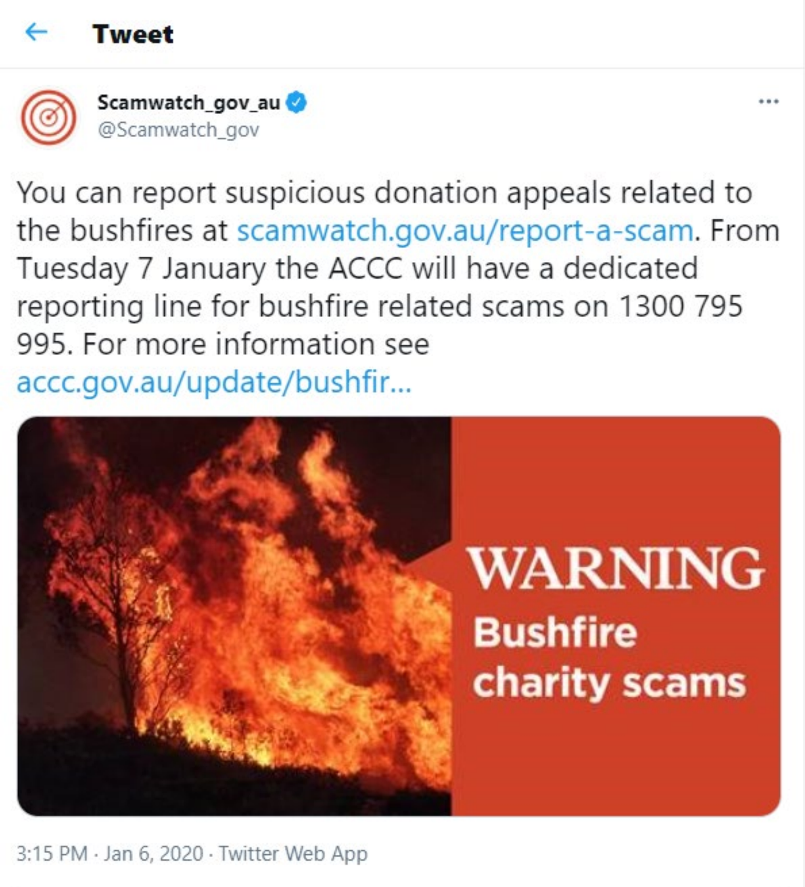
In August 2020, the UK NCSC identified links in celebrity endorsement scams promoted in fake news articles that were distributed by phishing emails and in digital advertising to trick people to give money or information to scammers. The NCSC warned the public to be wary of celebrity endorsements and fake investments on online platforms. It removed 300,000 of the malicious links advertising fake get-rich-quick schemes.

[37] www.zdnet.com/article/300000-links-taken-down-in-crackdown-on-investment-scams-with-bogus-celebrity-endorsements/.

4.4 Bushfire scams

During a crisis such as bushfires, scammers will often set up fake donation pages, fake charities or impersonate real charities.

On 6 January 2020, in response to the Australian bushfire crisis and reports of scam activity, the Australian Government asked the ACCC to create a dedicated Scamwatch hotline for people to report bushfire related scams. The ACCC opened the hotline on 7 January and received more than 1,000 calls until its closure on 27 March 2020. Scamwatch also received over 330 bushfire related Scamwatch reports through the website. The ACCC monitored bushfire scams daily and engaged with the Australian Charities and Not-for-profits Commission regularly. We published a media release on bushfire scams and sent warnings to the public via the Scamwatch website and Twitter account.[38]



Tweet

Scamwatch_gov_au
@Scamwatch_gov

You can report suspicious donation appeals related to the bushfires at scamwatch.gov.au/report-a-scam. From Tuesday 7 January the ACCC will have a dedicated reporting line for bushfire related scams on 1300 795 995. For more information see accc.gov.au/update/bushfir...

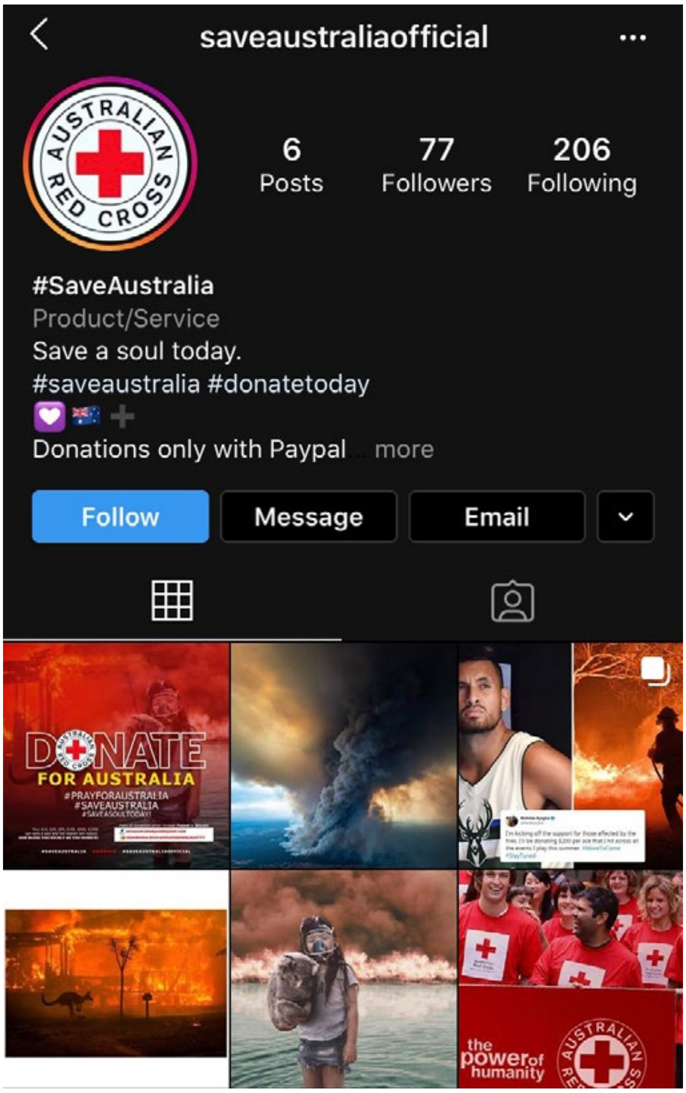
3:15 PM · Jan 6, 2020 · Twitter Web App

Most bushfire scam related web reports concerned fake charity scams with 3 main variants. Some reporters expressed doubt that stores were going to donate their stated proportion of profits from sales to charities. Others reported that scammers were soliciting donations for fictional charities. Some reported scammers impersonating real charities or even real bushfire victims.

The ACCC was able to shut down several fake bushfire charity and fundraising webpages on crowd-funding platforms and social media. In 2 instances, the ACCC was able to pass payment and suspect details to the Australian Federal Police and the Fintel Alliance.

[38] twitter.com/scamwatch_gov/status/1214052923480494082.

Bushfire scam with payment details example:



saveaustraliaofficial

6 Posts

77 Followers

206 Following

#SaveAustralia

Product/Service

Save a soul today.

#saveaustralia #donatetoday

💟 🇦🇺 ➕

Donations only with Paypal ... more

5. The people

5.1 Demographics

A range of people report scams to Scamwatch. Reporters differ in gender, age, location and ethnicity. This section of the report explores who reported scams to Scamwatch in 2020.

Not everybody who reports a scam provides their age, gender, location or ethnicity, but those that do provide us with valuable insight into how scams impact different demographics. This information is important as it allows the ACCC and other government agencies to target scam messaging and awareness raising activities to where they may be of the most benefit.

Gender[39]

In previous Targeting Scams reports there have been some distinct differences in the financial losses reported by men and women. Men have lost more than women in the last 5 scam reports.[40]

In 2020 the gap reduced, with men losing $87,980,854 and women losing $87,384,828. While men reported higher losses, women lost money more frequently, with 11,571 reports where a financial loss was incurred as outlined in table 5.1.

Table 5.1: Gender and scam reports and losses

Gender	Number of reports	Reports with loss	Losses
Female	108,995	11,571	$87,384,828
Male	103,057	11,132	$87,980,854
Non-specified	4,035	179	$318,409
Total	**216,087**	**22,882**	**$175,684,091**

While overall loss amounts were similar for men and women, the scams in which they lost the most money varied considerably as indicated in table 5.2.

Table 5.2: Scam types reported by men and women by highest loss

Scam type	Women		Men	
	Reports	Losses	Reports	Losses
Investment scams	2,377	$21,096,956	4,744	$44,653,829
Dating and romance scams	1,958	$28,097,935	1,689	$10,748,671
False billing	6,532	$12,768,252	6,346	$5,649,954
Threats to life, arrest or other	16,472	$8,148,537	15,236	$3,679,178
Remote access	4,194	$4,198,470	4,164	$4,233,794

Men reported losing twice as much as women to investment scams ($44.7 million compared with $21.1 million) in 2020. However, women lost almost 3 times the amount compared to men in romance scams ($28.1 million compared with $10.7 million).

[39] When reporting to Scamwatch, people are asked to report how they identify in terms of gender. The report form has 3 categories: 'male', 'female' or 'non-specified' for people who do not identify as either gender or would prefer not to say. The ACCC acknowledges that not all people identify as male or female; however, at this stage the majority of reporters (98% of all reports) identify as either male or female and are therefore discussed in those terms.

[40] In the last 5 Targeting Scams reports, men have lost between $8 million and $20 million more than women to scams.

Age

In 2020, people aged 25 to 34 made the most reports to Scamwatch, followed by those aged 35 to 44. However, neither of those age groups had the highest losses. People aged 65 and over had the highest losses and reported losing almost $38 million.

Older Australians are tending to lose more money per report where a financial loss is experienced. The average loss to a scam by someone aged 65 years or older was $16,139.

Table 5.3: Number of Scamwatch reports by age group – 2020 compared with 2019

	2020			2019	
Age group	**Reports**	**Reports with loss (% of total reports in age group)**	**Losses**	**Reports**	**Losses**
Under 18	1,810	429 (23.7%)	$496,156	1,645	$471,595
18–24	13,781	3,038 (22.0%)	$10,971,511	10,357	$4,677,469
25–34	33,122	4,619 (13.9%)	$24,225,924	21,823	$19,032,736
35–44	32,727	4,292 (13.1%)	$25,496,094	20,294	$26,032,736
45–54	28,908	3,292 (11.4%)	$32,658,050	19,810	$26,868,460
55–64	25,836	2,471 (9.6%)	$26,456,830	19,655	$29,866,466
65 and over	30,053	2,337 (7.8%)	$37,700,841	25,149	$23,613,316
Age not provided	49,850	2,407 (4.8%)	$17,678,685	49,064	$12,313,448
Total	**216,087**	**22,885**	**$175,684,091**	**167,797**	**$142,905,575**

People aged 35 to 44 years and 55 to 64 years lost less money in 2020 than they did in 2019. Both of these age groups had a higher number of reports than the previous years, but lower losses.

Scam losses experienced by different age groups

Anyone can be vulnerable to a scam at various life stages and circumstances. This section examines the scam types causing the most financial loss for the different age groups.

Under 18 year olds

Table 5.4: Top 5 scams by reported losses for people under 18 years

Scam category	Reports	Reports with loss	Losses
Jobs and employment scams	23	4	$138,020[41]
Online shopping scams	333	218	$115,863
Threats to life, arrest or other	194	9	$113,652
Classified scams	112	61	$69,014
Investment scams	46	18	$22,209

Of the 333 reports about online shopping scams made by people under 18 years, 218 involved a reported financial loss. This means the average loss experienced by young people to shopping scams was around $530. This is a relatively high amount for what are ostensibly school aged people with limited earnings potential.

Threat based scams also impacted young people, with $100,322 lost to Chinese authority scams.

[41] This figure was impacted by one loss scam of $136,000.

▶ Under 18 and you've seen something you like on social media?

Jenna was looking at her social media sites and saw some clothes one of her favourite influencers had promoted for sale. The price looked reasonable – not too cheap and not too expensive, so Jenna thought she would buy a couple of tops. She made the order, and paid for the tops through a pop-up shop on her socials. After several weeks when no delivery had arrived, Jenna checked the influencer's site. She found the influencer had not really promoted the pop-up shop, and that someone had used her photos to scam people. Jenna lost her money, but also lost her personal information such as address, full name and contact details.

18 to 24 year olds

Table 5.5: Top 5 scams by reported losses for people aged 18 to 24 years

Scam category	Reports	Reports with loss	Losses
Threats to life, arrest or other	2,315	180	$5,830,303
Online shopping scams	1,873	1,161	$1,127,790
Dating and romance scams	271	119	$1,019,455
Investment scams	471	253	$877,554
Classified scams	766	386	$689,065

For people aged 18 to 24 years, the scam category with the highest number of reports, and the largest losses, was threats to life, arrest or other, with over 2,000 reports and losses of more than $5.8 million.

A large proportion of the top 10 highest reported losses involving those scams were Chinese authority scams. In fact, of the top 10 losses, 9 were Chinese authority scams and accounted for almost $2.9 million. There were 59 Chinese authority scams in total reported in that category.

As this data illustrates, threat based scams tend to disproportionately affect younger people and those who speak Mandarin as their first language, including foreign students. In 2020, we sent material out to universities to warn international students about this type of scam, including detailed warnings about 2 specific scams affecting the Chinese community in Australia involving extortion and threats of arrest. This content was also translated into simplified Chinese and traditional Chinese.

▶ Case study 5.1: Threat based scams – Chinese authority scams

Jian received a phone call from someone claiming to be from the Chinese Embassy in Canberra. The Embassy official told him that his Chinese identity cards were used at a hospital in China where there had been a COVID-19 case detected on the same day. The Embassy official told Jian he had to isolate for 14 days. Jian told the caller that he had not been to China since before the pandemic broke out. The Embassy official said it sounded like someone was using Jian's identity and they would transfer Jian to the police in Beijing.

The Beijing police told Jian that his identity had been misused and his Chinese bank account was suspected of being involved with money laundering. They asked Jian to communicate via WhatsApp as it was more secure. Over several days the police kept contacting Jian, accusing him of different crimes. Jian gave them copies of his passport, bank account details and his employment details in Australia to prove he had a job and had not left the country.

The police said they believed Jian, but needed him to transfer money to them so they could trace his assets or they would have no choice but to arrest him.

Jian was very worried at this stage. He transferred $15,000 but finally told a friend what was happening. Jian's friend said he thought it was a scam.

25 to 34 year olds

Table 5.6: Top 5 scams by reported losses for people aged 25 to 34 years

Scam category	Reports	Reports with loss	Losses
Dating & romance scams	592	255	$7,403,012
Investment scams	1,313	526	$7,348,096
False billing scams	1,681	289	$1,979,252
Threats to life, arrest or other	6,174	146	$1,708,595
Online shopping scams	2,925	1,751	$1,546,762

Dating and romance scams are low volume/high value scams. Scamwatch receives several thousand reports a year about this scam type and the reports typically include high losses. Typically, it is older age groups that report significant losses to these scams. However, in 2020, 43% (255 reports) of 25–34 year olds who reported a romance scam incurred a financial loss. 87 involved romance baiting scams where a scammer made contact with a person on a dating app and lured them into investing money.

Investment scams also involved high losses for people aged 25 to 34 years, with $7.3 million. Of the 1,313 reported investment scams, 526 involved a financial loss (40.1%), and of those 308 were a cryptocurrency payment or investment.

▶ Case study 5.2: Romance baiting scam

Ling met Zac on a dating app. He was attentive, handsome and he ran his own business. During COVID-19, Zac was stuck overseas and was unable to get back to Australia. He told Ling that his business was suffering but that he had started investing and couldn't believe how easy it was. He showed Ling his investments, and she was impressed at the earnings.

Zac began to encourage Ling to invest in a new cryptocurrency that he said was guaranteed to be bigger than Bitcoin. He told Ling they could put the money towards their future. Ling transferred Zac $5,000 to set up an online account to purchase cryptocurrencies. Zac encouraged Ling to invest more and more money. Before long, when Ling realised she had transferred over $25,000, she decided she wanted some of her money back. She then discovered her account was frozen and to unlock it, she would need to pay an extra $5,000.

Ling didn't have the money. She contacted Zac but he blocked her on the app. Ling realised that Zac was a scammer and the investments were fake.

35 to 44 year olds

Table 5.7: Top 5 scams by reported losses for people aged 35 to 44 years

Scam category	Reports	Reports with loss	Losses
Investment scams	1,370	516	$11,748,694
Dating & romance scams	639	233	$5,240,241
False billing scams	1,593	297	$1,527,845
Online shopping scams	2,752	1,753	$1,527,845
Classified scams	1,369	496	$1,158,942

People aged 35 to 44 years lost the most money to investment scams, over $11 million. The average loss experienced to investment scams was almost $23,000. Over half of all online shopping scams (63%) reported by people aged 35 to 44 years involved a financial loss.

45 to 54 year olds

Table 5.8: Top 5 scams by reported losses for people aged 45 to 54 years

Scam category	Reports	Reports with loss	Losses
False billing scams	1,612	268	$10,786,748
Dating & romance scams	702	250	$8,687,479
Investment scams	1,024	361	$7,928,132
Online shopping scams	2,073	1,215	$1,076,985
Classified scams	1,321	413	$918,885

For people aged 45 to 54 years, false billing scams caused the highest losses. This category includes business email compromise scams (payment redirection) and fake invoices. For individuals, the most common losses were incurred transferring a large sum of money for things such as renovations, or conveyancing fees when buying or building property.

▶ Case study 5.3: A false billing scam using payment redirection

Sally and Jeff were buying their dream home. They were in constant communication with their conveyancing solicitor and the vendor, both via email and telephone. On 9 November, they received an expected email from their conveyancer, Rick – although in hindsight they now realise it wasn't Rick who sent the email, but a scammer.

The email provided details of the vendor's solicitor's trust account into which Sally and Jeff were to transfer the purchase deposit funds. The email was part of a trail of emails relating to the contract exchange. The 'from' and 'to' email address was Rick's correct email address, so everything looked fine.

The next day, Jeff and Sally went to their bank to arrange the transfer of $440,000 to the trust account. A couple of days later, they received an email from Rick, their conveyancer, which they now also know he did not send. The email confirmed that the deposit funds had been received.

A day after receiving that email, Sally and Jeff were advised that the vendor's solicitor had not received their deposit. After checking emails and making multiple phone calls with the conveyancer, it became clear that their email exchanges had been intercepted and diverted. Jeff and Sally immediately contacted their bank and the bank to which they transferred the money. They also contacted the police. They contacted their conveyancer via telephone. The conveyancer realised their email had been compromised.

Sally and Jeff are working with their bank to find out what happened to their funds.

Ages 55 to 64 years

Table 5.9: Top 5 scams by reported losses for people aged 55 to 64 years

Scam category	Reports	Reports with loss	Losses
Investment scams	881	321	$12,673,140
Dating & romance scams	541	181	$5,361,692
Health & medical products	174	68	$1,521,025
Remote access scams	129	114	$1,287,828
False billing scams	1,655	221	$1,223,967

Investment scams resulted in the highest losses for people aged 55 to 64, with $12.7 million in overall reported losses. Of all investment scams reported by people aged 55 to 64, 36% involved a financial loss. The average loss experienced by a person reporting an investment scam where a loss was incurred was $39,480.

This age group is the only one to include health and medical product scams in the top 5 scams causing financial losses. This was due to one large loss, reported by an overseas reporter, who believed they were dealing with an Australian company and trying to purchase personal protective equipment (PPE). In 2020, there were multiple reports to Scamwatch of people being scammed when trying to purchase face masks, hand sanitiser and other forms of PPE, likely as a result of the COVID-19 pandemic.

A celebrity endorsement scam falsely using the likeness of celebrity chef Maggie Beer also impacted this age group. The scam offered Cannabidiol (CBD) oil for pain relief. When people purchased the product, they would be charged additional fees or subscription fees, yet never receive the product.

65 years and over

Table 5.10: Top 5 scams by reported losses for people aged 65 years and over

Scam category	Reports	Reports with loss	Losses
Investment scams	827	253	$18,525,957
Dating & romance scams	402	146	$7,841,352
Remote access scams	2,013	298	$5,567,231
Unexpected prize & lottery scams	805	67	$745,837
False billing scams	2,647	256	$709,755

People aged 65 years and over lost the most money ($18.5 million) of all age groups to investment scams. What is most concerning about this finding is that of the 827 reports about investment scams made by people 65 years and over, only 253 (30%) of reports involved a financial loss. The means the average loss to an investment scam by a person aged 65 years and over was $73,225.

Remote access scams affect older Australians more than any other age group. In 2020, people aged 65 and over lost over $5.5 million to this scam type. Of the total $8.4 million lost by Australians to remote access scams in 2020, 66% was lost to people aged 65 years and over. In 2020, remote access scammers impersonated trusted organisations such as NBN Co, Telstra and Optus, internet providers and payment platforms such as PayPal.

▶ Case study 5.4: Remote access scams aimed at people aged 65 years and over

Grant received a phone call from someone saying they were from NBN Co asking if his internet was slow as apparently an automatic fault report had been sent to them. When Grant said yes, it was slow, he was transferred to an NBN Co representative. The representative advised Grant there were issues with his computer because overseas hackers were accessing the internet. The representative asked Grant to download a program so he could see what the hackers were doing and then they could be stopped.

Grant was a bit suspicious, but did as asked. The representative told him that when he opened the program, it would show a message about scammers. So, when the program opened with that message, Grant thought the representative must be legitimate.

The representative asked Grant what sort of sites he visited, what apps he used and if he used the computer for internet banking. Grant provided the information and the representative asked Grant to open his internet banking to see if the hackers were accessing that program too. The representative said the hackers had access to everything. He then asked Grant to check which lights were lit on his modem.

When Grant returned to the computer, he found the screen black. He asked the representative what had happened. The representative told Grant that because the lights were flashing a certain way, he had to run more security measures which could shine UV rays that were harmful to eyes so he had darkened the screen.[42]

He told Grant to leave the computer running overnight but to turn off the screen. He also told Grant to turn off his phone as it may be affected too. Grant had been on the phone for almost 2 hours while the representative did everything to fix the computer so he was happy not to receive any more calls.

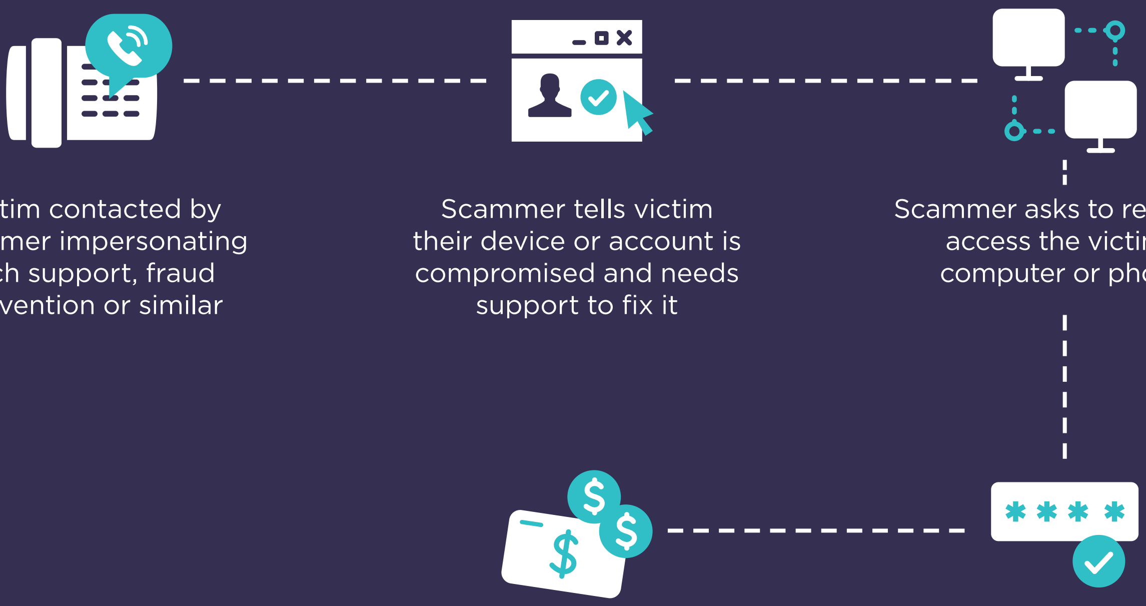
The next morning Grant turned on his phone and received several messages about amounts being transferred from his accounts. He called his bank and they told him he was the victim of a remote access scam.

Grant lost almost $30,000 to the scammer.

[42] This tactic is commonly used by scammers so victims cannot see what they are doing e.g. transferring money from their accounts.

REMOTE ACCESS SCAMS

Scammers convince victims to provide them with control of their phone or computer



Victim contacted by scammer impersonating tech support, fraud prevention or similar

Scammer tells victim their device or account is compromised and needs support to fix it

Scammer asks to remotely access the victim's computer or phone

Scammer requests the victim download remote access software and accept the scammer's request to connect to their device

Scammer accesses victim's banking/personal information, uses information to impersonate victim to commit identity theft or steal money

STATISTICS

Combined losses:

$33.7 million

Scamwatch and bank data in 2020

Scamwatch received **8,473 reports** in 2020, with **losses of $8.4 million**, almost double the losses from 2019

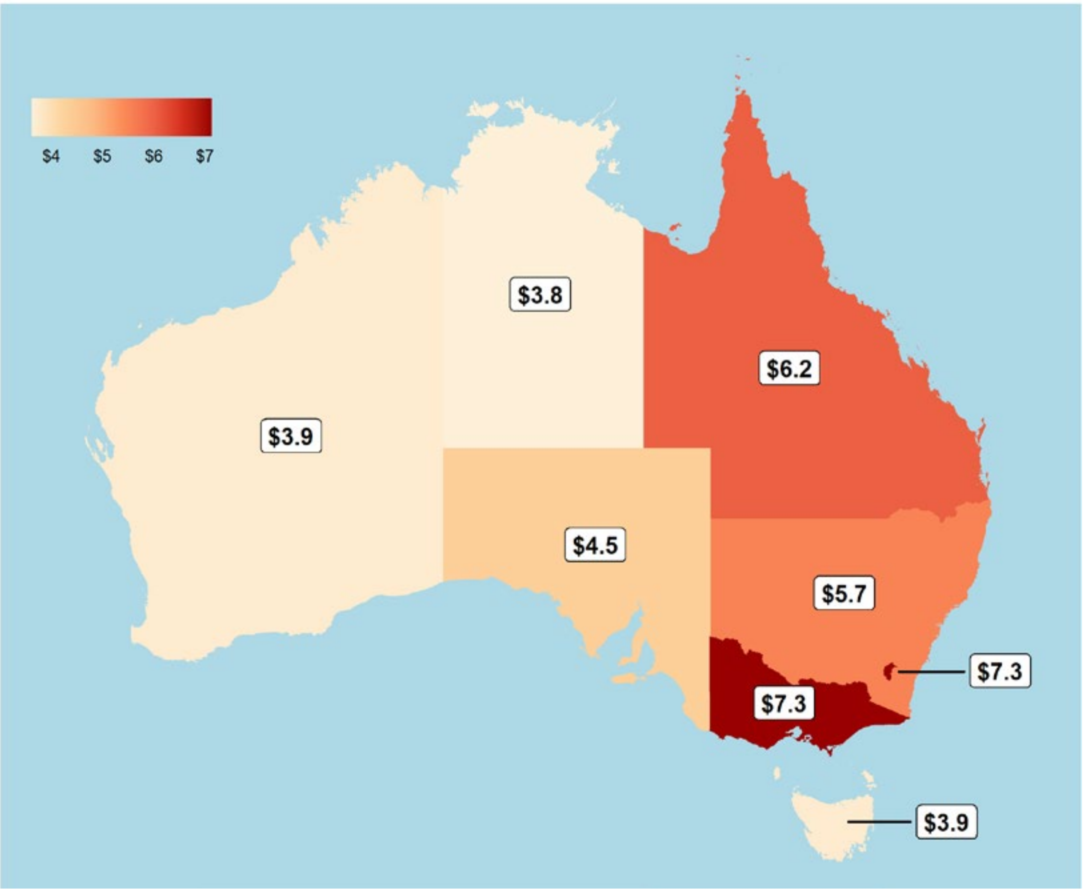
PROTECT YOURSELF

Never give an unsolicited caller remote access to your computer

If you receive a phone call out of the blue about your computer and remote access is requested – hang up

5.2 Location of scam activity

Figure 1: Amount lost to scams per capita[43]



This heat map illustrates the different ways that scams affected the states in 2020. Victoria and the Australian Capital Territory lost the most money to scams per capita.

For the first time, Victoria's losses were the highest of all the states and territories. In previous years, reporters from New South Wales reported the most scams and suffered the highest losses. In the ACCC's view, the increase in losses in Victoria is more than likely attributable to the lengthy Victorian lockdowns during the COVID-19 pandemic. The lockdowns caused changes in many circumstances, which may have resulted in increased susceptibility to scams including:

- people losing their jobs or accessing JobKeeper, which may have increased vulnerability to government impersonation, early access superannuation scams and investment scams (as a quick and easy way to make additional income)
- increase in online shopping scams due to many retail stores being closed
- increased loneliness, which may have had a range of effects including a rise in puppy scams as well as a rise in the use of online dating platforms and social media sites.

The Australian Capital Territory has just 1.7% of the Australian population. However, ACT residents were overrepresented in making scam reports. This means that on a per capita basis, the ACT lost a proportionally higher amount to scams of all states, except Victoria.

[43] Total amount lost to scams per state divided by latest state population estimate (Australian Bureau of Statistics). Only reports from Australian reporters are included in the heat map. Figures refer to millions.

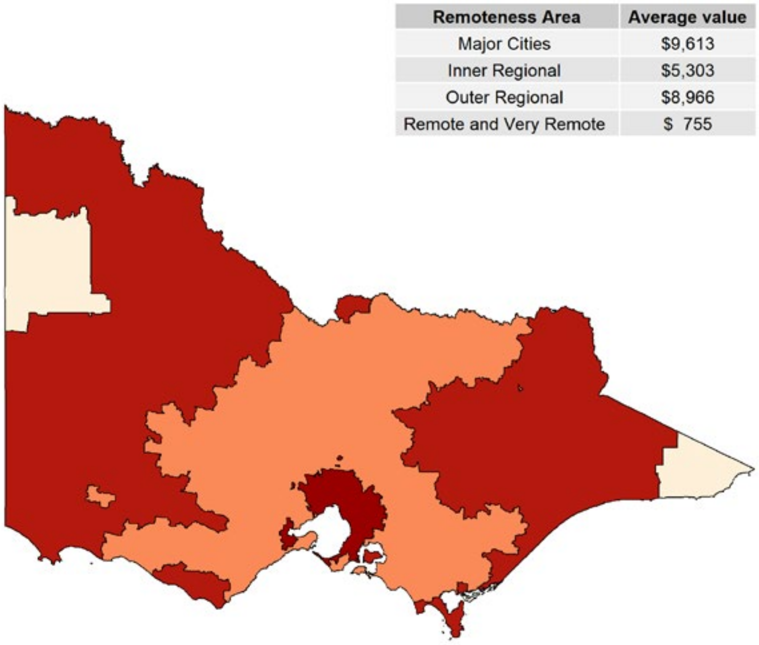
Table 5.11: Reports by location[44]

State/territory	Reports	Reports with loss	Losses
VIC	57,425	6,133	$49,096,516
NSW	64,960	6,134	$46,330,678
QLD	39,298	3,864	$32,184,253
WA	19,837	1,853	$10,307,928
SA	14,190	1,334	$7,986,068
ACT	7,235	288	$3,127,903
TAS	3,734	405	$2,123,588
NT	2,282	286	$928,801
Overseas	6,536	2,208	$14,719,630
Not provided	590	97	$8,878,726

The state reporting the highest average losses was Queensland, where for every scam reported by Queenslanders that included a financial loss, the average loss was $8,329.26.

Further analysis on Victoria was undertaken using heat maps to consider differences in metro, rural and remote areas (using the Australian Bureau of Statistics' remoteness areas[45]). The ABS has 5 categories: major cities, inner regional, outer regional, remote and very remote. Due to low numbers of reporters in both the remote and very remote geographical areas, these 2 classifications were merged for the purposes of creating heat maps.

Figure 2: Average loss to scams per region of Victoria



Remoteness Area	Average value
Major Cities	$9,613
Inner Regional	$5,303
Outer Regional	$8,966
Remote and Very Remote	$ 755

The red areas represent the higher average losses, which are concentrated around Melbourne and other cities in Victoria. However, as can be seen in the table, people in the outer regional areas (also shown as red) lost an average of $8,966 per scam. This may mean that more needs to be done to raise awareness about scams in regional Victoria.

[44] 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.

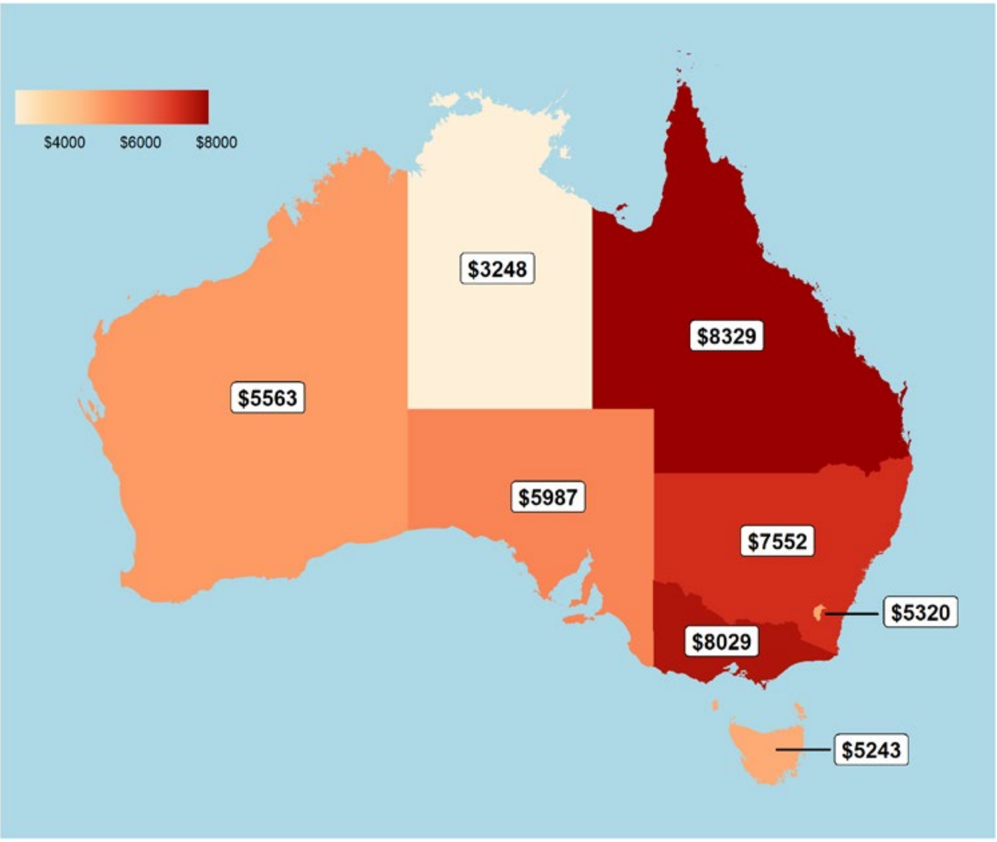
[45] ABS 2021 Regional population: Statistics about population and components of change (births, deaths, migration) for Australia's capital cities and regions.

Table 5:12: State and territory populations by reports

State	% of Australian population	% of reports made to Scamwatch	Reported losses	% of total reported losses	% change in losses from last year
NSW	31.8	30.1	$46,330,678	26.4	13.7
VIC	26.1	26.6	$49,095,516	27.9	73.6
QLD	20.1	18.2	$32,184,253	18.3	-4.1
WA	10.4	9.2	$10,307,928	5.9	-36.9
SA	6.9	6.6	$7,986,068	4.5	13.6
TAS	2.1	1.7	$2,123,588	1.2	-13.7
ACT	1.7	3.3	$3,127,903	1.8	-6.3
NT	1.0	1.1	$928,801	0.5	-67.0

The losses reported for each state and territory in 2020 were examined against the losses reported in 2019 to see if there were differences. New South Wales, Victoria and South Australia all contributed more to the overall losses for 2020 than they did in 2019. The losses experienced by Victorian reporters as part of the total losses in 2020 increased by 74% from the proportion of total Victorian losses experienced in 2019.

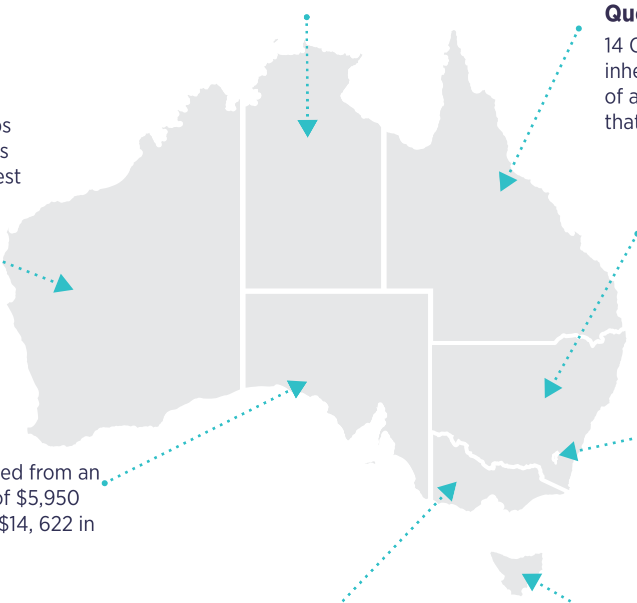
Figure 3: Average value of scams with losses in each state[46]



The average value of each scam tells a different story. Queensland residents reported the highest average losses to scams ($8,329), followed by Victoria with an average of $8,029. The Northern Territory had the lowest average losses at $3,248, down from $7,824 in 2019.

[46] Total amount lost to scams by state divided by number of scam reports that included a loss. Only reports from people in Australia were included in the analysis.

Figure 4: Points of interest from each state and territory



Northern Territory
Highest losses for dating and romance scams with $334,000 reported

Queensland
14 Queenslanders lost $825,62 to inheritance scams. So for every report of an interitance scam with a loss, that person lost $58,961

Western Australia
The average loss to jobs and employment scams was $16,196 – the highest average loss of all jurisdictions

New South Wales
On average, every person residing in NSW who reported a dating and romance scam with a financial loss lost $42,170

South Australia
Rebate scams increased from an average loss in 2019 of $5,950 to an average loss of $14, 622 in 2020

ACT
The largest single loss in the ACT was $300,000 to a cryptocurrency investment scam

Victoria
Of all Australian jurisdictions, Victoria has perhaps suffered the most due to COVID-19. This had an impact on scams reported, for example, Victorians lost over $2.1 million to health and medical products scams

Tasmania
The highest individual loss was $200,000 to an unexpected prize and lottery scam

5.3 The impact of scams on Indigenous Australians

In 2020, Indigenous Australians reported 3,445 scams, with reported losses over $2 million. While there were more scam reports made in 2020 than in 2019, the losses were 4% lower than the losses reported in 2019. This is a trend that continues from 2019, where the losses reported in that year were 30% lower than those in 2018.

Indigenous Australians reported 25% more scams in 2020 than they did in 2019. A corresponding increase in losses would therefore be expected. However, of the 3,445 scams reported, just 556 experienced a financial loss. Many reports (1,230) involved the loss of personal information.

The loss of personal information is problematic. 2020 saw an increase in phishing scams, identity theft and remote access scams (see appendices for comparison statistics). While an initial financial loss can be crippling, the lasting impacts resulting from the loss of personal identification information can have just as serious an effect in terms of causing lasting financial harm. It can also take victims significant time to recover their identity.

Table 5.13: Scam types reported by Indigenous people

Scam category	Reports	Reports with loss	Losses
Dating and romance scams	136	44	$590,553
Investment scams	131	61	$336,794
Online shopping scams	277	166	$275,661
Classified scams	149	59	$149,222
Jobs & employment scams	52	12	$146,385
Identity theft	376	18	$131,054
Threats to life, arrest or other	472	8	$89,882
False billing	203	36	$66,755
Unexpected prize & lottery scams	131	16	$65,135
Hacking	150	11	$26,829

The highest losses for Indigenous Australians were experienced by those aged 25 to 34.

Figure 5.13: Top 5 scams by highest reported losses to Indigenous consumers

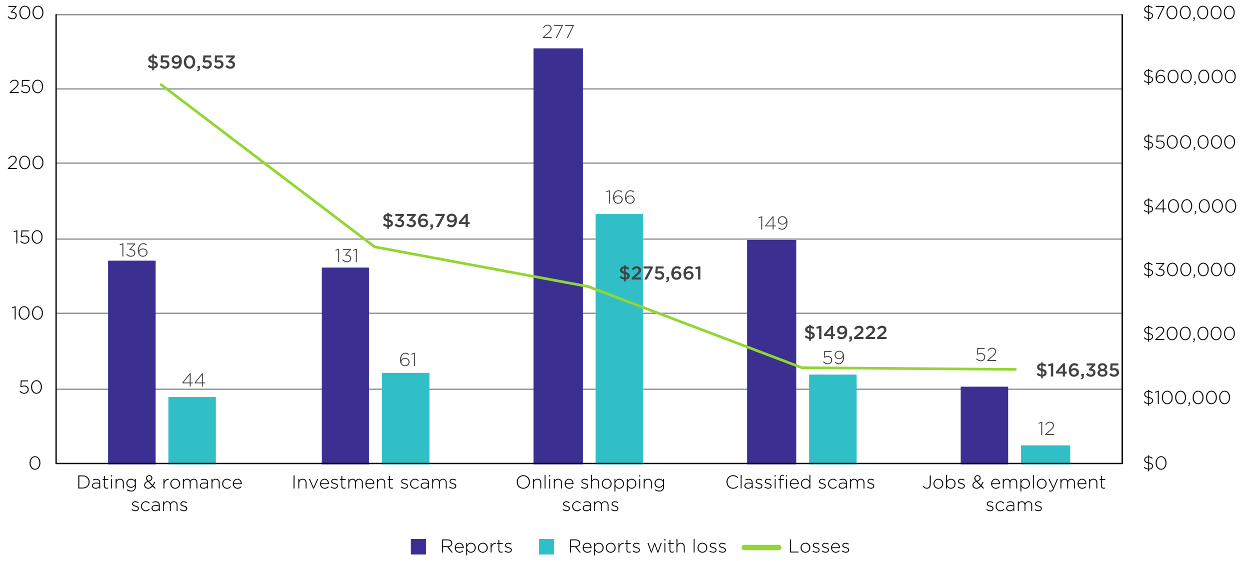


Table 5.14: Breakdown of age ranges in reports by Indigenous people

Age group	Reports	Reports with loss	Losses
Under 18	74	17	$140,484
18–24	413	100	$157,982
25–34	789	143	$818,700
35–44	595	117	$151,963
45–54	550	92	$311,269
55–64	351	37	$314,342
65 and over	185	16	$68,792
Age not provided	488	34	$39,996

▶ Case study 5.5: Dating and romance scam – Pat aged 55 to 64 years, losses of over $38,000

Pat was deceived by the promise of a lifetime relationship and marriage. The scammer used his claimed status as a single father and his dying mother as further ways to emotionally blackmail Pat in addition to making his claims to need money seem legitimate.

He asked Pat to help him get a visa to move to Australia. Pat paid all the fees and organised the paperwork, but he did not complete any of it. Neither did he get the police check or medical checks that Pat had arranged for him.

Pat eventually had to tell him she was out of money. That was the end of their relationship.

Table 5.15: Location of Indigenous people reporting to Scamwatch[47]

State	Reports	Losses	Percentage of total reports from Indigenous people	Percentage of Australian Indigenous population
NSW	1,133	$632,176	35.6%	33.3%
QLD	845	$579,952	26.6%	27.7%
VIC	401	$121,001	12.6%	7.2%
WA	252	$322,789	7.9%	12.6%
SA	176	$126,183	5.5%	5.3%
NT	156	$84,710	4.9%	9.5%
ACT	128	$61,039	4.0%	0.9%
TAS	88	$24,966	2.8%	3.6%
Total	**3,179**	**$1,952,816**	**99.9%**	**3.3%**

Indigenous people residing in Victoria represent approximately 7% of all Indigenous Australians. However, they reported almost 13% of all reports made by Indigenous people in 2020. Indigenous people in New South Wales and the Australian Capital Territory also reported proportionally higher scams than their state/territory's Indigenous population.

Your Rights Mob

The ACCC leverages social media to provide timely messages to Indigenous consumers, including scams information, through our Your Rights Mob Facebook page. Examples of scams information included on the page in 2020 were warnings of online shopping scams during the holiday season and scams on classified sites. The fact that 225 Indigenous consumers reported losing money to these types of scams in 2020 shows how important it is to issue these warnings.

The Your Rights Mob platform also encourages and facilitates reporting and discussion among Indigenous consumers about scam conduct. Telling friends and family about scams is one of the best ways to protect yourself and loved ones.

National Indigenous Consumer Strategy

The ACCC is the Chair of the National Indigenous Consumer Strategies (NICS) National Project (Too Good to be True). As the COVID-19 pandemic resulted in the ACCC and other NICS regulatory office members suspending physical outreach visits to Indigenous communities, we deferred the implementation of the 2020–2022 NICS Action Plan to assist members in reprioritising resources due to COVID-19.

While the COVID-19 pandemic prevented staff from undertaking physical outreach with Indigenous communities, the NICS team found other ways to stay in touch with Indigenous stakeholders and their advocates.

Activities undertaken during the pandemic included discussions about Australian Consumer Law (ACL) related matters, and scam conduct that may be occurring within Indigenous communities.

[47] Table only includes reports from Indigenous Australians who provided state/territory information.

5.4 The scams experienced by CALD communities

Reports by people with English as a second language[48]

In 2020, people with English as a second language made 11,702 reports to Scamwatch, with $22.1 million in losses. This represents a 50% increase in reports from 2019 as well as an increase of 61% in losses. In terms of the wider population of reporters to Scamwatch, people who identified as speaking English as a second language represented 5.4% of all reports made to Scamwatch, but 12.6% of all losses for 2020.

Threats to life, arrest or other contributed to the increase in losses for linguistically diverse communities (see table 5.16). These losses increased by almost 248% from the $1.7 million reported lost in 2019 to almost $6 million in 2020.

Table 5.16: Top 10 scams by loss for people with English as their second language

Scam category	Reports	Reports with loss	Losses	% change in losses from 2019
Investment scams	548	279	$6,319,927	19.8%
Threats to life, arrest or other	1,952	156	$5,998,117	248.0%
Dating and romance scams	356	138	$5,569,619	107.4%
Online shopping scams	975	608	$798,395	189.4%
Remote access scams	399	43	$579,202	15.8%
Classified scams	414	176	$422,020	5.9%
Identity theft	1,500	78	$389,173	203.8%
False billing	472	130	$366,858	-41.0%
Betting & sports investment scams	22	15	$352,480	124.9%
Phishing	1,575	48	$301,362	-5.0%

The 2016 Australian Bureau of Statistics census found that most of the population who were born overseas lived in a capital city, with the highest proportion living in New South Wales.[49]

Table 5.17: State or territory where culturally diverse people resided, by highest losses

State/territory	Reports by state, all reporters	Reports by culturally diverse people (% of all reports)	Reports with a financial loss (CALD)	Losses
NSW	64,960	3,776 (5.8%)	537	$7,537,884
VIC	57,425	3,178 (5.5%)	591	$6,308,517
QLD	39,298	1,750 (4.5%)	266	$4,220,623
WA	19,837	737 (3.7%)	118	$686,082
ACT	7,235	389 (5.4%)	62	$662,624
SA	14,190	632 (4.5%)	91	$491,337
TAS	3,734	119 (3.2%)	20	$251,520
NT	2,282	143 (6.3%)	23	$210,518
Overseas	6,536	907 (13.9%)	262	$401,819
Not provided	590	71 (12.0%)	14	$1,371,583

[48] Whilst the ACCC typically uses the terminology of 'Culturally and Linguistically Diverse' (CALD) to refer to this segment of the Australian population, we have used the phrase 'people with English as a second language' here as the Scamwatch report form asks reporters whether they speak English as a second language.

[49] ABS 2017. 2071.0 Census of Population and Housing: Reflecting Australia – Stories from the Census, 2016: https://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/2071.0~2016~Main%20Features~Cultural%20Diversity%20Data%20Summary~30.

Chinese authority scams (threats to life, arrest and other)

Since 2018, reports and losses to Chinese authority scams have consistently increased. In 2020, Scamwatch received 2,082 reports, with reported losses of $7,044,098. This is a 77% increase in the number of reports and a 250% increase in the amount reported lost compared with 2019. Chinese authority scams specifically target Mandarin speakers in Australia.

Most Chinese authority scams are robocalls, which may impersonate the Chinese Embassy in Australia, or more commonly, a courier company. There are many variations of this scam but a common scenario reported to Scamwatch is one in which the scammer claims to be from a courier company and that the person has tried to send a package to China that contains contraband, such as counterfeit credit cards or fake driver licences.

The scammer then tells the person they will transfer the call to the police in mainland China to sort out the misunderstanding. The police (scammers) will then negotiate with the person to pay money to begin an investigation, or to pay money into a holding account as proof they have money and would therefore not be engaged in criminal activities.

In 2020, these scams also used the fear associated with the pandemic to coerce people into paying money. Scamwatch received several reports of scammers pretending to be the Chinese Centre for Disease Control and Prevention or the Beijing Centre of Epidemic Prevention, accusing people of violating quarantine or not reporting to the Australian Government.

▶ Case study 5.6: Chinese authority scam

Terry received a call on a Monday morning, purportedly from DHL, the global logistics company, telling him that he had sent an illegal parcel to Shanghai.

The DHL representative said they were going to transfer the call to the police in Shanghai so Terry could tell them a mistake had been made.

The police (scammers) told Terry they suspected he was involved in money laundering and he might be extradited to China. They told Terry to call them back on a WhatsApp number. They showed him a warrant for his arrest and stated that if he didn't cooperate, they would have him arrested. Terry was told that to avoid arrest, he had to transfer all money from his Australian bank accounts to China so the police could check the serial numbers. He was also told to provide a bail pending payment for the investigation to proceed.

After a few days, Terry had not heard back from the Chinese police. He called the Australian police to see if they had heard anything, who informed Terry he was the victim of a scam.

Terry lost $150,000 to the scammers.

Reducing the impact of scams on culturally diverse people

People who speak English as a second language or live in culturally and linguistically diverse (CALD) communities are just as vulnerable to scams as other sections of the community. However, ensuring scam warnings reach these groups can be more challenging.

In 2020, the ACCC took additional steps to ensure scam warnings reached a diverse range of communities. With the increase in reports and losses to Chinese authority scams, the ACCC translated messages into traditional and simplified Chinese to warn people, especially young students about these scams.

For example, in order to make the Chinese community aware of these scams and how to avoid them, in 2020 the ACCC:

- updated the Scamwatch website with information about these scams and how consumers can protect themselves[50]
- discussed these scams in 2 media releases, which included warnings for the Chinese community in Australia[51]
- produced a factsheet about threat based scams in simplified Chinese and traditional Chinese
- sent information to universities to provide to their international students to warn them about these type of scams.

The ACCC's *Little Black Book of Scams* also contains information about threat based scams and is available in simplified Chinese.

[50] www.scamwatch.gov.au/types-of-scams/threats-extortion/chinese-authority-scams.

[51] www.scamwatch.gov.au/news-alerts/scams-target-all-sections-of-australian-society-including-cald-and-indigenous-communities; www.scamwatch.gov.au/news-alerts/threat-based-scams-targeting-young-people-and-chinese-community

CHINESE AUTHORITY SCAMS

Scammers impersonate Chinese authorities or businesses to intimidate victims into sending them money

Scammers call victims, say they are from a package delivery company, the Chinese government or Chinese police

Victims are told a crime has been committed in their name and are threatened with jail unless they pay

Victims may be falsely accused of attempting to import drugs, breaching COVID-19 quarantine or money laundering

Victims pay scammers out of fear of being arrested or otherwise penalised

STATISTICS

Losses: Over **$7 million** reported lost

Reports to Scamwatch in 2020

Losses from Chinese authority scams **more than tripled** compared to 2019

PROTECT YOURSELF

Legitimate organisations will never send pre-recorded messages to your phone or threaten you with immediate arrest

Never send money or give credit card details or personal information to anyone you don’t know or trust

Migration scams

In 2020, the ACCC received reports of people impersonating Australian migration agents, either in their home countries or in Australia. Migration scams can be costly and can lead to further scamming as applicants typically supply all their identification, education and work history to migration agents for the purpose of obtaining citizenship.

Last year, people reported losing $71,900 to scammers fraudulently representing themselves as migration agents or people who claimed they could help with applying for Australian citizenship.

Government impersonation scams

In 2020, there were more than 260 reports with losses of over $32,000 from people who were called by scammers pretending to be from the Department of Home Affairs – Immigration. For most Australians, these were nuisance calls and they promptly disconnected. However, these scams appeared more genuine to non-citizens (for example, permanent residents, temporary residents and people seeking citizenship) when told they had not paid an immigration tax, or that they had made a mistake on one of their immigration forms. People in this situation often pay the fines and taxes to scammers to avoid cancellation of their visa.

During 2020, the ACCC worked with government agencies to promote information and warnings about government impersonation scams. This included, where consent was provided to do so, passing on scam reports to relevant government agencies being impersonated, to help them provide early warnings about scams.

▶ Case study 5.7: Government impersonation scams

Binh received a phone call at 2.30pm. The caller introduced himself as Leo Garcia, a government officer from the ATO. He told Binh she was under investigation for fraud. He said that Binh needed to cooperate so he could clear up the matter.

He provided a case reference number, AT102315, saying he knew that Binh had withdrawn some money from her superannuation. He told Binh that he knew she was a permanent resident of Australia. He also informed her that her application for citizenship would be declined and that she was at risk of being arrested or deported. He advised the investigation was ongoing and then hung up.

Binh then received a phone call from what she thought was a police station in Melbourne. She declined the call, and looked up the phone number on a website to find it was the correct number. When the same number rang again, Binh accepted the call. She was transferred to a police officer named Henri. He told Binh that the fraud investigation involved 15 bank accounts open in her name and that the police needed to freeze all her accounts in order to investigate and catch the real criminal. The police officer told her to go to the bank and withdraw $10,500 from her account. Then he asked her to go to a Bitcoin ATM and deposit the money so the police could trace its movements. Binh did as requested.

The next day, Officer Henri called her again to organise her withdrawal of more money. When Binh went to the bank, the teller asked her why she kept withdrawing large amounts. Scared, Binh told him the whole story. The teller told Binh that it sounded like a scam.

Thankfully, Binh didn’t lose any more money, but she had already lost over $10,000.

5.5 The impact of scams on people with disability

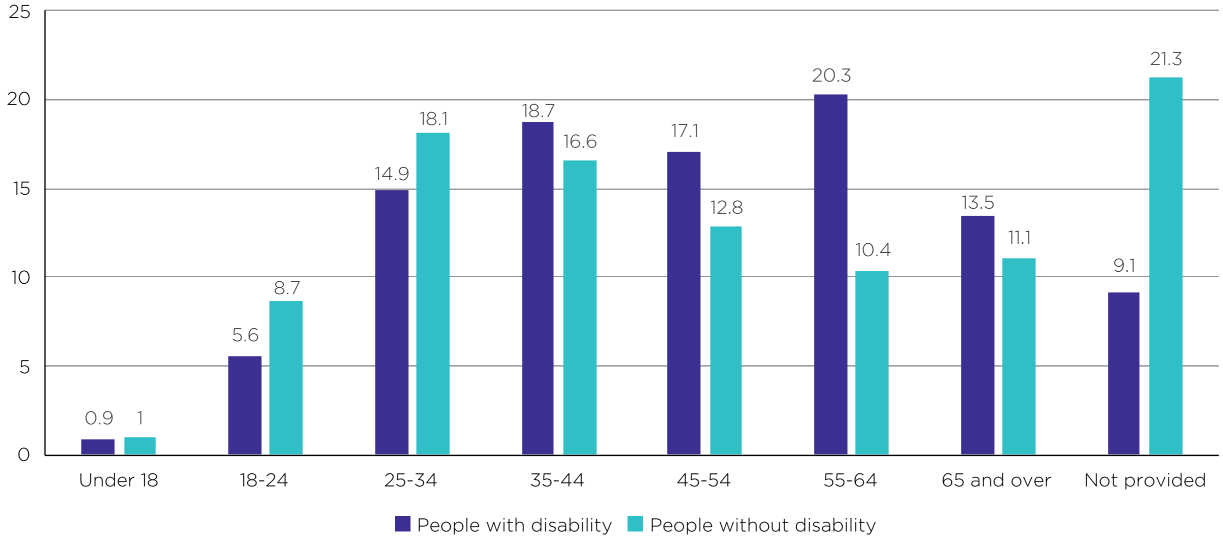
In 2020, there were 7,543 scam reports to the ACCC from people who identified as having a disability[52] or made on behalf of those with a disability, with losses of over $9.7 million. Worryingly, one third of all reporters with disability (33.2% or 2,508 reports) lost personal information to a scammer. This rate of loss of personal information to a scam for people with disability is higher than the 25% experienced by people without disability. The loss of personal information can lead to further scamming and ultimately financial loss.

The Australian Institute of Health Welfare[53] estimates there are 4 million people in Australia living with disability. Research suggests that some people experiencing vulnerability, such as some older people, people with a disability or those with a traumatic brain injury, may be at greater risk of scam victimisation.[54]

People with disability may be eligible for a range of government supports and benefits[55], and as such may be targeted by scammers trying to access government funds. The loss of personal information can lead to fraud against government agencies such as Services Australia, the Australian Tax Office, the National Disability Insurance Scheme and other agencies.

People with disability aged 35 years and over lost personal information to scammers at a higher proportion than people without disability.

Figure 6: Age and percentage of people with and without disability reporting loss of personal information



[52] When reporting to Scamwatch, people have the option of disclosing if they have a disability or some other condition which might make them more vulnerable to scams compared to the general population. This may include age related factors, having a chronic illness or a disability. This is a self-report function and no further questions are asked about the nature or type of disability or illness.

[53] AIHW 2019 'People with disability in Australia 2019: In brief': www.aihw.gov.au/reports/disability/people-with-disability-in-australia-in-brief/contents/how-many-people-have-disability.

[54] Gould K, 2020. Monash University Lens 'Blind spot: Are those with acquired brain injuries more vulnerable to being scammed?' lens.monash.edu/@medicine-health/2020/12/16/1381858/blind-spot-are-those-with-acquired-brain-injuries-more-vulnerable-to-being-scammed.

[55] Services Australia: www.servicesaustralia.gov.au/individuals/people-disability.

Specific scams impacting people with disability

People with disability lost the most money to romance scams ($5.5 million). Dating and romance scams involving a financial loss comprised 39% (112 reports), compared with 25% of the wider Australian population.[56]

Little research has been undertaken on people with disability and scam vulnerability. However, there is some evidence to suggest that people with disability may be more vulnerable to romance scams. Research conducted by Dr Gould from Monash University into scams and people with acquired brain injury (ABI) found that people with these injuries were vulnerable to romance scams in particular, but also fake charities, jobs and employment scams, and investment scams.[57]

This research indicated that people with acquired brain injury can be particularly vulnerable to romance scams due to a number of factors. Pre-existing relationships formed before these injuries can become strained, people may separate from partners, some sufferers may have received compensation payouts from accidents and some are lonely following their injury.

The study also found that people with acquired brain injury are less likely to be in romantic relationships.[58] Of people with ABI, 75% are male with an average age of 35 years. For this group, a common goal of finishing rehabilitation is to have a romantic partner. Dr Gould found in a survey of 101 Australian and New Zealand clinicians working with people with brain injuries, 50% reported having clients who had some point been involved with a romance scammer.[59]

As shown in table 5.18, reports of investment scams by people with disability caused losses of $2.6 million. Other scams with high losses were online shopping, classified, remote access, and threats to 'life, arrest or other' scams.

Table 5.18: Top 10 scams reported by people with disability in 2020, by highest losses

Scam category	Reports	Reports with loss	Losses
Dating and romance scams	285	112	$5,543,375
Investment scams	350	95	$2,624,007
Online shopping scams	478	250	$242,955
Remote access scams	305	33	$200,427
Threats to life, arrest or other	947	22	$165,775
Classified scams	239	90	$150,076
Unexpected prize & lottery scams	279	28	$116,552
Inheritance scams	86	6	$108,848
False billing	438	71	$101,637
Phishing	1,326	34	$82,051

[56] This percentage only includes reports where the reporter did not select that they had a disability.

[57] Gould K, 2020. Monash University Lens 'Blind spot: Are those with acquired brain injuries more vulnerable to being scammed?' www.lens.monash.edu/@medicine-health/2020/12/16/1381858/blind-spot-are-those-with-acquired-brain-injuries-more-vulnerable-to-being-scammed.

[58] ibid.

[59] ibid.

More research is needed to understand the vulnerabilities of people with disability to scams. Disability is an umbrella term for impairments, activity limitations and participation restrictions, all of which can interact with a person's health condition(s) and environmental and/or individual factors.

People with disability are diverse, and may include people with cognitive impairments, illnesses such as Alzheimer's or dementia, vision or hearing impairments and mobility issues. The diversity of disability means that warnings about scams need to be varied and wide-reaching to best educate this section of society on how to be scam aware.

Reducing the impact of scams on people with disability

The ACCC arranged a presentation for the Scams Awareness Network by Dr Kate Gould, to increase awareness of the impact of acquired brain injury and vulnerability to scams. The ACCC also held meetings with disability advocacy groups to find out more about scams impacting this section of society. Although the pandemic meant attending community groups to talk about scams was impossible, it did provide the ACCC's Scamwatch team the opportunity to speak to more community groups about scams via virtual presentations. These meetings allowed attendees to write questions in chat boxes if they did not want to speak in front of people, which for some members of the community can be difficult. The ACCC will continue providing virtual presentations about scams throughout 2021, although we are hoping in person community events will be back soon.

6. The businesses

Scam losses reported by businesses increased by 260% in 2020, from $5 million in 2019 to $18 million. The top 5 scam categories reported by businesses are outlined below.

Table 6.1: Top 5 scams reported by businesses

Scam category	Number of reports	Reports with loss	Reported losses
False billing	917	201	$13,509,327[60]
Other scams	694	37	$11,733
Phishing	689	21	$52,057
Identity theft	278	22	$57,121
Hacking	229	8	$26,902

Businesses made the most reports to Scamwatch about false billing scams and suffered the highest reported losses to these scams. Common false billing scams include:

- business email compromise (also known as payment redirection scams). Scammers trick people into changing payment details to divert money, usually by impersonating the intended recipient of a payment. See Case Study 6.1 and Section 6.2 for more information
- scammers requesting payment for fake invoices e.g. for directory listings, advertising, domain name renewals or office supplies that were not ordered or delivered.

Businesses also reported high losses to health and medical scams. Around half of the overall $3.9 million in losses reported to health and medical scams were from businesses. This appeared to be due to COVID-19 as businesses attempted to procure personal protective equipment and other hygiene products to comply with government guidelines and keep their staff safe.

Businesses also reported almost $500,000 in losses to online shopping scams. There were a number of common scenarios that appeared to contribute to this:

- No goods delivered scams – scammers set up fake websites purporting to sell items ranging from electronic devices to vehicles to farming equipment. COVID-19 was used as an excuse to not allow buyers to view goods in person prior to making payment.
- Fake buyers – scammers posed as legitimate customers and tried to scam businesses out of goods.
- Impersonation – fake websites were set up to impersonate a legitimate business in order to scam customers.

Table 6.2: Breakdown of scam reports by business size

Business size	Number of reports	Reports with loss	Reported losses
Micro (0–4 staff)	1,304	173	$2,057,087
Small (5–19 staff)	1,056	153	$4,950,593
Medium (20–199 staff)	651	90	$1,578,852
Large (over 200 staff)	321	29	$9,031,213
Size of business not provided	852	49	$783,418
Total	**4,184**	**494**	**$18,401,163**

The largest number of scam reports from businesses came from micro and small businesses. The majority of reports from small and micro businesses were false billing (536 reports), phishing (315 reports) and identity theft (156 reports). Of the 139 reports received about fake charity scams, 49 were from small and micro businesses.

There were also a large number of reports about classified scams. This is likely due to the many vehicle and heavy machinery classified advertising scams that targeted farm owners during the pandemic.

[60] This included one high loss scam of $8 million lost to a Hong Kong business through an Australian bank account.

Large businesses experienced the highest losses. Reports from large businesses were spread more evenly across the scam categories, but the most reported category by large businesses was phishing, with 77 reports.

Losses reported by small businesses increased in 2020, largely due to a $2 million scam related to the purchase of PPE during COVID-19. In addition, small businesses reported a handful of business email compromise scams, with losses of $1.7 million.

▶ Case study 6.1: Payment redirection scam impacts small conveyancing business

Lisa ran a small conveyancing business. A fake domain of www.123lavv.com.au had been registered to send phishing emails to Lisa's clients.

On 10 March 2020, Lisa received an email that appeared to be from Simone, one of the firm's clients, about an upcoming property settlement. The email address Simone normally used was Simone@prankington.com, but the scammer had emailed Lisa and changed one letter so the email read as Simone@prankrington.com, which went unnoticed by the firm.

On the same day, Simone, the client, received a modified email purporting to be from Lisa's assistant Dom, with an email address of Dom@123lavv.com.au. However, Dom's real email address was Dom@123law.com.au.

Simone received an email from the scammer purporting to be Dom on 20 March 2020 requesting payment to a fake bank account for settlement in April. In April, Simone transferred $150,000 from her bank account to the specified account, 123Law Client Trust, at a big 4 bank. The bank did not detect the discrepancy.

The next day, when the money had not been received into the correct account, the conveyancing firm became aware of the issue and contacted Simone. Simone then sought to get the money back from the bank. The conveyancing business reported the issue to Scamwatch.

6.1 Heavy machinery/tractor sales

Last year, Scamwatch received 334 complaints about a new scam type involving tractor and heavy machinery, with $1.1 million in reported losses. These scams arose during the COVID-19 pandemic and involved fake online listings for farm equipment, such as tractors, bulldozers, backhoes, diggers and other agricultural machinery, at prices well below the average market rate. Heavy machinery scams predominantly targeted farmers who were looking for a good deal on equipment. In many of the instances reported to us, the scammers used COVID-19 as an excuse to convince small business owners to pay up-front for these items without physically seeing them.

▶ Case study 6.2: Heavy machinery scam report

'The scammers have a very impressive website offering cheap tractors that prove too good to be true. The website is even written eloquently but when you contact them, the replies (supposedly from the sales manager) are in terrible English.

They are claiming due to COVID-19 you cannot visit them or inspect the tractors, but they will deliver for free in 14 days with a free return policy. It all starts to become very fishy and when you image search their profile photos (taken from the About Us page) you realise it is all a scam.'

6.2 Business email compromise scams

Combined losses for business email compromise scams totalled $128 million in 2020. While down slightly from 2019, these scams remain a significant problem for businesses and individuals.

Scamwatch received around 1,300 reports of business email compromise scams in 2020, with over $14 million in reported losses. This was a substantial increase from approximately 900 reports and $5 million in losses in 2019, although it was impacted by some significant high loss reports. These scams targeted a large range of businesses, including real estate, construction, law, recruitment, sports and community clubs, and universities.

Business email compromise scams, also referred to as payment redirection scams, involve scammers impersonating a business or its employees via email and requesting that money be sent to a fraudulent account. Scamwatch receives reports both from businesses that have been impersonated in this way and other businesses or individuals who have paid a scammer as a result of a business email compromise scam.

Scammers can quickly find the names of a business' senior staff and the likely format of their email addresses online. They can also hack into email accounts, including through information gathered in phishing scams.

▶ **Case study 6.3: Business email compromise scam**

Scammers hacked Fiona's work email account and created a new email rule that redirected any emails containing the words 'payment', 'invoice' or similar terms to the scammer's email address. The scammer was then able to intercept an invoice Fiona sent a client and changed the payment details on the invoice to their own bank account. When the client received the invoice, which appeared to come from Fiona, they paid over $15,000 directly into the scammer's bank account.

If a scammer gains access to a business email account, they can use the business' mailing lists to send large numbers of fake invoices that provide the scammer's payment details in place of the real bank details. Scammers may 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.

'They intercepted an email PDF invoice to one of our clients and emailed them to advise that our business bank accounts had changed. They made the email look like it came from me.' April 2020, $15,482 lost.

Another variant of this scam type involves no actual compromise of a business' email account. Instead, scammers create an email address that looks like the business' email on casual inspection and uses it to contact their staff or clients. Scammers often rely on urgency to pressure people into transferring funds quickly, before their story can be checked.

▶ **Example** – a scammer impersonating the email address john-smith123@email.com might use the same email but with a slight change, such as john_smith123@email.com, then send their scam from the fake email, making it hard for recipients to tell that it's a fake. A scammer might pretend to be someone's manager and email them asking them to complete an urgent task, in order to get the victim to act quickly and without questioning.

The ACCC has been actively working with banks and law enforcement agencies to help prevent these scams occurring by sharing Scamwatch data and providing scammers' contact and account details where possible. The ACCC has also been advocating for improvements to payment systems in Australia to check names against BSB and account numbers.

7. The fight against scams

In the continuing fight against scams, scams awareness and disruption remained major priorities for the ACCC in 2020. The ACCC's goal in responding to scams is to minimise the opportunity for harm to consumers, business and the broader economy.

The conduct described in this report as 'scams' is generally criminal conduct perpetrated by individuals or criminal organisations often (but not always) based overseas. The investigation, arrest and prosecution of these offenders is a matter for law enforcement agencies in Australia and overseas. Investigations are complex and lengthy but we are seeing more instances of coordinated actions around the world. Some of these are covered in this report. Many of these are only enabled because people reported the conduct and organisations shared information.

7.1 The significance of scam reports and information sharing

The ACCC cannot investigate individual scam reports; however, we increased our capacity to analyse reports and share intelligence with law enforcement and other government agencies during 2020. We also expanded our work with the private sector to raise awareness and disrupt scams including by sharing scam reports relating to their services or platforms.

Sharing reports with law enforcement and government

In 2020, the ACCC shared tens of thousands of Scamwatch reports with other government agencies and law enforcement on 262 occasions. Full Scamwatch reports are only shared where a person actively consents to share. These comprised 154 disseminations of Scamwatch reports to relevant taskforces and 108 disseminations of Scamwatch reports to other government agencies.

The reports were shared for use in specific operations or investigations or to provide more strategic understanding of scams. The specific type of reports shared varies depending on the recipient and purpose of the dissemination.

Scam watchlists and other sharing with the private sector

Since 2019, the ACCC has shared relevant anonymised or particular intelligence with private sector organisations, to assist their scams disruption activity. This work was continued and expanded in 2020.

Where the reporter has consented to their report being shared with the relevant body, the ACCC shares Scamwatch reports with the following organisations:

- Big 4 banks via the Australian Financial Crimes Exchange
- Facebook
- Gumtree
- Western Union
- MoneyGram.

We also share Scam watchlists and collaborate with other private sector organisations including:

- NBN Co
- LinkedIn
- SEEK
- Afterpay.

Under the ACCC's Intelligence Sharing Project, we share Scamwatch telephone numbers reported as being used by scammers to telecommunications providers including Telstra, Optus and Vodafone (for more detail about the data shared with these providers, please refer to the Contact Methods section of chapter 2 on page 22.

Feedback from these organisations indicates that Scamwatch reporting is a useful source of intelligence and assists them to minimise the prevalence of scams. These businesses have reported that as a result of receiving this data 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
- can more meaningfully engage with their intermediaries to discuss scams affecting them both
- 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
- removed scam pages and profiles.

As outlined earlier, the ACCC also shares scammer telephone numbers in scam reports with Telstra and a range of other telecommunications companies to assist them to comply with their obligations under the Reducing Scam Calls Code.

International data sharing

In 2020, the ACCC worked with the US Federal Trade Commission to set up processes for sharing select Scamwatch information on alleged scammers each month through the Consumer Sentinel Network, providing access and receiving access to similar reports from 44 other countries. The ACCC assists with law enforcement requests from both domestic agencies and international agencies via the INTERPOL network. We also collaborate via bilateral relationships with foreign partners.

7.2 Law enforcement

ReportCyber

In Australia, victims of cybercrime can report the incident to ReportCyber, a portal that triages information and makes it available to police jurisdictions in the states and territories and the Australian Federal Police.

In 2020, ReportCyber received 58,120 scam reports, with $338.7 million in losses. The highest losses were due to business email compromise scams, with losses of $75.7 million.

Law enforcement during COVID-19

Many law enforcement agencies shifted focus during 2020 to dedicate more resources to fraud and cybercrime during COVID-19.

Law enforcement agencies were able to secure some important results in the fight against scammers in 2020. Internationally, INTERPOL's Operation First Light, a year-long operation that concluded in November 2020, resulted in more than 21,000 arrests of persons involved in telephone and online scams, and over USD 153 million of illicit funds being intercepted.[61]

Similarly, Operation Falcon, a joint INTERPOL, Group-IB and Nigerian Police Force cybercrime investigation, resulted in arrests of people responsible for distributing malware, carrying out phishing

[61] 'More than 20,000 arrests in year-long global crackdown on phone and Internet scams' media release, 10 December 2020: www.interpol.int/en/News-and-Events/News/2020/More-than-20-000-arrests-in-year-long-global-crackdown-on-phone-and-Internet-scams.

campaigns and scam activity worldwide. The gang was believed to have compromised government and private sector companies in more than 150 countries since 2017.[62]

Every year sees domestic prosecutions of scammers. Some examples of scam arrests and prosecutions in Australia from 2020 include:

- The Australian Federal Police and NSW Police arrested 2 members of a text message phishing syndicate as part of Operation Genmaicha in September 2020. A number of private sector organisations including Westpac, Commonwealth Bank, ANZ and TPG Telecom collaborated to provide assistance throughout the operation.[63]
- Victoria Police arrested a man allegedly involved in a suspected financial investment scam in October 2020. The arrest was made as a result of investigations by the Victoria Police E-Crime Squad and the Australian Securities and Investments Commission.[64]
- There were several arrests of independent puppy scammers in different states including a Victorian woman[65] and a Sydney man.[66]
- Queensland Police and the Australian Federal Police made a significant arrest relating to business email compromise where an accountant received funds in excess of $3.3 million from a range of compromised businesses who had their emails intercepted by hackers.[67]
- NSW Police arrested 2 men in connection with a $2.6 million business email compromise scam. The syndicate stole money from businesses across a range of industries including property development, finance and construction.[68]

7.3 Consumer protection

International activity

A common theme across international reports on fraud in 2020 was scammers taking advantage of the COVID-19 pandemic, particularly via emerging cybercrime scams and an increase in phishing, particularly phishing emails.

In the UK and the United States, online shopping scams emerged as one of the most commonly reported scams. The fifth edition of the *Little Book of Big Scams*, published by the Metropolitan Police in the UK, noted that the majority of fraud took place over the internet with online shopping fraud being almost always top of the list in terms of number of reports.

US Federal Trade Commission

The United States Federal Trade Commission (FTC) is the ACCC's counterpart agency in the United States and accepts reports on various types of fraud and scams. The population of the US is much larger than Australia and this is reflected in the high volume of reports it receives.

The FTC recently released a report stating it received 2.2 million fraud reports from consumers in 2020 with $3.3 billion in total reported fraud losses.[69] This was an increase from $1.8 billion in 2019.

[62] threatpost.com/bec-phishing-ring-3-arrests/161616/.

[63] 'SMS phishing fraudster charged in Sydney' media release, 24 September 2020: www.afp.gov.au/news-media/media-releases/sms-phishing-fraudster-charged-sydney.

[64] '20-244MR Man arrested following suspected financial investment scam' media release, 15 October 2020: asic.gov.au/about-asic/news-centre/find-a-media-release/2020-releases/20-244mr-man-arrested-following-suspected-financial-investment-scam/.

[65] 'Woman arrested, charged over string of online puppy scams' media release, 1 August 2020: www.news.com.au/national/victoria/crime/woman-arrested-charged-over-string-of-online-puppy-scams/news-story/fd87b9be1d7982660a47cbdc2a10e8ef.

[66] 'Police arrest man over online puppy scam targeting the lonely during coronavirus' media release, 19 August 2020: www.abc.net.au/news/2020-08-19/police-arrest-man-over-dog-scam-targeting-coronavirus-lonely/12574638.

[67] mypolice.qld.gov.au/news/2020/08/20/money-laundering-arrest-involving-business-email-compromise-scam/.

[68] www.infosecurity-magazine.com/news/australians-arrested-over-26m/.

[69] www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers.

The FTC reported that identity theft, imposter scams (which include romance scams, the impersonation of government and other organisations, and the impersonation of relatives) and online shopping scams were the most common scams reported. Almost $1.2 billion of the total losses were due to imposter scams and $246 million was due to online shopping scams.

The FTC also reported losses of $304 million due to romance scams, an increase of around 50% from 2019. The FTC noted that the economic and social impact of the pandemic might explain this increase.

An FTC press release in December 2020 announced a nationwide crackdown on income scams, which had increased since the COVID-19 pandemic. This crackdown, called Operation Income Illusion, focused on the perpetrators of scams targeting those working from home, those involved in employment scams, pyramid schemes, investment scams and fake coaching courses.[70]

The FTC also took consumer protection action against 2 Voice over Internet Protocol (VoIP) service providers in 2020. This was the first time the FTC had taken action against VoIP service providers:

- In September 2020, the FTC announced that Globex Telecom, Inc. and an affiliated company would pay a total of $1.9 million (USD) to settle FTC and State of Ohio charges that they facilitated a scheme by a third party, Educare, that marketed (including via illegal robocalls) fake credit card interest rate relief, illegally charging consumers millions of dollars.[71]
- In December 2020, the FTC announced that Alcazar Networks Inc. and its owner had settled FTC charges that they facilitated tens of millions of illegal telemarketing phone calls, including some calls from overseas and some that displayed spoofed caller ID numbers.[72]

ACCC consumer protection actions

The ACCC is an independent statutory government authority. Most of our compliance and enforcement work is conducted under the provisions of the *Competition and Consumer Act 2010* (the Act), which includes the Australian Consumer Law. The purpose of the Act is to enhance the welfare of Australians by:

- promoting competition among business
- promoting fair trading by business
- protecting consumers in their dealings with business.

The full list of ACCC compliance and enforcement priorities are publicly listed on the ACCC's website.[73]

While not involving direct action against scammers or scam conduct, some of the actions taken by the ACCC against alleged misleading and deceptive conduct are set out below.

While these cases do not involve scammers as they are commonly understood, they do provide examples of the important consumer protection enforcement activities undertaken by the ACCC that seek to protect consumers both from the misuse of data and from conduct that might be seen by the public to be scam-like. For more information on the ACCC's consumer protection enforcement activities, as well as those relating to competition, product safety, cartels and other priority areas, refer to the annual report for 2019–20 and the 2020–21 report to be released later this year.

- The ACCC instituted proceedings in the Federal Court against Lorna Jane Pty Ltd for alleged false or misleading claims about its 'Anti-virus Activewear'. Lorna Jane claimed that the activewear, which was sprayed with a substance called 'LJ Shield', eliminated and stopped the spread of COVID-19 and provided protection against viruses and pathogens, including COVID-19. The ACCC alleges these claims to be false and misleading. The case is currently before the Court.
- Superfone was ordered to pay $300,000 for making unsolicited calls and misleading consumers after more than 1,400 consumers, including many elderly people, were contacted by its telemarking agents.

[70] www.ftc.gov/news-events/press-releases/2020/12/scammers-leverage-pandemic-fears-ftc-law-enforcement-partners.

[71] www.ftc.gov/news-events/press-releases/2020/09/globex-telecom-associates-will-pay-21-million-settling-ftcs-first.

[72] www.ftc.gov/news-events/press-releases/2020/12/ftc-takes-action-against-second-voip-service-provider.

[73] www.accc.gov.au/about-us/australian-competition-consumer-commission/compliance-enforcement-policy-priorities.

- The ACCC issued a public warning notice about Unfair Dismissals Direct Pty Ltd in December 2020.

Increasingly, the ACCC has focused on the actions of large digital platforms and businesses, particularly in how they handle data and privacy. This includes the publication of the Digital Platforms Inquiry Final Report and the ongoing work and actions taken to implement the recommendations contained within it.[74]

Examples of actions taken that highlight the work of the ACCC in relation to major platforms and the protection of consumer data in 2020 include:

- HealthEngine Pty Ltd (HealthEngine) was ordered by the Federal Court to pay $2.9 million in penalties for engaging in misleading conduct in relation to the sharing of patient personal information to private health insurance brokers and publishing misleading patient reviews and ratings.
- The ACCC lodged an appeal against the Federal Court's decision to dismiss its case against Employsure, in which the ACCC alleged that Employsure's Google Ads misrepresented that Employsure was, or was affiliated with, a government agency.

  On 1 October 2020, the Federal Court found that the Google Ads were not misleading. The trial judge concluded it would be clear to a reasonable business owner that the search results were ads and not affiliated with the government, because they were marked with the word 'Ad' and linked to a '.com', not '.gov', URL. The Court also found that the words 'fair work' had a broad descriptive meaning and were not limited to government agencies.

  'We have appealed this decision because we believe the judge made an error in finding that reasonable business consumers, including smaller and less sophisticated business owners, would not have been misled by the Google Ads,' ACCC Commissioner Sarah Court said. **As at 1 June 2021, the case is currently before the Court**.

WA ScamNet

WA ScamNet is run by the Western Australia Department of Mines, Industry Regulation and Safety. It received 3,489 scam reports in 2020, with reported losses of over $11.8 million. It received the most reports about phishing, classified and online shopping scams, with investment, dating and romance, and threat to life or arrest scams representing the highest reported losses.

WA ScamNet removed 41 scam websites and 84 scam social media accounts during the year. WA ScamNet was also able to assist 14 victims to recover $13,134.99 in funds lost to scammers.

[74] www.accc.gov.au/system/files/Digital platforms inquiry - final report.pdf.

8. The future

This report has outlined a wide range of activities that are being undertaken to combat scams. The ACCC through Scamwatch will continue to work with law enforcement, government and the private sector to minimise the harm caused by scams to Australians.

The ACCC will expand its information sharing and encourage the private sector, particularly financial institutions, digital platforms and telecommunications providers, to identify solutions to prevent scams. In addition, business and government need to protect personal information and increase cyber security to ensure Australia is more resilient to the threats posed by scams.

The ACCC will also continue to use the information in scam reports to inform our awareness raising activities and ensure that Australians have access to information about how to avoid new and common scams. We will also continue to explore how we can improve the information we provide to people who report to Scamwatch, especially to victims of scams.

It is hard to predict the new ways scams will evolve over the coming years. However, there are some prevailing trends that will likely become more prominent in the near future.

It is very common for scammers to utilise current events and crises to make their scam appear more legitimate. We saw this in 2020 where scammers first used the bushfire emergency and then the COVID-19 pandemic as a basis for new scams, including fake charity, puppy scams, phishing and superannuation scams, as discussed earlier in this report. We expect that the COVID-19 pandemic will continue to be exploited by scammers, specifically as vaccines are distributed throughout 2021. For example, scams relating to vaccinations may be:

- buying and selling scams claiming to offer the vaccine in exchange for money
- phishing scams that appear to be for vaccine registration or application
- health based scams that involve selling products that scammers claim to be vaccines.

We also expect the growing trend of scammers claiming to be from the government to continue. New forms of government impersonation scams may also occur, such as emails or text messages containing malware links that may hold threats if an attachment or link is not actioned, similar to the threat based scam phone calls that occurred in 2020.

To help the ACCC identify new scams and new scam trends, we encourage both people who have been scammed and who believe they have spotted a scam, to report it to Scamwatch.

8.1 Concluding comments

Each year the impact of scams increases in Australia. In 2020, scams caused significant financial and other losses at a time when many were already experiencing hardship. However, without the increased focus and initiatives by government, law enforcement and the private sector, the harm would likely have been much worse.

The increasing losses and reports to the ACCC and other agencies demonstrate the need for a continued and concerted whole of community effort to raise awareness of, prevent and disrupt scams. We all have a role to play, whether it is as law enforcement pursuing scammers, businesses and platforms investing in new technology and educating consumers about scams on their websites, or as individuals learning about how to avoid scams and sharing information with family and friends.

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

Reports by losses

Scam type	Number of reports 2020	Reported losses 2020	Number of reports with loss	Percentage change in losses since 2019
Investment scams	7,295	$65,820,313	2,464 (33.8%)	▲6.5%
Dating & romance scams	3,708	$38,916,120	1,289 (34.8%)	▲36.0%
False billing	13,120	$18,464,903	1,799 (13.7%)	▲82.6%
Threats to life, arrest or other	32,215	$11,833,508	558 (1.7%)	▲178.1%
Remote access scams	8,473	$8,441,632	667 (7.9%)	▲74.5%
Online shopping scams	15,306	$7,384,733	8,349 (54.5%)	▲52.4%
Classified scams	7,928	$5,529,413	2,497 (31.5%)	▲96.4%
Health & medical products	1,459	$3,915,689	382 (26.2%)	▲2,079.8%
Identity theft	20,939	$3,072,287	673 (3.2%)	▼-28.7%
Unexpected prize & lottery scams	4,543	$1,706,253	298 (6.6%)	▼-28.5%
Phishing	44,079	$1,689,406	696 (1.6%)	▲11.3%
Inheritance scams	1,676	$1,434,544	59 (3.5%)	▼-45.3%
Hacking	8,691	$1,419,353	425 (4.9%)	▼-72.4%
Jobs & employment scams	2,933	$1,268,582	290 (9.9%)	▼-26.6%
Betting & sports investment scams	448	$985,926	150 (33.5%)	▼-18.2%
Nigerian scams	577	$896,115	92 (15.9%)	▼-16.0%
Overpayment scams	1,658	$701,729	358 (21.6%)	▼-37.1%
Rebate scams	1,827	$701,250	91 (5.0%)	▲217.8%
Pyramid schemes	406	$286,107	85 (20.9%)	▼-82.9%
Scratchie scams	143	$243,348	14 (9.8%)	▼-42.0%
Psychic & clairvoyant	230	$230,273	90 (39.1%)	▼-49.1%
Mobile premium services	1,523	$141,549	148 (9.7%)	▼-25.0%
Fake charity scams	1,425	$133,214	139 (9.8%)	▼-67.6%
Ransomware & malware	3,885	$74,076	42 (1.1%)	▼-52.7%
Travel prize scams	151	$11,754	17 (11.3%)	▼-96.7%
Other scams	31,449	$382,014	1,213 (3.9%)	▼-17.3%
Total	**216,087**	**$175,684,091**	**22885 (10.6%)**	**▲22.9%**

Reports by numbers

Scam type	Number of reports 2020	Reported losses 2020	Number of reports with loss	Percentage change in number of reports since 2019
Phishing	44,079	$1,689,406	696 (1.6%)	▲75.1%
Threats to life, arrest or other	32,215	$11,833,508	558 (1.7%)	▲140.9%
Identity theft	20,939	$3,072,287	673 (3.2%)	▲84.1%
Online shopping scams	15,306	$7,384,733	8,349 (54.5%)	▲53.8%
False billing	13,120	$18,464,903	1,799 (13.7%)	▲16.6%
Hacking	8,691	$1,419,353	425 (4.9%)	▲4.5%
Remote access scams	8,473	$8,441,632	667 (7.9%)	▼-6.1%
Classified scams	7,928	$5,529,413	2,497 (31.5%)	▲59.9%
Investment scams	7,295	$65,820,313	2,464 (33.8%)	▲45.8%
Unexpected prize & lottery scams	4,543	$1,706,253	298 (6.6%)	▼-52.0%
Ransomware & malware	3,885	$74,076	42 (1.1%)	▼-13.9%
Dating & romance scams	3,708	$38,916,120	1,289 (34.8%)	▼-6.1%
Jobs & employment scams	2,933	$1,268,582	290 (9.9%)	▲17.1%
Rebate scams	1,827	$701,250	91 (5.0%)	▲20.2%
Inheritance scams	1,676	$1,434,544	59 (3.5%)	▼-42.6%
Overpayment scams	1,658	$701,729	358 (21.6%)	▼-7.6%
Mobile premium services	1,523	$141,549	148 (9.7%)	▼-27.7%
Health & medical products	1,459	$3,915,689	382 (26.2%)	▲70.0%
Fake charity scams	1,425	$133,214	139 (9.8%)	▲22.1%
Nigerian scams	577	$896,115	92 (15.9%)	▼-12.7%
Betting & sports investment scams	448	$985,926	150 (33.5%)	▼-10.9%
Pyramid schemes	406	$286,107	85 (20.9%)	▼-31.9%
Psychic & clairvoyant	230	$230,273	90 (39.1%)	▲18.6%
Travel prize scams	151	$11,754	17 (11.3%)	▼-79.3%
Scratchie scams	143	$243,348	14 (9.8%)	▼-81.2%
Other scams	31,449	$382,014	1,213 (3.9%)	▼-10.5%
Total	216,087	$175,684,091	22885 (10.6%)	▲28.8%

Appendix 2: Breakdown of scam reports by state and territory

Australian Capital Territory

Scam type	Reported losses 2020	Number of reports 2020	Number of reports with loss	Percentage change in losses since 2019
Investment scams	$952,351	171	73 (42.7%)	▲157.3%
Dating & romance scams	$547,474	66	28 (42.4%)	▼-52.1%
False billing	$379,526	465	51 (11.0%)	▲322.2%
Threats to life, arrest or other	$252,290	1,367	15 (1.1%)	▼-32.6%
Online shopping scams	$251,718	391	204 (52.2%)	▲285.5%
Classified scams	$227,380	221	58 (26.2%)	▲432.2%
Remote access scams	$173,597	235	16 (6.8%)	▼-8.8%
Inheritance scams	$134,000	46	2 (4.3%)	▲4,835.5%
Phishing	$42,448	1,748	21 (1.2%)	▲26.8%
Overpayment scams	$38,089	52	10 (19.2%)	▼-7.4%
Identity theft	$34,152	673	19 (2.8%)	▲76.3%
Nigerian scams	$15,700	22	4 (18.2%)	▲248.9%
Ransomware & malware	$15,100	113	2 (1.8%)	▲1,577.8%
Hacking	$14,847	208	11 (5.3%)	▼-65.7%
Betting & sports investment scams	$11,000	5	2 (40.0%)	▲55.8%
Jobs & employment scams	$10,450	53	7 (13.2%)	▼-66.5%
Unexpected prize & lottery scams	$9,733	113	5 (4.4%)	▲459.0%
Health & medical products	$2,603	40	12 (30.0%)	▲336.0%
Fake charity scams	$355	70	2 (2.9%)	▼-87.0%
Psychic & clairvoyant	$270	3	2 (66.7%)	▼-94.0%
Pyramid schemes	$60	14	1 (7.1%)	▼-99.6%
Scratchie scams	$0	2	0	▼-100.0%
Mobile premium services	$0	33	0	▼-100.0%
Travel prize scams	$0	2	0	▼-100.0%
Rebate scams	$0	40	0	▼-100.0%
Other scams	$14,760	1,082	43 (4.0%)	▲52.2%
Total	**$3,127,903**	**7,235**	**588 (8.1%)**	**▲13.2%**

New South Wales

Scam type	Reported losses 2020	Number of reports 2020	Number of reports with loss	Percentage change in losses since 2019
Investment scams	$16,257,953	1,993	518 (26.0%)	▲32.6%
Dating & romance scams	$13,367,800	866	317 (12.8%)	▲92.7%
False billing	$3,207,601	3,954	506 (12.8%)	▲43.2%
Threats to life, arrest or other	$2,937,214	9,802	118 (1.2%)	▲392.8%
Remote access scams	$2,759,798	2,399	190 (7.9%)	▲76.1%
Online shopping scams	$2,040,380	4,439	2,373 (53.5%)	▲102.0%
Classified scams	$1,496,858	2,286	673 (29.4%)	▲101.2%
Identity theft	$836,897	6,691	199 (3.0%)	▼-54.5%
Jobs & employment scams	$623,629	612	67 (10.9%)	▲95.5%
Nigerian scams	$433,943	147	17 (11.6%)	▲120.4%
Hacking	$365,739	2,818	133 (4.7%)	▼-80.7%
Inheritance scams	$352,121	386	16 (4.1%)	▼-62.0%
Phishing	$318,675	14,018	190 (1.4%)	▼-0.2%
Unexpected prize & lottery scams	$283,890	1,253	71 (5.7%)	▼-37.3%
Rebate scams	$232,604	521	24 (4.6%)	▲293.7%
Overpayment scams	$175,907	478	92 (19.2%)	▲43.2%
Betting & sports investment scams	$164,800	107	38 (35.5%)	▼-33.2%
Health & medical products	$129,008	506	112 (22.1%)	▲171.4%
Fake charity scams	$63,089	440	39 (8.9%)	▼-38.6%
Pyramid schemes	$57,470	97	17 (17.5%)	▼-92.5%
Mobile premium services	$53,018	462	39 (8.4%)	▼-14.1%
Psychic & clairvoyant	$30,891	43	16 (37.2%)	▼-89.3%
Ransomware & malware	$25,387	1,267	14 (1.1%)	▼-51.9%
Travel prize scams	$2,216	39	5 (12.8%)	▼-93.2%
Scratchie scams	$1,500	47	1 (2.1%)	▼-89.4%
Other scams	$112,290	9,289	350 (3.8%)	▼-8.7%
Total	**$46,330,678**	**64,960**	**6135 (9.4%)**	**▲39.5%**

Northern Territory

Scam type	Reported losses 2020	Number of reports 2020	Number of reports with loss	Percentage change in losses since 2019
Investment scams	$346,379	72	29 (40.3%)	▼-45.7%
Dating & romance scams	$334,468	97	29 (29.9%)	▼-66.8%
Online shopping scams	$52,263	145	82 (56.6%)	▼-28.9%
Threats to life, arrest or other	$42,260	364	11 (3.0%)	▼-66.2%
Classified scams	$29,095	78	21 (26.9%)	▲27.7%
Overpayment scams	$28,263	30	8 (26.7%)	▼-43.5%
Phishing	$18,753	400	10 (2.5%)	▲1,647.7%
Remote access scams	$15,739	54	5 (9.3%)	▼-56.8%
False billing	$12,318	144	17 (11.8%)	▼-64.0%
Identity theft	$8,199	206	7 (3.4%)	▼-88.0%
Psychic & clairvoyant	$7,875	6	2 (33.3%)	▲564.0%
Unexpected prize & lottery scams	$6,532	73	11 (15.1%)	▼-92.7%
Nigerian scams	$6,500	7	1 (14.3%)	▼-74.4%
Jobs & employment scams	$3,936	29	7 (24.1%)	▼-87.0%
Health & medical products	$2,546	13	4 (30.8%)	▲86.2%
Fake charity scams	$2,483	15	6 (40.0%)	▲893.2%
Hacking	$1,756	92	4 (4.3%)	▼-93.1%
Inheritance scams	$750	39	1 (2.6%)	▲275.0%
Pyramid schemes	$725	9	5 (55.6%)	▼-97.0%
Betting & sports investment scams	$617	4	2 (50.0%)	▼-62.6%
Mobile premium services	$200	11	1 (9.1%)	▼-97.6%
Rebate scams	$122	14	1 (7.1%)	▼-79.8%
Ransomware & malware	$0	28	0	▼-100.0%
Travel prize scams	$0	2	0	▼-100.0%
Scratchie scams	$0	5	0	▼-100.0%
Other scams	$7,022	345	22 (6.4%)	▼-3.5%
Total	**$928,801**	**2,282**	**286 (12.5%)**	**▼-60.0%**

Queensland

Scam type	Reported losses 2020	Number of reports 2020	Number of reports with loss	Percentage change in losses since 2019
Investment scams	$10,563,706	1,195	340 (28.5%)	▼-0.4%
Dating & romance scams	$10,128,169	598	242 (40.5%)	▲47.6%
Threats to life, arrest or other	$3,022,345	6,003	118 (2.0%)	▲466.0%
Remote access scams	$1,690,814	1,553	119 (7.7%)	▲220.5%
False billing	$1,440,759	2,651	341 (12.9%)	▼-16.3%
Online shopping scams	$1,426,894	2,543	1375 (54.1%)	▲125.4%
Classified scams	$1,032,608	1,618	426 (26.3%)	▲141.3%
Inheritance scams	$825,462	306	14 (4.6%)	▼-25.2%
Unexpected prize & lottery scams	$518,551	927	58 (6.3%)	▲25.0%
Identity theft	$336,990	3,738	119 (3.2%)	▼-43.9%
Hacking	$319,671	1,637	77 (4.7%)	▼-77.4%
Phishing	$214,872	7,777	116 (1.5%)	▼-9.4%
Betting & sports investment scams	$137,996	83	21 (25.3%)	▼-48.7%
Overpayment scams	$116,438	298	57 (19.1%)	▼-59.2%
Pyramid schemes	$101,456	59	10 (16.9%)	▼-83.1%
Rebate scams	$83,165	345	12 (3.5%)	▲322.1%
Jobs & employment scams	$44,459	361	36 (10.0%)	▼-90.4%
Health & medical products	$28,597	227	76 (33.5%)	▲276.5%
Nigerian scams	$27,003	85	12 (14.1%)	▼-84.6%
Mobile premium services	$18,901	257	32 (12.5%)	▼-9.3%
Psychic & clairvoyant	$16,481	34	15 (44.1%)	▲1,711.1%
Fake charity scams	$13,628	237	24 (10.1%)	▼-90.4%
Ransomware & malware	$4,400	789	5 (0.6%)	▼-86.6%
Travel prize scams	$4,291	33	4 (12.1%)	▲70.8%
Scratchie scams	$3,700	21	4 (19.0%)	▼-96.3%
Other scams	$62,897	5,923	211 (3.6%)	▼-36.8%
Total	**$32,184,253**	**39,298**	**3864 (9.8%)**	**▲17.9%**

South Australia

Scam type	Reported losses 2020	Number of reports 2020	Number of reports with loss	Percentage change in losses since 2019
Investment scams	$3,687,483	397	134 (33.8%)	▲39.4%
Dating & romance scams	$1,628,527	193	83 (43.0%)	▲314.7%
Remote access scams	$414,434	583	54 (9.3%)	▲26.3%
Identity theft	$371,625	1,302	45 (3.5%)	▲62.3%
Classified scams	$370,322	586	162 (27.6%)	▲122.6%
Online shopping scams	$365,899	879	457 (52.0%)	▲58.4%
False billing	$249,643	972	123 (12.7%)	▼-45.9%
Threats to life, arrest or other	$214,797	2,109	22 (1.0%)	▼-30.2%
Phishing	$154,555	2,903	35 (1.2%)	▲83.3%
Rebate scams	$116,980	132	8 (6.1%)	▲391.5%
Hacking	$98,338	590	26 (4.4%)	▼-41.2%
Unexpected prize & lottery scams	$96,981	353	18 (5.1%)	▼-73.5%
Overpayment scams	$51,876	94	19 (20.2%)	▲92.4%
Pyramid schemes	$35,110	20	6 (30.0%)	▼-20.0%
Nigerian scams	$30,620	33	5 (15.2%)	▼-80.9%
Betting & sports investment scams	$24,265	24	5 (20.8%)	▲3,468.4%
Jobs & employment scams	$13,706	101	10 (9.9%)	▼-41.2%
Inheritance scams	$13,000	110	2 (1.8%)	▲6,400.0%
Health & medical products	$7,689	102	29 (28.4%)	▼-16.9%
Fake charity scams	$7,665	113	7 (6.2%)	▼-43.5%
Mobile premium services	$5,865	102	7 (6.9%)	▲109.5%
Ransomware & malware	$3,099	222	2 (0.9%)	▼-53.8%
Travel prize scams	$2,500	15	1 (6.7%)	▲61.0%
Psychic & clairvoyant	$520	4	1 (25.0%)	▼-81.7%
Scratchie scams	$308	19	2 (10.5%)	▼-99.2%
Other scams	$20,261	2,232	71 (3.2%)	▼-31.1%
Total	**$7,986,068**	**14,190**	**1334 (9.4%)**	**▲38.5%**

Tasmania

Scam type	Reported losses 2020	Number of reports 2020	Number of reports with loss	Percentage change in losses since 2019
Investment scams	$538,691	100	34 (34.0%)	▼-53.7%
Dating & romance scams	$448,693	53	19 (35.8%)	▲27.7%
Unexpected prize & lottery scams	$267,715	107	10 (9.3%)	▲1,401.8%
False billing	$236,126	270	38 (14.1%)	▲141.6%
Online shopping scams	$146,952	273	139 (50.9%)	▲182.6%
Threats to life, arrest or other	$119,064	557	7 (1.3%)	▲238.7%
Classified scams	$106,779	177	53 (29.9%)	▲250.3%
Identity theft	$96,526	325	11 (3.4%)	▲101.7%
Remote access scams	$81,519	144	12 (8.3%)	▲12.3%
Hacking	$32,082	129	6 (4.7%)	▲25.5%
Phishing	$18,650	744	12 (1.6%)	▼-0.1%
Overpayment scams	$8,530	33	13 (39.4%)	▲265.8%
Betting & sports investment scams	$6,608	15	4 (56.7%)	▲652.6%
Inheritance scams	$3,000	29	3 (10.3%)	▼-70.0%
Pyramid schemes	$1,700	8	1 (12.5%)	▲142.9%
Health & medical products	$1,540	21	7 (33.3%)	▼-53.6%
Fake charity scams	$1,055	43	6 (14.0%)	▲270.2%
Jobs & employment scams	$695	24	1 (1.2%)	▲100.0%
Nigerian scams	$365	7	2 (28.6%)	▼-75.7%
Rebate scams	$100	34	1 (2.9%)	▲100.0%
Mobile premium services	$30	37	1 (2.7%)	▼-97.5%
Travel prize scams	$0	2	0	▼-100.0%
Ransomware & malware	$0	59	0	N/A
Scratchie scams	$0	1	0	N/A
Psychic & clairvoyant	$0	2	0	N/A
Other scams	$7,168	542	25 (4.6%)	▼-31.6%
Total	**$2,123,588**	**3,736**	**405 (10.8%)**	**▲9.1%**

Victoria

Scam type	Reported losses 2020	Number of reports 2020	Number of reports with loss	Percentage change in losses since 2019
Investment scams	$20,529,439	1,533	463 (30.2%)	▲148.3%
Dating & romance scams	$7,423,008	670	288 (43.0%)	▲153.3%
Threats to life, arrest or other	$4,829,812	9,099	204 (2.2%)	▲178.2%
False billing	$3,003,222	3,198	470 (14.7%)	▲19.4%
Remote access scams	$2,922,226	2,758	211 (47.7%)	▲155.1%
Health & medical products	$2,154,000	296	83 (28.0%)	▲14,256.2%
Online shopping scams	$2,022,630	4,179	2370 (56.7%)	▲95.4%
Classified scams	$1,691,479	2,051	783 (38.2%)	▲112.1%
Identity theft	$979,961	5,927	201 (3.4%)	▲57.0%
Phishing	$687,379	12,010	200 (1.7%)	▲5.7%
Betting & sports investment scams	$602,035	79	27 (34.2%)	▲89.7%
Hacking	$420,060	2,337	118 (5.0%)	▼-63.6%
Unexpected prize & lottery scams	$299,290	1,044	62 (5.9%)	▼-31.8%
Nigerian scams	$287,326	111	21 (18.9%)	▲24.8%
Rebate scams	$254,037	553	35 (6.3%)	▲426.6%
Scratchie scams	$237,840	35	7 (20.0%)	▲1,707.8%
Overpayment scams	$212,791	407	94 (23.1%)	▼-23.3%
Jobs & employment scams	$141,035	550	73 (13.3%)	▼-33.0%
Psychic & clairvoyant	$111,939	44	25 (56.8%)	▲288.4%
Inheritance scams	$86,770	313	7 (2.2%)	▲538.0%
Mobile premium services	$38,683	460	39 (8.5%)	▲15.8%
Fake charity scams	$33,934	309	25 (8.1%)	▼-46.3%
Ransomware & malware	$16,066	977	10 (1.0%)	▲36.4%
Pyramid schemes	$14,136	78	16 (20.5%)	▼-80.2%
Travel prize scams	$2,515	35	5 (14.3%)	▼-95.9%
Other scams	$94,903	8,372	278 (3.3%)	▼-6.6%
Total	**$49,096,516**	**57,425**	**6115 (10.6%)**	**▲115.4%**

Western Australia

Scam type	Reported losses 2020	Number of reports	Number of reports with loss	Percentage change in losses since 2019
Investment scams	$4,786,110	600	195 (32.5%)	▼-34.7%
Dating & romance scams	$2,052,689	308	109 (35.4%)	▼-18.7%
False billing	$915,063	1,251	173 (13.8%)	▲79.2%
Online shopping scams	$463,323	1,329	655 (49.3%)	▲28.5%
Classified scams	$380,271	698	221 (31.7%)	▲52.8%
Remote access scams	$346,917	637	40 (6.3%)	▼-3.4%
Threats to life, arrest or other	$250,438	2,767	41 (1.5%)	▼-31.2%
Jobs & employment scams	$242,933	848	15 (1.8%)	▲118.7%
Unexpected prize & lottery scams	$202,402	419	35 (8.4%)	▼-17.3%
Phishing	$192,987	3,991	67 (1.7%)	▲104.9%
Hacking	$147,663	717	29 (4.0%)	▼-58.1%
Identity theft	$114,314	1,822	51 (2.8%)	▼-65.5%
Pyramid schemes	$49,850	30	6 (20.0%)	▼-37.0%
Overpayment scams	$39,105	154	25 (16.2%)	▼-52.8%
Betting & sports investment scams	$20,712	45	5 (11.1%)	▼-63.2%
Mobile premium services	$19,575	125	15 (12.0%)	▼-39.7%
Psychic & clairvoyant	$10,959	17	4 (23.5%)	▲100.0%
Health & medical products	$8,772	173	34 (19.7%)	▲71.1%
Ransomware & malware	$7,488	370	5 (1.4%)	▲100.0%
Nigerian scams	$7,350	39	2 (5.1%)	▼-74.1%
Inheritance scams	$5,000	161	2 (1.5%)	▼-95.5%
Fake charity scams	$4,072	101	12 (11.9%)	▼-86.1%
Rebate scams	$3,638	160	4 (2.5%)	▼-4.3%
Travel prize scams	$98	18	1 (5.6%)	▼-98.2%
Scratchie scams	$0	13	0	▼-100.0%
Other scams	$36,199	3,044	107 (3.5%)	▼-22.9%
Total	**$10,307,928**	**19,837**	**1853 (9.3%)**	**▼-22.5%**

Appendix 3: Scam reports from businesses

Scam type	Reported losses 2020	Number of reports 2020	Number of reports with loss	Percentage change in losses since 2019
False billing	$13,509,327	917	201 (21.9%)	▲468.4%
Health & medical products	$2,053,745	39	5 (12.8%)	▲48.2%
Investment scams	$1,674,473	84	23 (27.4%)	▲407.8%
Online shopping scams	$496,947	227	88 (38.8%)	▲67.1%
Classified scams	$200,911	214	49 (22.9%)	▼-0.5%
Jobs & employment scams	$181,632	76	11 (14.5%)	▼-8.4%
Identity theft	$57,121	278	22 (7.9%)	▼-60.7%
Threats to life, arrest or other	$56,440	142	2 (1.4%)	▼-46.0%
Phishing	$52,057	689	21 (3.0%)	▼-36.9%
Hacking	$26,902	229	8 (3.5%)	▼-41.0%
Overpayment scams	$23,212	88	6 (6.8%)	▼-27.9%
Rebate scams	$20,532	25	2 (8.0%)	▲23.1%
Remote access scams	$10,300	160	2 (1.3%)	▲2.8%
Mobile premium services	$10,200	21	2 (9.5%)	▲11.9%
Ransomware & malware	$4,000	95	1 (1.1%)	▲100.0%
Fake charity scams	$3,641	92	11 (12.0%)	▲100.0%
Dating & romance scams	$3,452	10	1 (10.0%)	▲100.0%
Nigerian scams	$240	32	1 (3.1%)	▲100.0%
Pyramid schemes	$106	5	1 (20.0%)	▲100.0%
Betting & sports investment scams	$0	4	0	N/A
Inheritance scams	$0	41	0	N/A
Psychic & clairvoyant	$0	2	0	N/A
Scratchie scams	$0	1	0	N/A
Travel prize scams	$0	1	0	▼-100.0%
Unexpected prize & lottery scams	$0	18	0	N/A
Other scams	$15,925	694	37 (5.3%)	▲35.7%
Total	**$18,401,163**	**4,184**	**494 (11.8%)**	**▲249.4%**

Appendix 4: 2020 Scams media releases

Media release	Date published
Romance scammers move to new apps	9-Feb-20
Gen Z the fastest growing victims of scams	10-Mar-20
Warning on COVID-19 scams	20-Mar-20
Scammers targeting superannuation in COVID-19 crisis	6-Apr-20
Don't get scammed looking for a lockdown puppy	18-May-20
Scams cost Australians over $630 million	22-Jun-20
Business email compromise scams cost Australians $132 million	23-Jun-20
Scams target all sections of Australian society including CALD and Indigenous communities	25-Jun-20
Government impersonation scams on the rise	21-Jul-20
National Scams Awareness Week: 'This Is Not Your Life'	17-Aug-20
Rental scams targeting more Australians during pandemic	21-Sep-20
Threat based scams targeting young people and Chinese community	26-Oct-20
Watch out for online shopping scams this holiday season	24-Nov-20

Appendix 5: Support resources

If you are the victim of a scam, or know someone who is the victim of a scam, the following free resources can aid in recovering mentally and financially.

There is information about how you can protect yourself from scams in the future on the Scamwatch website. We also encourage you to report scams.

Identity theft

IDCARE is a free service that will work with you to develop a specific response plan to your situation and support you through the process. Visit the IDCARE website or call 1300 IDCARE (432273).

Commonwealth Victims' Certificate – a certificate that helps support your claim that you have been the victim of identity crime and can be used to help re-establish your credentials with government or financial institutions. Visit Commonwealth identity crime.

Support and counselling services

Lifeline Saving Lives Crisis Support. Suicide Prevention.	When you need support in a crisis, contact **Lifeline** on 13 11 14 (24/7) or visit https://www.lifeline.org.au/
beyondblue	For information about depression or anxiety, contact **beyondblue** on 1300 22 4636 or visit www.beyondblue.org.au
SUICIDE CALL BACK SERVICE free telephone counselling	Free professional telephone and online counselling for anyone affected by suicide. Suicide **Call Back Service**: 1300 659 467
Kids Helpline	Telephone and online counselling and support service for young people aged between 5 and 25 years. **Kids Helpline**: 1800 55 1800
Talk it over Mens Line AUSTRALIA	Telephone and online support, information and referral service for men with family and relationship concerns. **MensLine Australia**: 1300 78 99 78

Financial assistance/complaints

Scams can be financially devastating, but there is free help and counselling available. You can visit the National Debt Helpline website or speak to a counsellor for free financial counselling on 1800 007 007 for consumers or 1800 413 828 for small businesses.

The Australian Financial Complaints Authority (AFCA) independently assists consumers and small businesses to make and resolve complaints about financial firms. If you have sent money to a scammer via your financial firm and have been unsatisfied with their response, you can make a complaint to the AFCA.

Specific government organisations

Certain scams are within the jurisdiction of particular government agencies and they can often provide specialist assistance, such as temporarily adding additional protective measures to your account or assisting in removing image based abuse from social media.

- Report Centrelink, Medicare, Child Support and myGov related scams to the Services Australia Scams and Identity Theft Helpdesk by calling 1800 941 126
- Report image based abuse (sextortion), cyberbullying and illegal content to the Office of the eSafety Commissioner
- Report tax related scams to the Australian Taxation Office
- Report cybercrime to the Australian Cyber Security Centre via ReportCyber
- Report financial and investment scams to the Australian Securities and Investments Commission
- Report fraud and theft to your local police by calling 131 444 or the number of your local police station in Victoria.

For tips about online safety and security and an Australian Government directory for where to get help see the Be safe Be alert online quick reference guide.

Glossary

Scam terms

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

Please refer to payment redirection scams below.

Celebrity endorsement scams

Scammers use the image, name and personal characteristics of a well-known person to sell a fake product or service. Often, scammers also write fake news articles about celebrities claiming that they have endorsed a product or investment.

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.

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 and they are increasingly introducing investment scams. They cause devastating emotional and financial damage.

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 such as, for example, the 2020 bushfires and the COVID-19 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.

Government impersonation scams

In addition to impersonating the ATO, scammers often pose as myGov or other government agencies in order to phish for personal information. For instance, scammers sent phishing text messages and emails purporting to be from a government agency about COVID-19 throughout the pandemic.

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 scams.

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 guarantee to make fast money or a high-paying job for little effort.

Migration scams

Scammers impersonate Australian migration agents, either in their home countries or in Australia, and steal applicants' personal information and money.

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 text message 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 for which they have purportedly been charged too much money. The victim later discovers the scammer never paid the initial amount in the first place.

Payment redirection scams

Note these scams are sometimes referred to as business email compromise scams

These scams involve targeted phishing and hacking of a business. Scammers commonly send emails to the business' 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.

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.

Puppy scams

Scammers create a fake website claiming to sell in-demand dog breeds. During the COVID-19 pandemic, buyers were unable to see the dogs in person prior to purchase. Once a victim purchases a puppy, the scammer will continue to demand additional money for things such as transport, vaccinations, grooming, insurance and other costs relating to the dog.

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, 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.

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.

Romance baiting

A scam involving a combination of a dating and romance scam with an investment scam. The scammer initially contacts a victim via a dating app, then quickly moves the conversation to an encrypted chat site. After a few weeks of developing a relationship, the scammer will begin asking about the victim's finances and encourage them to participate in an investment opportunity.

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.

Superannuation scams

During COVID-19, scammers attempted to take advantage of people in financial hardship by attempting to steal their superannuation or by offering unnecessary financial services and charging a fee.

Threats to life, arrest or other/threat based scams

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 making threats against them if they do not cooperate. Chinese authority scams are an example of this type of scam, as are sextortion scams in which scammers threaten to release embarrassing photos of victims to their email 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.

Wangiri scams

A scammer calls from an overseas number and hangs up after one ring. Calling back the number results in premium charges for the caller and scammers will try to keep callers on the phone as long as possible, for example by playing hold music.

Payment methods

Australia Post Load & Go pre-paid debit cards

A pre-paid, gift card style Mastercard debit card. Load & Go cards have now been discontinued but were used in a number of scams throughout 2020.

Bitcoin

Bitcoin is a type of cryptocurrency (see below) that is commonly used by scammers.

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.

Ukash

Ukash was an electronic money system that allowed users to exchange their cash for a secure code to make payments online. It has been acquired by Skrill Group (see above).

WorldRemit

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

AUSTRALIAN COMPETITION
& CONSUMER COMMISSION