AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

Targeting scams

Report of the ACCC on scams activity 2021

July 2022

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

ACCC 06/22_22-40 www.accc.gov.au

Foreword

This report is the 13th annual Targeting Scams report and the final report I will be involved with in my role as Deputy Chair. It outlines the range of scams that have continued to impact Australians in 2021, and the enormous efforts by government, law enforcement, the private sector and community to combat scams.

Scam losses grow to over $2 billion

In 2021 we continued to see record levels of scam activity in Australia. Nearly $1.8 billion in losses were reported to Scamwatch, ReportCyber, 12 financial organisations and other government agencies. When we take into account the fact that around one third of scam victims don't report to anyone, it is clear that the real loss figure is well over $2 billion. We also know that the true cost of scams is far more than just financial – it leads to emotional stress and can have life changing consequences for many individuals, families, and businesses.

The largest combined losses in 2021 were:

- $701 million lost to investment scams
- $227 million lost to payment redirection scams
- $142 million lost to romance scams.

The most frequently complained about scams to Scamwatch in 2021 were:

- phishing & identity theft scams with over 93,000 complaints
- threats to life, arrest or other with over 32,000 complaints
- false billing with over 21,000 complaints
- online shopping scams with over 20,000 complaints.

As only about 13% of victims report to Scamwatch, it is clear that these numbers vastly understate the extent of these scams.

In 2021 scams have sadly continued to cause harm to people in all sections of the community. Worryingly, some of the more vulnerable members of the community are reporting increasingly high losses. Indigenous Australians, older Australians, people from culturally and linguistically diverse communities and people with disability are losing far more than ever before. As a community we need to focus more effort on disrupting & preventing scams both by stopping scammers connecting with potential victims in the first place as well as stopping money reaching scammers.

Urgent work is needed to combat cryptocurrency investment scams

The popularity and hype of cryptocurrency has led to a surge in losses to investment scams with combined losses to investment scams of $701 million. At the same time, it is also becoming the preferred method of payment across all types of scams.

Cryptocurrency has been described as the wild west with many countries now seeking to regulate aspects of it. In March 2022, the Australian government began consultation on approaches for licencing digital currency exchanges and custody requirements for crypto assets. While ongoing I am hopeful that this and other regulatory measures will slow the growth of cryptocurrency scams in Australia. It is also pleasing to see Google taking steps to address scammers exploiting their platform with the recent announcement that it will make changes to its advertising policy and require advertisers wanting to promote financial services in Australia to complete a verification process and demonstrate that they are licensed by ASIC. That said, there is still more work that needs to be done to prevent scams across all digital platforms.

Telecommunications industry making progress but more needs to be done

It is fantastic seeing the results of the important work undertaken by the ACMA, telecommunications industry and other agencies to combat scams. The Reducing Scam Calls Code has led to a reduction in phone scam reports to the ACCC of almost 50% in 2022. While SMS scams have filled the gap, the industry is currently finalising the expansion of the Code to place obligations on telcos to monitor and block scam SMS. Similarly, new rules have commenced to require better identification for high-risk telco transactions. We hope to see the results of these initiatives in 2022 and 2023.

Working together

This work shows that when regulators and industry work together and share information effective disruption can achieve results. We hope to see more examples in other sectors, including the banking sector, in the coming year as it is clear more work across all parts of the economy will be required if we are to truly get on top of the problem. Just one example of a change that would have an impact, especially on payment redirection scams where over $220 million was lost in 2021, is introduction of confirmation of payees by banks. There is, sadly, no case to relax our efforts as we are in the equivalent of an arms race with scammers constantly finding new ways to get around disruption efforts.

Final words

I want to finish by thanking the millions of people who have made reports to Scamwatch over the years and shared their stories to help others or to stop scammers. Without these reports all the good work that has occurred could not have been done. We know that most people are unable to recover the money lost but the experiences that are shared assist us across all the work we do.

I also want to thank the Scamwatch team, especially Jayde Richmond, and other ACCC staff who over the years have worked tirelessly on our scams prevention and disruption work. I'd also like to especially thank the team at IDCARE who do so much to help the victims of scams. In addition I'd like to thank the staff across other government agencies, the police, the private sector, the media, consumer advocates, financial and other counsellors, and our international counterparts. While this is my last Targeting Scams report I look forward to seeing the good work continue.

It is only through our combined efforts that we can make a real difference to this enduring problem. By sharing information, collaborating to increase awareness of scams, innovating to disrupt scammers and fixing the systems or processes that scammers seek to exploit we can make Australia a harder target for scammers, prevent loss especially to the vulnerable and improve the outcomes of those who have experienced harm from scams.

Delia Rickard
Deputy Chair, ACCC

Contents

Targeting scams 2021

Losses

$2+ billion*

Total combined losses reported to Scamwatch, ReportCyber, 12 financial institutions and government agencies

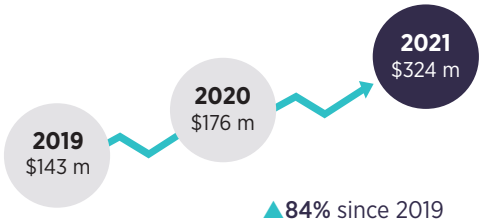
$324 million ▲84%

Amount reported lost to Scamwatch

286,622 ▲33%

reports to Scamwatch

216,087 reports in 2020



▲**84%** since 2019

Average loss: $12,742

Top 3 scams causing the most financial harm to Australians in 2021

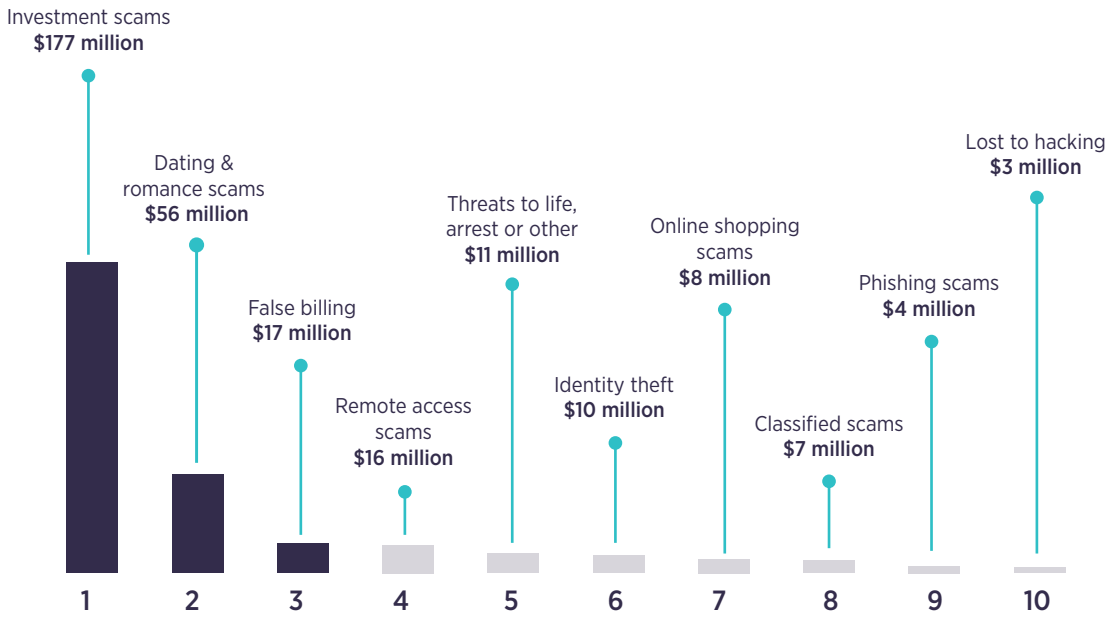
$701 million
combined losses to investment scams

$227 million
lost to payment redirection scams

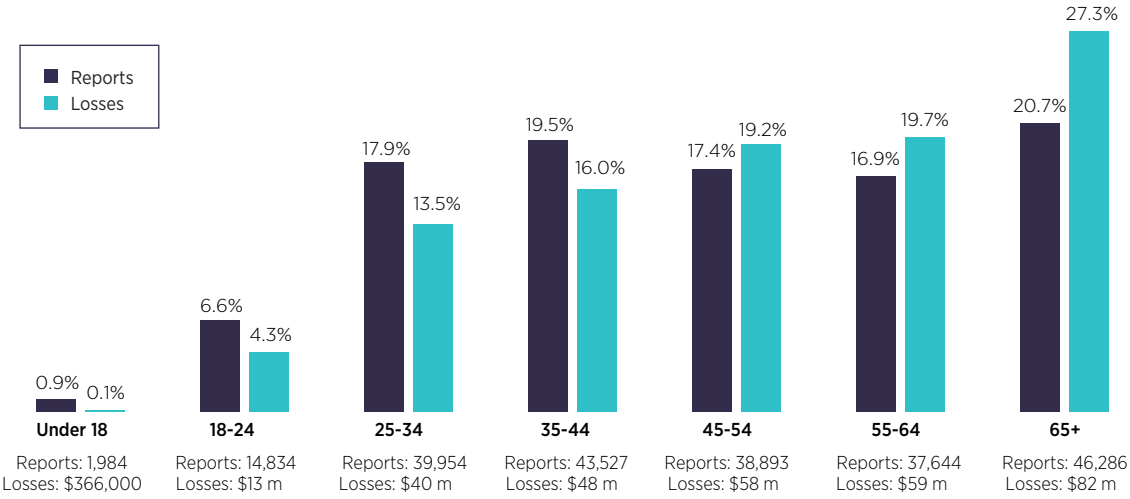
$142 million
combined losses to romance scams

* Research shows that a third of scam victims do not report so the true cost is well over $2 billion.

Top scams by loss as reported to Scamwatch



Age



Gender

Male
$190 million
138,591 reports
59% of losses

Female
$131 million
142,092 reports
40% of losses

Non-specified
$2 million
5,939 reports
1% of losses

Top contact methods by reports

50%
Phone
144,603 reports
$100 million reported lost

23%
Text message
67,180 reports
$10 million reported lost

14%
Email
40,186 reports
$48 million reported lost

4%
Internet
12,502 reports
$51 million reported lost

4%
Social networking/ online forums
10,140 reports
$56 million reported lost

The role of Scamwatch

Scamwatch (www.scamwatch.gov.au) 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, law enforcement and the private sector to disrupt and prevent scams.

The ACCC outlines its approach to scams each year in its Compliance and Enforcement Policy. In 2022, the policy[1] states:

> The ACCC, government agencies and the private sector work together to prevent Australians from falling victim to scams. The ACCC does this by:
>
> - analysing data collected through Scamwatch to identify trends, monitor financial losses, and inform our scam prevention strategies
> - informing the public about current and emerging scams through our Scamwatch website, social media and engagement work
> - partnering with government and the private sector to reduce scam opportunities by enhancing consumer protections and disrupting scam activity through the use of telecommunication services, financial services, and other technology services including digital platforms.

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.

1 ACCC Compliance and Enforcement Policy and Priorities, 2022 https://www.accc.gov.au/about-us/australian-competition-consumer-commission/compliance-enforcement-policy-and-priorities.

Notes on data in this report

The data in this report is from the calendar year 1 January to 31 December 2021. All case studies are adjusted to protect the privacy of reporters.

Except where specified, all data is based on phone and web reports made to Scamwatch. Scamwatch data may be adjusted throughout the year because of quality assurance or changes to categories. While effort is made to verify high loss reports, reports are unverified.

Reference to combined reports or losses include data from Scamwatch, ReportCyber, other government agencies and financial institutions. 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.

This report contains data extracted from ReportCyber an online reporting portal for cybercrimes administered by the Australian Cyber Security Centre (ACSC) which is based within the Australian Signals Directorate (ASD).[2] The ACSC triages reports and refers some to the appropriate law enforcement jurisdiction for investigation.

We thank all 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), HSBC Bank Australia Limited (HSBC), ING Group (ING), MoneyGram International (MoneyGram) and The Western Union Company (Western Union) all contributed data to this report.

2 https://www.cyber.gov.au/acsc/report.

1. Scam activity in 2021

1.1 Key statistics 2021

- Scamwatch, ReportCyber, other government agencies, banks and money remitters received a combined total of over **566,648 reports**, with reported losses of almost **$1.8 billion** in 2021. One third of victims do not report scams[3], so actual losses were well over **$2 billion**.
- Investment scams caused the most financial loss, with combined losses of **$701 million**. This was followed by payment redirection[4] with **$227 million** lost, and romance scams with **$142 million** lost.
- Only 13% of victims report to to Scamwatch. In 2021, Scamwatch received **286,622 reports**, a 33% increase from the 216,087 reports received in 2020.
- Financial losses reported to Scamwatch totalled more than **$323 million** in 2021. This is an increase of 84% compared to the $175 million in losses reported in 2020.
- Investment scams and romance scams continued to cause the most financial loss. $177 million was reported lost to investment scams and $56 million to romance scams.
- Scamwatch received the most reports about phishing scams (71,308 reports). This was a 62% increase on the number of these reports in 2020 (44,079 reports), which was a 183% increase on the number of reports in 2019 (25,168 reports).
- 25,407 (9%) of people reported a financial loss to Scamwatch for an **average loss of $12,742**. 73,613 people (26%) reported loss of personal information.
- Research commissioned by the ACCC in 2021 found that 96% of people have been exposed to a scam in the last 5 years with half of these contacted weekly or daily by scammers.
- 30% of victims do not report the scam to anyone.

1.2 The contact and payment methods

- **Phone** (voice) continued to be the most common contact method reported to Scamwatch in 2021 with **144,603 reports** (50% of all reports). $100 million was reported lost to phone scams which represents 31% and was the highest loss contact method.
- Text message was the second most common contact method with 67,180 reports up by 107% from 2020.
- The second highest contact method in terms of loss was **social media**[5] with $56 million lost (17% of total losses).
- **Bank transfer** continued to be the most common payment method for scams with **$129 million** reported lost, up 32% compared to the $97 million reported in 2020.
- More scammers are seeking payment with **cryptocurrency** and losses to this payment method increased 216% to **$84 million**.[6]

3 See section 2.2 for more details about the ACCC's commissioned research on unreported scam activity.

4 Payment redirection scams are often referred to by government and law enforcement as business email compromise. $227 million refers to business email a compromise as well as some other scams.

5 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 forum'.

6 In 2021 the category for cryptocurrency was only 'Bitcoin'. The 'other payment' method also includes some cryptocurrency reports so the figure is likely higher. 'Other payments' total $67 million. In March 2022 the category 'Bitcoin' was changed to cryptocurrency.

1.3 The people who have lost money

- People **aged 65 and over** made the most reports (46,286) to Scamwatch and lost more money than any other age group with almost **$82 million** reported lost. Losses increased with age.
- Losses reported by **men** increased 116% from $87.9 million in 2020 to more than **$190 million** in 2021. Women reported a 50% increase in losses from $87.3 million in 2020 to more than $131 million in 2021.
- Men reported losing twice as much money to investment scams than women (Men lost $118.4 million and women lost $58.1 million). Men reported losing money to romance scams more often than women, but women lost more in total to these scams than men (women lost $32 million and men lost $24 million).
- People from **New South Wales** made the most reports (92,118) and lost the most money with $110 million in reported losses. People in the **Australian Capital Territory** lost more money to scams on a per capita basis.
- Scamwatch received 4,958 reports from **Indigenous**[7] reporters with **$4.8 million** reported lost. This represents a 43% increase in reports and 142% increase in losses. Younger Indigenous people lost more money compared to older people which was a different trend from the total reports.
- Indigenous people in Queensland lost the most money with $2.4 million reported lost.
- People from culturally and linguistically diverse (CALD) communities made 14,060 reports and lost **$42 million** which was an 88% increase compared to 2020. The median loss for people from CALD communities was higher than for the overall median across all reporters ($1,200 vs $845). Scams over mobile apps resulted in the most losses for CALD communities largely due to the Hope Business app scams.
- Scamwatch received 15,387 reports from **people with disability** with more than **$19.6 million** in losses. This was almost double the reports and losses reported in 2020.

1.4 The businesses which have lost money

- **Payment redirection** (business email compromise) is the scam that caused the highest losses to businesses with combined losses of **$227 million** in 2021. Businesses reported more of these scams to ReportCyber and the banks.
- Financial loss reported to Scamwatch by **businesses** fell by 27% in 2021, to **$13.4 million** from $18.4 million in 2020. The number of reports made by businesses fell by 13% to 3,624.
- Businesses reported the most losses to **false billing scams** (which includes many payment redirection reports) with $6.7 million reported lost and investment scams with $5.1 million lost.
- **Small businesses** had the highest median loss of $3,812 and lost a total of $3.5 million.

1.5 The scams

Investment scams

- Combined losses to investment scams in 2021 climbed 135% to **$701 million**.
- **Scamwatch** received over 9,600 reports about investment scams with $177 million lost and made up 55% of the total losses reported in 2021.
- The main driver of the increase was **cryptocurrency investment** scams which increased in losses by 270% in 2021. Scamwatch received 4,730 cryptocurrency investment scams with **$99 million** in reported losses.
- Scamwatch received 221 reports about **imposter bond scams** with **$16 million** in reported losses.

7 The Scamwatch webform does not specify Indigenous 'Australian' therefore some reports are received from people who are Indigenous in other countries.

- **Ponzi scams** and pyramid schemes increased in 2021. Scamwatch received over 2,000 reports with almost **$8 million** in losses, an increase of 368% compared to 2020. Many of these scams impacted younger people and those from CALD communities.
- The ACCC received 231 reports about 'Hope Business' and 'Wonderful World', app scams that were spread on Facebook and WhatsApp.

Flubot scam

- In August 2021, Australians began receiving text messages concerning missed packages and voicemails escalating into the **largest scam text message campaign** in Australia's history.
- From 2 August–31 December Scamwatch received **26,496 reports** about Flubot text messages with $10,743 in reported losses. Many more people may have experienced indirect loss from compromise of their personal information.

Remote access scams

- Combined losses to remote access scams were **$112 million** in 2021.
- Scamwatch received over 15,600 reports about remote access scams with a 94% increase in losses to over **$16 million** in 2021.
- Scammers adapted their methodology to frighten victims into downloading remote access software and set up accounts on cryptocurrency exchanges. They also moved to SMS as well as phone for initial contact.
- These scams continued to impact older Australians more than others with those aged 65 and over losing the most money ($8 million).

The continued impact of COVID-19

- Scam reports that mentioned COVID-19 fell in 2021 with 4,283 reports received and $8.6 million in reported losses.
- Reports to Scamwatch about **Government impersonation scams** fell 25% to 18,000 but losses increased 31% to over **$2 million**.
- Scamwatch received over 1,500 reports related to COVID-19 **vaccinations**. 277 of these mentioned rapid antigen tests with **$60,000** in reported losses.
- Reports about **pet scams** increased by 48% to 3,332 in 2021 with over **$4 million** reported lost. The majority of these related to puppies and kittens.

Agriculture scams

- Australian farmers and small businesses lost over **$1.5 million** to scammers targeting the agriculture industry in 2021.
- The most common scam was fake online sales for heavy machinery/tractors. Scamwatch received 313 reports about the sale of **tractors** and agricultural machinery with $1.4 million lost.

1.6 The fight against scams

- In 2021, the ACCC increased its work with other government agencies, law enforcement (in Australia and overseas) to share intelligence, disrupt scams and raise awareness in the community.
- The ACCC collaborated with other agencies, the Australian Cyber Security Centre, the Australian Federal Police and the major banks and telecommunications providers to combat the **Flubot SMS scam**. An international effort including with the Australian Federal Police led to a Europol operation disrupting the Flubot infrastructure rendering the strain of malware inactive in June 2022.
- The ACCC worked with the Department of Home Affairs and state and territory licensing authorities to make it more difficult for criminals to use lost or stolen driver licences and less challenging for victims to recover from **identity crime**.

- The ACCC continued its work with other government agencies and the telecommunications industry on the Australian Communication and Media Authority (ACMA) led **Scams Telecommunications Action Taskforce**. Key outcomes in 2021 include:
  - the new *Reducing Scam Calls Industry Code* and the increased use of call blocking to disrupt phone scammers with over **357 million scam calls blocked** in the first year
  - a significant reduction in mobile porting scams following the introduction of the *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020*
  - ongoing development of measures to prevent sim swap fraud and improve identity verification for all high-risk transactions in the telco sector
  - work on measures to require telcos to monitor and block malicious scam SMS messages.
- Scamwatch shared thousands of telephone numbers provided in scam reports with the telcos and the ACMA every week to assist them to identify scam call traffic and disrupt scammers.
- The ACCC continued to work with the financial sector to share information about scams. In 2021 Scamwatch expanded its information sharing through the Australian Financial Crimes Exchange which supports the banks to identify scams, scammer accounts and block transactions.
- In 2021, the banks and financial institutions that provided data for this report told the ACCC that they prevented or recovered more than $340 million from being sent to scammers and **refunded more than $102 million** to customers who were the victims of scams.
- The ACCC met regularly with payment system providers, finance and banking industry bodies, banks, ASIC, the AFCA and others in the financial sector to share scam trends, learn about initiatives to prevent scams, and encourage initiatives to reduce the losses to scams in Australia.
- The ACCC continued to monitor initiatives overseas and advocate for more scam prevention measures in the financial system, including the United Kingdom's requirements for **Confirmation of Payee** in the *Authorised Push Payment Scams Contingent Reimbursement Model Code*.
- In 2021, Scamwatch in collaboration with NBN Co, worked with **TeamViewer** to significantly reduce the number of **remote access scams** using TeamViewer software to scam victims. TeamViewer introduced technical solutions and worked with a number of banks to successfully reduce remote access scams using that platform.
- The ACCC continued to advocate for **digital platforms** to take more action to address scams. In March 2022, the ACCC commenced proceedings in the Federal Court against **Facebook owner Meta Platforms Inc** and Meta Platforms Ireland Limited alleging that they engaged in false, misleading or deceptive conduct by publishing scam advertisements featuring prominent Australian figures.
- In 2021, the ACCC recognised the increase in vulnerable people reporting financial loss or identity compromise to Scamwatch and provided more tailored referrals for vulnerable scams victims to **support services**, including **IDCARE**.
- The ACCC continued to expand its sharing of Scamwatch data with the private sector including for example the following businesses in 2021: Gumtree, Facebook, Seek, MoneyGram, LinkedIn, NBNCo, Autotrader, Coinspot, Afterpay, Amazon and Microsoft.
- The ACCC commenced sharing scammer intelligence in Scamwatch reports with the **US Federal Trade Commission** for sharing across 32 countries through the Consumer Sentinel Network.
- Scamwatch provided more than **150 disseminations** of scam reports on high risk or current scam trends to law enforcement and government. This intelligence assisted state and federal police to investigate and, in some instances, prosecute scammers. Police were able investigate, charge and/or arrest individuals involved in money muling rings; roofing scams; puppy scams; identity theft; investment scams and phone scams impersonating law enforcement or banks.
- Scamwatch provided Flubot URLs to the Australian Cyber Security Centre to facilitate website removal requests on 18 occasions.
- From 8–12 November the ACCC led the Scams Awareness Week campaign which was supported by over **350 partner organisations**. The campaign encouraged the public to Stop Scams. Speak Up and reached an estimated **15 million people**.

- By the end of 2021, Scamwatch had **127,972 subscribers** to its email alert service and published **9 media releases** warning the public about scams.
- The Scamwatch website had over **8 million page views** in 2021, and the ACCC's **Little Black Book of Scams** was viewed 21,910 times and downloaded 12,391 times. We distributed **91,413 hard copies**.
- In 2021 the **Scamwatch Twitter** account (@Scamwatch_gov_au) posted 261 tweets and by the end of 2021 had a following of over **35,000**.
- In June 2021, the ACCC released its 2020 Targeting Scams report which was viewed 7,507 times and downloaded 5,222 times.
- In 2021 there was an increase in demand for information about scams and trends. The ACCC responded to hundreds of media requests. 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.
- The ACCC's Indigenous outreach teams visited Bagot Community, Belyuen Community, Knuckey Lagoon and Palmerston Indigenous village in 2021, where among other things staff provided information and responded to concerns about scams.
- Scamwatch staff presented at many forums in 2021 including, but not limited to:
  - Multicultural Australia
  - ASEAN consumer affairs program webinar
  - ATO CALD community leader network
  - QPS Gold Coast cross cultural liaison unit
  - Police ethnic advisory group
  - Australian Prudential regulation association
  - ACSC partnership network
  - UNSW Canberra cyber
  - National Disability Insurance Agency
  - Canterbury Bankstown city council
  - Australian Financial Industry Association
  - Global Online Scams Summit
  - Victoria Teachers Association
  - Department of Health
  - AusPost
  - Lendlease
  - AMP
  - National Australia Bank (podcast)
  - Dept of Education Skills & Employment (podcast).
- Examples of working groups and networks Scamwatch participated in 2021:
  - Counter Fraud Reference group – Cth Fraud Prevention Centre
  - Cyber Security & Safety Communications Working group(Home Affairs led)
  - GASA International law enforcement working group
  - CJLEF
  - Operation Ashiba (AFP led)
  - ReportCyber Project Board
  - Consumer Education Network
  - Disability Royal Commission
  - Interdepartmental Committee – National Plan to Combat Cybercrime
  - Scams Telecommunications Action Taskforce (ACMA led)
  - Inter Regulator Fraud Group (ASIC led)
  - Scams Awareness Network (ACCC led)

- Online harms industry and international engagement working group
- Home affairs cyber security outreach network
- Fintel Alliance
- IDCARE working Group (Home affairs led)
- NICS
- RoundTable on remote access scams with Teamviewer, banks and telcos.

2. Scam activity in 2021

2.1 Combined data – the bigger picture

To better understand the impact of scam activity in Australia, the ACCC obtained scam data from 12 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 2021 was almost $1.8 billion across **566,648 reports**. Taking into account the level of unreported scam activity, the ACCC estimates the actual level of financial loss to be well **over $2 billion**. Scamwatch received the largest number of reports.

Table 2.1 Losses reported to all agencies and banks

Agency/organisation	Reports	Losses
Scamwatch	286,622	$324m
ReportCyber	62,349	$766m
12 banks & money remitters	146,198	$499m
ATO	50,684	$800,000
Services Australia	7,674	N/A
WA ScamNet	2,526	$14m
ACMA	16,494	N/A
ASIC	3,866	$291m
AFCA	3,257	N/A
Adjustments for duplications*	-13,022	- $131m
Total	**566,648**	**$1.76 billion**

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

The combined loss data highlights the scams that caused the most financial harm to Australians in 2021. The highest loss category was investment scams with $701 million lost. This was followed by $227 million lost to payment redirection (business email compromise). Romance scams and remote access scams also caused significant losses.

Table 2.2 Combined losses by category reported to all agencies and banks

Scam type	Scamwatch	ReportCyber	Bank losses	ASIC	Adjusted Total[8]
Investment scams	$177m	$306m	$219m	$58m	$701m
Payment redirection	$13m	$94m	$121m	N/A	$227m
Romance scams	$56m	$51m	$48m	$7m	$142m
Remote access scams	$16m	$12m	$106m	N/A	$112m

2.2 The impact of scams and unreported scam activity

ACCC research

In 2021 the ACCC commissioned research[9] to better understand the impact of scams and level of unreported scam activity. The research highlighted that exposure to scams is almost ubiquitous. The research findings related to 2 key areas: people who encountered scams (both victims and also

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

9 1,508 surveys were completed online using the Roy Morgan Consumer Panel. The data was weighted to represent the Australian population aged 18 years or older.

non-victims who recognised avoided the scams) as well as people who were victims of scams. Key findings of the research included:

- 96% of respondents were contacted or exposed to scammers in the last 5 years. Half of these were contacted weekly or daily.
- 20% of people were a victim of a scam in the past 5 years; one third of these were a victim more than once.
- 56% of victims did not recover any money lost.
- 43% of victims lost their identity or personal information.
- 30% of victims did not report it to anyone.
- Of those victims who did not report, 40% did not report because they thought nothing could be done.

Scamwatch was the most common government reporting service where **victims** reported a scam. In terms of scam victims:

- 37% reported to a bank
- 16% reported to police
- 13% reported to Scamwatch.

The research also found that people who spoke a language other than English and low-income earners ($50k or less) were more likely to be a victim of a scam than others.

Men were more likely to lose larger amounts of money when scammed and women were more likely to lose their identity or personal information when scammed.

When including all of those respondents who **encountered**[10] a scam (both victims and non-victims), 63% of people discussed it with friends or family. 68% did not report the scam to a government or law enforcement agency. The most common places victims and non-victims reported included:

- 11% reported to a bank
- 7% to Scamwatch
- 4% to police
- 4% to social media platforms/website.

The main reasons people gave for reporting scams was to stop scammers (52%), inform authorities (46%) and help others (46%).

The research also assisted in helping identify what is effective in helping prevent people falling for scams. The survey asked participants to identify why they were able to avoid falling for scams they encountered with 49% of people responding that they had seen warnings about the scam. Participants also identified where they sourced their information about scams:

- 45% from the media
- 39% from the Internet
- 14% from Scamwatch.gov.au.

This research highlights the importance of continuing to increase initiatives that raise awareness and educate the public to prevent scams.

10 This will include all people who encountered or were exposed to a scam – victims and non-victims.

Other research

The ACCC's research is consistent with research findings by the ACMA in 2021[11] which found that in the 6 months before the survey, 98% of Australians received some form of unsolicited communication with the majority being calls phone calls (97%). Scams were the most common type of unsolicited communication (92%). 40% of people experienced scam calls weekly.

Similarly, the Australian Banking Association published[12] data in 2021 that showed that 37% of Australians lost money to a scam or knew a close friend or family that had. 66% of Australians fend off a scam every week and 29% every day. 92% of Australian adults had been exposed to a scam or fraud in the past year.

2.3 Scamwatch statistics in 2021

The ACCC received 286,622 scam reports in 2021, with reported losses of $324 million. Reports increased by 33% compared to 2020, and financial losses increased by 84%.

Table 2.3 Losses and number of reports by category

Scam category	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in losses since 2020
Investment scams	$177,184,295	9,664	4,068 (42.1%)	169.2%
Dating & romance scams	$56,175,428	3,424	1,379 (40.3%)	44.4%
False billing	$17,303,665	21,545	1,881 (8.7%)	-6.3%
Remote access scams	$16,412,258	15,698	1,330 (8.5%)	94.4%
Threats to life, arrest or other	$11,077,551	32,426	658 (2.0%)	-6.4%
Identity theft	$10,159,930	22,354	951 (4.3%)	230.7%
Online shopping scams	$8,074,469	20,694	7,436 (35.9%)	9.3%
Classified scams	$7,114,830	9,561	3,080 (32.2%)	28.7%
Phishing	$4,324,128	71,308	861 (1.2%)	156.0%
Hacking	$3,041,484	15,141	547 (3.6%)	114.3%
Jobs & employment scams	$2,697,500	3,453	308 (8.9%)	112.6%
Travel, prizes and lottery scams*	$1,984,215	4,976	322 (6.5%)	1.0%
Pyramid Schemes	$1,341,389	487	215 (44.1%)	368.8%
Ransomware & malware	$1,172,034	3,623	54 (1.5%)	1,482.2%
Rebate scams	$1,145,112	2,046	132 (6.5%)	63.3%
Betting & sports investment scams	$976,214	328	125 (38.1%)	-1.0%
Inheritance and unexpected money*	$923,256	1,831	150 (8.2%)	-60.0%
Overpayment scams	$841,060	2,027	315 (15.5%)	19.9%
Other scams	$690,788	40,970	1,018 (2.5%)	80.8%
Health & medical products	$372,014	1,588	289 (18.2%)	-90.5%
Psychic & clairvoyant	$358,501	187	89 (47.6%)	55.7%
Fake charity scams	$188,457	835	101 (12.1%)	41.5%
Mobile premium services	$165,139	2,456	102 (4.2%)	16.7%
Grand Total	**$323,723,717**	**286,622**	**25,411 (8.9%)**	**84.3%**

* Note: Scamwatch data and categories may change from time to time. Highlighted categories were combined in 2021 and data is a combination of previous categories which consistently received very small numbers of reports.

11 ACMA, Unsolicited communications in Australia: Consumer experience research 2021 (Jan 2022) interactive report https://app.powerbi.comview?r=eyJrIjoiNDgyMGI4OTEtMDE2My00N2YxLWI4OGYtZjI3OTBiNTgwNDEyIiwidCI6IjBkYWM3ZjM5LWQyMGMtNGU3MS04YWYzLTcxZWU3ZTI2OGEyYiJ9.

12 https://www.ausbanking.org.au/aba-launches-new-awareness-campaign-as-scams-grow/.

The 3 scams with the highest reported losses in 2021 were investment scams, romance scams and false billing scams.

The 3 most reported scam categories were phishing scams, threats to life, arrest or other, and identity theft.

Contact methods

Phone call, text message and email were the top 3 ways scammers contacted Australians in 2021.

Phone continued to be the most common way scammers contact victims. Reports about phone scams increased 40% to over 144,000 with the most reported being phishing (31,026) and threats to life arrest or other (30,636). Losses to phone scams increased by 108% to over $100 million due to high losses to investment scams and remote access scams where contact was initiated by phone.

Text message scam reports increased by 108% to over 67,000 largely due to Flubot text messages which emerged in August 2021 and resulted in over 13,000 reports about scam text messages that month. Losses to scams via text message also increased 227% to $10 million. The highest losses for text scams came from investment scams, romance scams and ransomware and malware.

Scammers continued to use **social media platforms** to contact people with 10,140 reports and $56 million lost, an increase in losses of 107%. The most reported scam on social media was online shopping with 2,381 reports. The highest losses were to investment scams ($27 million) and romance scams ($23 million). Losses also increased significantly for identity theft and jobs and employment scams over social media.

Table 2.4 Contact mode reports and losses in 2020 and 2021

Contact Mode	2020 Reports	2021 Reports	Percentage change in number of reports	Reported losses 2020	Reported losses 2021	Percentage change in reported losses
Phone	103,153	144,603	40%	$48m	$100m	108%
Text Message	32,337	67,180	108%	$3m	$10m	227%
Email	47,503	40,186	-15%	$35m	$48m	37%
Internet	13,636	12,502	-8%	$27m	$52m	94%
Social Networking	9,687	10,140	5%	$27m	$56m	107%
Mobile Apps	4,348	6,544	51%	$22m	$36m	67%
Mail	2,625	2,218	-16%	2m	$2m	2%
In Person	1,814	1,773	-2%	$11m	$18m	62%
Fax	109	54	-50%	$52,428	$8,182	-84%
Not provided	875	1,422	63%	$63,372	$278,300	339%

Payment methods

In 2021, the highest reported losses were via bank transfers, Bitcoin (cryptocurrency) and other payments. The ‘other payments’ category includes cryptocurrencies aside from Bitcoin such as USDT and Ethereum, as well as charges to phone bills, Afterpay, Payeer, digital payment apps such as GCash and even goods and items sent but not paid for by scammers.

Table 2.5 Payment methods, reports, and losses by highest loss

Payment method	Reports	Losses	Percentage change in reported losses
Bank	10,315	$129m	32%
Bitcoin/cryptocurrency[13]	3,021	$84m	217%
Other payment /cryptocurrency	3,203	$66m	175%
Cash	1,144	$14m	62%
Credit Card	5,315	$9m	7%
Money remitters[14]	402	$6m	59%
Other gift cards[15]	1,270	$4m	135%
PayPal	2,189	$3m	62%
Google Wallet	77	$1m	N/A
iTunes gift card	303	$872,000	2%
Aus Post Load & Go prepaid debit	71	$105,000	-57%
Payment method not provided	259,312	$7m	N/A

2.4 Data from the financial sector

Scamwatch data shows that most scam transactions were undertaken via bank transfer. Each year we obtain data from a range of financial institutions and money remitters to identify the level of scam activity reported to them and the amount lost. We know from our research that the most common place a victim will report a scam is to their bank, so this data helps us to understand the bigger picture. We also share information with financial institutions to disrupt scams and raise awareness.

The scams that caused the highest losses as reported to banks is consistent with Scamwatch and other scam data. Investment scams caused the most significant loss in 2021 with $219 million reported lost. What is clear from the data is that banks received more reports about remote access scams and much higher losses than were reported to Scamwatch, with 24,983 reports and $106 million reported lost.

Table 2.6 Highest loss scams in 2021 reported to Banks & Money Remitters

Scam type	Reports	Losses
Investment scams	16,903	$219m
Payment redirection & other	98,484	$121m
Remote access scams	24,983	$106m
Romance scams	5,828	$48m

In 2021, financial institutions told the ACCC that they prevented or recovered nearly $341 million from scammers. In addition, they also refunded almost $103 million to customers who were victims of scams.

All banks, payment platforms and financial institutions 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.

13 In March 2022 the ACCC changed the category from Bitcoin to cryptocurrency.

14 World Remit, Western Union, MoneyGram, Money Transfer, and UKASH/Skrill.

15 Includes Google Play, Steam, supermarket gift cards and Amazon gift cards.

Case study: Payment redirection in property settlement $440,000 lost

Sophia purchased an investment property. She contacted her solicitor who sent her an email from the correct email address, in fact it was part of an email chain sent from them with details of the bank account and BSB to transfer the funds through for settlement.

Sophia proceeded to do one of 3 transfers through 3 different banks. The first was one of $90,000 through her account with Big4BankA and the other of $350,000 through her Big4BankB account. Both were processed without issue. The third transfer was through her mid-tier bank. The mid-tier bank did not proceed, they detected an issue and called Sophia, they told her to ask the solicitor to verify the payee account details. Sophia called and the solicitor told her that the details from the email were the incorrect. Sophia immediately contacted her Big4 banks who both launched investigations.

Australian Financial Crimes Exchange

The Australian Financial Crimes Exchange (AFCX) is an independent, non-profit that brings together businesses, government, law enforcement agencies and industry groups to protect Australian consumers and businesses from financial and cybercrime in Australia. It provides the security capabilities technology and intelligence in a central platform.

In 2021, the AFCX collected data from 7 participating financial institutions which found that $635 million was exposed to scam activity across 71,000 transactions. Consistent with Scamwatch, investment, remote access and romance scams dominated 2021 and made up 80% of the amount lost by victims. Cryptocurrency became a significant enabler of scams and the AFCX saw increases in the number and value of scams. Remote access scams made up the highest number of transactions and second highest in terms of value. Investment scams was the lowest in terms of transactions but highest in terms of value.

Australian Financial Complaints Authority

The Australian Financial Complaints Authority (AFCA) is a non-government organisation providing free, fair, and independent help with financial disputes. Their role is to assist consumers and small businesses to reach agreements with financial firms about how to resolve their complaints. AFCA receives a wide variety of complaints involving scams including investment, romance, invoice hacking, telecommunications, and Australian Government agency scams (such as those purporting to involve the police or the tax office). If consumers are not satisfied with the response from the bank or financial firm to a scam report or claim, they can lodge a complaint with AFCA.

AFCA commenced reporting on scams data in October 2020. Since then, AFCA saw scam complaints increase each year. Most scam complaints resolve directly between financial firms and complainants without case management. For complaints that do not resolve directly, the majority resolve early in case management with AFCA's involvement to negotiate and conciliate outcomes acceptable to both parties. A small percentage progress to investigation where AFCA has issued a preliminary assessment or final decision.[16]

In 2021, 5% (3,257 complaints) of AFCA's 68,950 complaints related to scams. The monthly average scam complaints received in 2021 was 271 cases, an increase of 16% from the monthly average in 2020 (233 cases). 98% of complaints were closed in 2021, and 13% of complaints was in favour of the complainant. Over $13 million was compensated.

The banks

All banks reported an increase in scam activity in 2021. The ANZ reported a 47% increase in scam losses with remote access and investment scams driving the increases. This was a consistent trend across the banks. Similarly, Macquarie Bank saw double the cases of investment scams and the value of attempts was 5 times more than the previous year. Suncorp reported about 100 scam cases per month on

16 AFCA decisions are available at: https://www.afca.org.au/what-to-expect/search-published-decisions.

average and highlighted a 50% increase in monthly cases of remote access scams and the movement of these scams to devices like phones and tablets. HSBC and Macquarie noted a higher number of lower dollar value scams with purchase and buy/sell scams on Facebook marketplace and Gumtree as well as puppy scams prominent.

The most consistent trend related to investment scams and the growth of cryptocurrency investment scams. This was identified as a key driver in increasing losses.

Westpac highlighted the Hope Business pyramid scams with large numbers of small value victims causing large case volumes. Similarly, the Commonwealth Bank noted that Hope Business scams (such as Wonderful World, Starlike) affected several thousand CBA customers. The ANZ also continued to deal with the ramifications of the Hope Business App noting the volume of victims and money movement made it a challenging issue for banks. The banks noted close work with the ACCC's Scamwatch in responding to these.

The ANZ undertook several investigations into imposter bond scams where criminal syndicates would impersonate legitimate investment firms and offer unsuspecting consumers opportunities to invest. The minimum buy-in for investors were often above $100,000. In most cases the quality of paperwork and websites supporting the scam were of a very high quality and were difficult for customers to identify as a scam. The scammers would contact via cold call from offshore call centres. Recipient accounts were generally held with Australian banks with the criminals' moving funds to digital wallets and disbursing the proceeds elsewhere making recoveries difficult.

2.5 Data from government agencies and law enforcement

ReportCyber – reports to law enforcement

In Australia, victims of cybercrime can report the incident to ReportCyber, a portal administered by the Australian Cyber Security Centre and overseen by the Australian Signals Directorate. Reports are triaged and referred or made available to police jurisdictions in the states and territories and the Australian Federal Police.

ReportCyber covers cyber abuse, online fraud, online image abuse, identity theft, cyber security incidents, and ransomware or malware.

In 2021, ReportCyber received 62,349 scam reports, with $766 million in losses. This was an increase of 7% in reports and 126% in reported losses compared to 2020. The highest losses were to investment scams, with losses over $306 million. $94 million was reported lost to payment redirection scams.

Australian Securities and Investments Commission – investment scams

The Australian Securities and Investment Commission (ASIC) is Australia's corporate, markets and financial services regulator. It receives reports of misconduct (misconduct reports) from members of the public, their representatives (like lawyers, accountants and other advisors) and other stakeholders. Misconduct reports are used to identify areas of regulatory concern in the industries that ASIC regulates.

Some misconduct reports are scams with the intention of fraudulently obtaining money and information (like identity details) from victims. In 2021, ASIC received 3,866 scam reports[17], with reported losses of $291 million.[18] The top 3 categories by case were investment scams, cryptocurrency scams, and unlicensed conduct.[19] The top 3 categories by losses were unlicensed conduct, investment scams, and cryptocurrency scams. People aged between 35 to 44 reported the most cases (19%), while the 45 to 54 age group reported the most losses (32%).

17 In 2021 41% of reports were from Australian residents and 20% from overseas residents. The overseas nature of victims and scammers can limit action available to regulators such as ASIC.

18 The reported loss amount has not been confirmed or otherwise verified by ASIC.

19 Members of the public may report scammers as people operating without a financial license.

Close to 1,600 reports involved cryptocurrency[20], this was 41% of total scam cases. The reported losses were over $48 million. Many cryptocurrencies are not financial products under law. Because of this, many cryptocurrencies and the platforms where consumers buy and sell cryptocurrency may not be regulated by ASIC and consumers are unlikely to have protections if the platform fails or is hacked. When a cryptocurrency or cryptocurrency platform fails, investors will most likely lose all the money they put in. In most countries, cryptocurrencies are not recognised as legal tender. People are only protected to the extent that they fit within existing laws.[21]

Australian Communications and Media Authority – phone scams

The Australian Communications and Media Authority (ACMA) regulates communications and media to maximise economic and social benefits of communications infrastructure, services, and content for Australia.

In 2021, the ACMA received more than 57,000 complaints about telemarketing and spam. 34% of telemarketing complaints and 20% of spam complaints (29% overall) were categorised as scam complaints. From August 2021, about 58% of spam scam complaints related to Flubot messages.

Australian Taxation Office

The Australian Taxation Office (ATO) is the Australian Government's principal revenue collection agency. It manages and shapes the tax, excise and superannuation systems in Australia. In 2021, the ATO received 50,684 scam reports. Of those, 147 victims lost just over $800,000 to scammers. This was a 47% decrease in reports and a 34% decrease in the number of clients who paid scammers (34%) from 2020.

The ATO saw a different trend to Scamwatch with people aged between 18 and 24 losing the most money to tax scams.[22] The ATO saw a 48% increase to nearly $130,000 in payments via gift cards for use in Australian stores with young people paying the most.

The ATO also observed several concerning new scam trends in 2021:

- A rise in people losing money to automated phone scams about suspended tax file numbers due to illegal activity.
- Scammers calling and emailing people pretending to be financial advisers and superannuation experts. Scammers encouraged people to invest in a high performing self-managed super fund so they could harvest personal information and steal their superannuation savings.
- In early 2021 scammers emailed people to update their myGov or myGovID details via a fake myGov logon page designed to steal personal information, including passport and drivers licence details.
- During tax time there was a rise in people losing money to scams through different payment methods such as Cardless cash, Coles/Myer, Kmart and JB-Hifi gift cards, courier services who collect cash payments and in-person cash delivery payments.
- There was a resurgence of an ATO Impersonation email scam, advising people they were due to receive a refund. The email contained an attachment that enticed people to enter their personal information and financial details into a fraudulent website to receive their 'refund'.

20 This analysis is based on a Key Term of Cryptocurrency attached to cases that involve such products. While the case involves cryptocurrency, the scam category may be different, such as Investment scams.

21 https://moneysmart.gov.au/investment-warnings/cryptocurrencies.

22 In 2021 18–24 year olds made 14,384 reports to Scamwatch with almost $13 million lost. This was the age group with the lowest reports and losses.

Case study: 2021 ATO – In person payment methods

In 2021 the ATO observed scammers demanding money through new payment methods, including courier services collecting cash payments directly from scam victims and cash deliveries made in person at a pre-determined public location.

The new methods suggested that scammers were using local money mules to collect funds in Australia and highlighted a personal safety risk for victims.

The ATO saw one scammer lure a young woman out of lockdown in New South Wales to drop off $30,000 in cash at a local hardware store. The scammer claimed to be from the 'federal police', and told the woman her tax file number was compromised and threatened her with arrest. The victim had sent photocopies of her driver's licence and Medicare card to the scammer before reporting the scammer to the ATO and the police.

Another report came from a Victorian man who paid $50,000 to someone who collected the cash from his front door. The scammer demanded personal details such as his tax file number, address and name over the phone before the home visit and 'guaranteed' the victim would get his money back if he paid upfront.

The ATO issued an urgent community warning, asking anyone who had paid a scammer through one of the above methods to report it to police and contact their financial institution immediately.

Services Australia

Services Australia delivers government payments and services. Like the ATO, it is often impersonated in scams and receives reports from the public about scams.

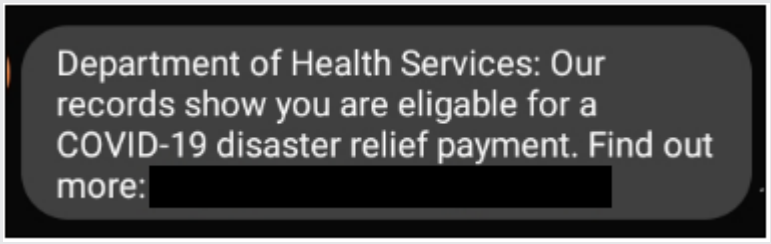
In 2021, Services Australia's scams and identity theft Helpdesk received 7,674 scam reports, which was a 34% decrease from the 11,553 reported in 2020. 680 victims reported a financial loss in 2021. Those aged 65 or older made the most reports.

During 2021, Services Australia referred 238 unique government impersonation scams for investigation, monitoring or disruption efforts. This included scams via phone, SMS, email and platforms such as Facebook:

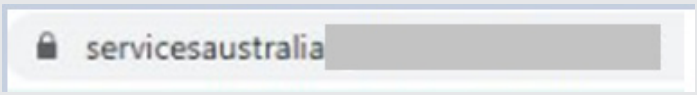
- 229 of these scams contained a myGov theme or referenced myGov.
- The majority (214) were phishing emails. These typically directed people to a fake myGov site built to capture financial and personal identity information.

Case study: Service Australia COVID Vax Payment

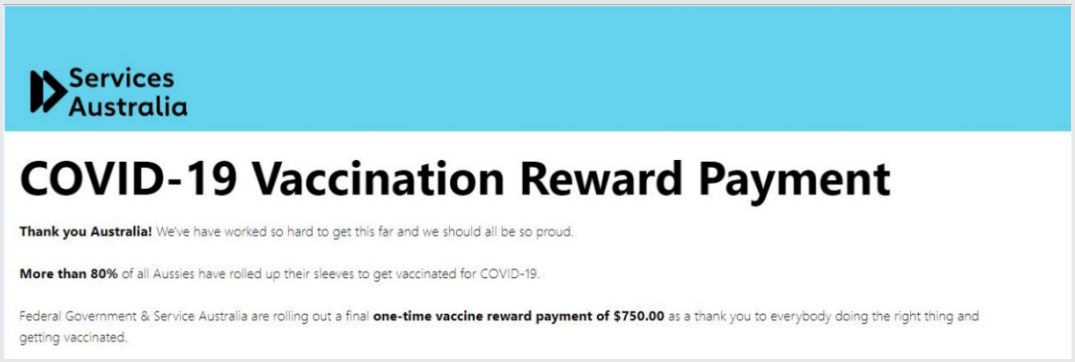
COVID-19 was an attractive theme for scam activity. In October 2021, Services Australia was alerted to an SMS scam targeting the vaccinated. The message stated that the recipient was eligible for a COVID-19 disaster relief payment:



Recipients who clicked on the link were directed to a sophisticated fake Services Australia website:



The methodology highlighted careful planning by malicious actors. Timed to coincide with local events, the landing page read:



The wording 'one-time' payment and the amount of $750 were carefully selected to align with the economic response payments administered by Services Australia at the start of the pandemic:

Services Australia continued to see iterations of this scam which demonstrates how scammers evolve to the current ever-changing environment to take advantage of struggling Australians.

Western Australian Government – ScamNet

WA ScamNet[23] is run by the Western Australian Department of Mines, Industry Regulation and Safety.

In 2021 it received 2,526 scam reports, with reported losses of over $14 million.

23 https://www.scamnet.wa.gov.au/scamnet/Home.htm.

IDCARE

IDCARE support members of the community across Australia and New Zealand who have concerns about their identity or related cyber security.

In 2021, IDCARE received 129,139 contacts (this is up 22% from 2020). Around 1 in 5 of these clients were referred by Commonwealth agencies, including Scamwatch, as cases impacting Commonwealth legislation, programs and/or offence categories. The costs of supporting these Commonwealth-referred clients were covered under the Commonwealth agreement with IDCARE.

IDCARE identified the following trends in reports in 2021:

- Phone was the most prominent method channel of scam activity (representing 78% of known compromise channels, versus around 11% SMS and 10% email).
- Around 58% of the people who engaged with IDCARE experienced further identity or account misuse following an initial scam or compromise event.
- Telstra, Amazon and the NBN were the 3 most impersonated brands reported.
- Where social engineering was used by scammers, such as knowing the victim's name or date of birth, the time taken to detect the scam was more than 3 times longer than scammers not using these techniques.

IDCARE highlighted the financial and psychological impacts to victims of scams and identity compromise in 2021, including the following:

- The average value of losses to scam events reported was $25,751.
- At the time of engaging IDCARE victims indicated that only 6% of these funds were recovered.
- The highest losses on average were relationship scam victims ($73,799 per event) and investment fraud victims ($64,681 per event).
- Approximately 26% of individuals who experience a scam and were registered with IDCARE's specialised case managers presented with symptoms of depression, anxiety or stress (DAS-scale)[24] as a result of experiencing these crimes.

24 Depression and Anxiety Stress Scale – a 42 item self-report instrument designed to measure the 3 related negative emotional states of depression, anxiety and tension/stress.

3. Scamwatch trends in 2021

3.1 Investment scams

Combined losses to investment scams in 2021 were over **$701 million**. Scamwatch received over 9,600 reports about investment scams with over **$177 million** in losses – a 32% increase in reports and an almost 170% increase in losses compared with 2020.

Investment scams made up 55% of the total losses reported to Scamwatch in 2021.

Cryptocurrency scams

The main driver of the increase in investment scams were cryptocurrency investment scams which increased in losses by 270% in 2021. In 2021 Scamwatch received 4,730 cryptocurrency investment scams with **$99 million** in reported losses.

These scams generally involve scammers setting up fake investment and cryptocurrency trading platforms, sometimes impersonating legitimate, well-known websites, to steal money from people looking to invest in cryptocurrency. Some lured people into buying a fake crypto wallet or tricked them into giving away their seed phrase for an existing wallet. Others offered to assist people unfamiliar with cryptocurrency by remote accessing their computer or device to set them up on a cryptocurrency platform and then steal their money.

Losses to cryptocurrency investment scams were high across almost all age groups with those aged 65 and over losing the most money ($26.5 million) closely followed by the 45–54 age group with $19.6 million lost. Most of these scams occurred following contact via phone or social media or involved a website (internet).

Imposter bond scams

Scamwatch observed an increase in reports about imposter bond scams in 2021 with a spike in November. Scamwatch received 221 reports with almost $16 million reported lost as scammers impersonated legitimate companies and sold fake high yield corporate or government bonds.

Bonds are an investment option designed to generate regular income for the investor. The buyer gives the bond issuer (corporation or government) a loan, and is paid back the principle over time, plus regular payments of interest. Generally, longer-term bonds produce higher yields for the investor. Buying and selling bonds quickly usually results in lower yields.

Scammers often promised high yields for short term investments and directed investors to send money to a bank account that would be managed on their behalf. In many cases, reporters noted they were contacted after submitting queries on investment comparison websites and felt pressured into investing.

Ponzi schemes and related scams

In 2021 there was a 20% increase in reports to Scamwatch and 368% increase in losses relating to pyramid and ponzi schemes, largely due to ponzi investment scam apps. Scamwatch received over 2,000 reports with almost $8 million in losses to these scams. This includes over 1,100 jobs & employment scams, 490 investment scams and 436 reports of pyramid schemes.

Ponzi schemes use funds collected from new investors to pay existing investors. No real investment exists, and these schemes inevitably collapse.

Unlike other investment scams these scams impacted younger people more than older people with the highest losses in the 25–34 age group. Most of the losses resulted from contact over social media followed by mobile apps.

Scam apps like Hope Business and Wonderful World drove a surge in reports about Ponzi schemes throughout 2021. Users were told they could make commissions if they recruited their friends to download the apps too. Apps like Hope Business were marketed to people to make extra money while doing easy work from home. They were told the more people they recruited, the more commission they would make.

Case study: Wonderful World scam – $60,000 lost

Rudra received a random message from Jenny and then talked regularly over WhatsApp. They became good friends and Jenny suggested Rudra earn commission through a company called Wonderful World. Rudra created an account and started earning commission. When he tried to withdraw the money, it failed. Jenny told him to withdraw small amounts of $100. Then Jenny asked him to put in more money to increase his level in the pyramid to qualify for a higher withdrawal limit. So, Rudra topped it up with $60,000. After this Rudra was then unable to withdraw any and customer care via his WhatsApp started giving him excuses. Rudra noticed the company was de-registering from ASIC and realised he had lost all his money.

When a new user first signed up, they would see a commission growing in their account. But when they tried to withdraw their money, they would be blocked from doing so. Once many people invested in the scheme, the scammers disappeared with the money.

Victims were often recruited into these schemes via the internet or chat sites, and by friends and family members who genuinely believed it was a good investment opportunity. Pyramid and Ponzi schemes disproportionately impacted people from culturally and linguistically diverse backgrounds, with almost 20% of reports and over 35% of losses in 2021 coming from people with English as a second language.

Ponzi scheme case study – Hope Business App

The Hope Business app was launched around May 2021. The app was a scam, and took 'investments' from users and claimed they would be paid dividends if they completed tasks or games within the app.

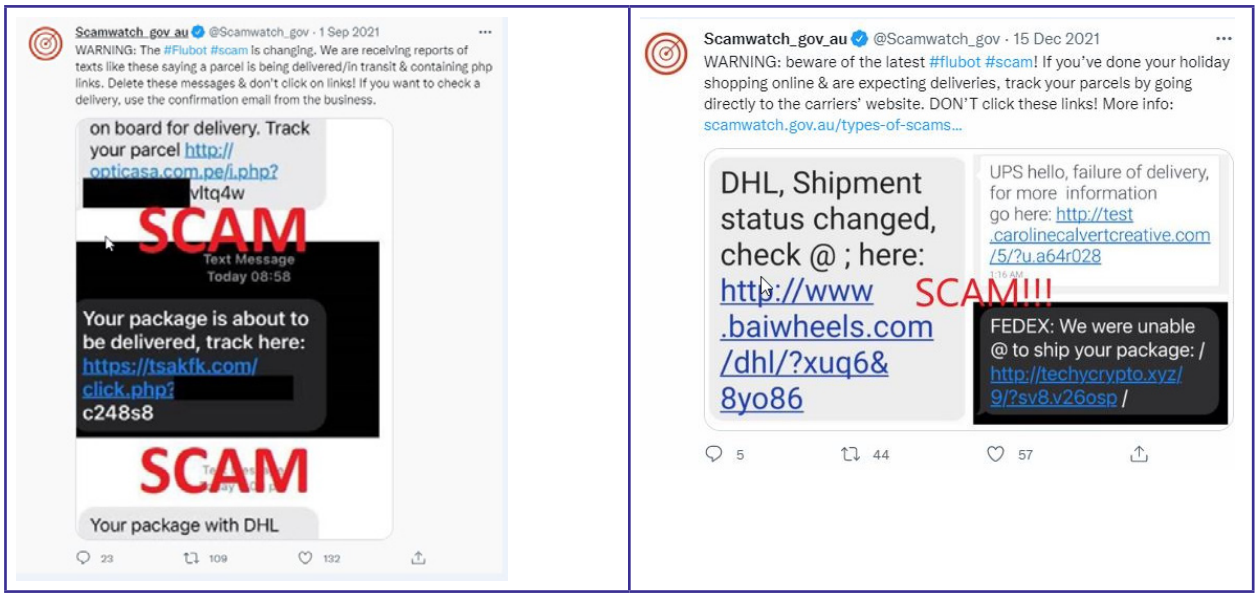
Users were initially able to withdraw funds. They were encouraged to recruit their family and friends to the app, but were later blocked from withdrawing their money.

After receiving reports of around $400,000 in losses to the Hope Business app, the ACCC warned consumers and alerted Google and Apple. Hope Business was quickly removed from app stores. The ACCC also shared information about this scam with banks in Australia. The police are continuing to investigate the app, and victims continue to try to recover money.

3.2 Flubot SMS scam – largest SMS scam in Australia

Scamwatch was one of the first agencies to identity the emergence of the Flubot scam in Australia after receiving reports from 2 August 2021. Many Australians received scam text messages about missed calls or deliveries. Scamwatch received almost 26,500 reports about Flubot text messages between August and December 2021. Many people lost personal information and $10,743 was reported in direct financial loss.

Flubot is a form of malware that operates on Android phones through a malicious link. It is hidden through an SMS message that the user opens leading to a chain of similar messages to people on the person's contact list to potentially put others at risk. The malware can harvest the contact list to spread to other devices. It can not only infect the device but access personal information and banking data. People who received the text message and gave permissions would have their contact lists added to the list of phone numbers used to distribute Flubot. Flubot messages were then sent to randomly selected numbers on the list. The infection also attempted to steal banking credentials by inserting 'overlays' when users attempt to login to key Australian sites such as banks.



Government, law enforcement and the private sector worked together to combat this scam. An international effort including with the Australian Federal Police resulted in a Europol operation disrupting the Flubot infrastructure rendering the strain of malware inactive in June 2022.[25]

Case study: Flubot scam

'I got a call from a lady who had received the link from my phone and thought I was the scammer and told me that she was going to report my phone number to the police as me being the hacker.'

I was contacted by the scammer through a text message that provided a link to track my package online. I clicked on the link that appeared to downloaded the DHL mobile express app on my phone. It asked for a couple of permissions to access my phone and then I could not get the app to open. I tried to delete the app but could not. I rebooted my phone back to factory settings but even after that I received multiple calls from people that had been getting the same text message with the link on their phone. I got the text message from other numbers as well. I called CrimeStoppers and they told me to report this to Scamwatch and contact my telco for help.

3.3 Remote Access scams

Remote access scams continued to increase in 2021. Total combined losses to remote access scams were **$112 million**. Scamwatch received over 15,600 reports about remote access scams, an 85% increase on 2020, with over $16 million in losses, almost double the losses from the previous year.

In nearly all instances of remote access contact was first initiated by phone.

25 https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones.

Case study: Remote access scam – $400,000 lost

Melanie had been having issues with NBN broadband at her house. During this time Melanie received a call from a scammer called Sean claiming to be an NBN security employee. Sean told Melanie to install some software on the computer to stop her bank accounts being hacked and said she needed to convert the money to cryptocurrency. Melanie had experienced an issue with credit card compromise a few weeks earlier. Under Sean's guidance Melanie created a series of accounts with cryptocurrency exchanges, Coinspot and Blockchain. Sean accessed Melanie's private email and was able to pass the verification steps on cryptocurrency transactions and used the email address to impersonate Melanie. Two transactions of $200,000 each were processed with funds transferred through the cryptocurrency exchanges and then the funds disappeared.

Older Australians tend to be more impacted by remote access scams. People aged 65 and over lost the most money (almost $8 million) and made the most reports. People under 55 are less like to lose money to these scams.

Case study: Remote access and threats – $40,000 lost

Myrtle, aged 89 years old received a phone call from David advising that she was entitled to a $400 rebate. David asked Myrtle for bank account details to credit the money. David continued to call Myrtle and told her they had incorrectly paid a rebate of $40,000 which she had to repay immediately or the ATO and government would chase her up and take all assets and the house. The scammers then emailed a hyperlink through which they took control of Myrtle's home computer. Instructions were sent to her printer for telegraphic transfer to an overseas bank. Myrtle was scared and sent money, she lost $40,000. David and the scammers continued to call Myrtle every day until her children realised and reported the scam to the police and the bank.

Scammers also tried different methods such as initiating remote access via SMS. Victims received a text message from a scammer posing as their bank or an online platform such as Amazon or PayPal, advising that their account had been charged for a purchase. The text message prompted the victim to call a number if they wanted to dispute the charge. Once on the phone, the scammer would send one-time-pin codes to the victim's phone, and ask the victim to read them out, to 'authorise' the refund. These codes would either give the scammer access to the victim's online accounts or authorise transactions from their bank account or credit card. Scammers would sometimes repeat this process 4 or 5 times with the same victim, until the victim noticed money coming out of their account and realised they were being scammed.

Case study: Remote access via SMS – over $4,500 lost

Max received a text message confirming a purchase of an expensive camera from his Amazon account, with a number to call if he wanted to dispute the transaction. Max had not purchased anything, so he called the number and spoke to someone who claimed to be from Amazon. The scammer said that in order to cancel the purchase of the camera, he was going to send Max another text message containing a 6 digit number and told Max to read the number back to him. Max felt that something might be off. He checked his bank account and saw there had been another amount taken out. Later that night, he received a notification that his Amazon password had been changed and received an email confirming the purchase of an expensive laptop from his account.

Max reported the issue to Amazon and his bank, and realised that the 6 digit code he had given to the scammer was his Amazon one-time-password. This allowed the scammer to gain access to Max's account and spend money using his bank account.

3.4 Continuing impacts of COVID-19

In 2021, scammers continued to use the COVD-19 pandemic to perpetrate scams. Scamwatch received 4,283 reports that mentioned COVID-19 and $8.6m in reported losses.

Government impersonation scams

Government impersonation scams decreased in 2021 with reports down 25% to 18,000, however losses to these scams increased 31% to over $2 million.

These scams rely on fear, intimidation, and a desire to comply with authority to convince people into parting with their money. Commonly impersonated government agencies or brands in 2021 included the Australian Taxation Office (ATO) the Australian Federal Police (AFP), MyGov (Services Australia), the Department of Home Affairs and the Australian Border Force.

The most common types of government impersonation scams seen in 2021 were threats to life arrest or other, phishing scams and identity theft.

Almost 95% of government impersonation scams in 2021 were conducted by phone. The majority of the remaining 5% of reports listed email or text message as the contact method.

Common **fake government campaigns** included:

- Messages purporting to be from MyGov, inviting the recipient to click a link to claim a 'one-off COVID-19 relief payment'. The link took the recipient to a page to 'verify' their personal information in order to confirm they were eligible for the payment.
- Messages impersonating the ATO, claiming that the recipient was suspected of tax evasion and asking them to click a link to provide more information. One message commonly reported read 'ATO: You are suspected in Tax Evasion. Connect your cryptocurrency wallet to provide transaction history please visit https://my.gov.au.wallet-security.info/'. If followed, this link was designed to capture personal information which scammers could then use to impersonate the victim to access government benefits.
- Facebook Messenger scams in which victims were messaged about a 'COVID relief grant', 'COVID-19 relief prize', or 'COVID-19 social grant' which required a 'clearance fee' to access. The scams claimed the grants were for a variety of groups including seniors, home buyers, medical bills, individuals starting their own business, continuing education and retirees. In some instances, this message came from the compromised Facebook accounts of the recipients' friends.
- Cold calls stating the recipient was entitled to $3500–$3700 as COVID relief (requiring extensive personal identification information and clearance fees to access).
- Cold calls claiming the government was cancelling superannuation policies due to COVID and requiring the recipient to provide their personal and superannuation information
- Text messages from 'GOV-AU' stating: 'You have received the appointment for the 3rd dose. For more Info visit: https://vaccine-appointment.link/'.

Vaccine scams

In 2021, Scamwatch received 1,522 vaccine scam reports. Of these 277 reports mentioned rapid antigen tests, with over $60,000 in reported losses.

Scammers were attuned to developments in Australia. The vaccine rollout commenced in July and Scamwatch started receiving vaccine reports from around August 2021. The first wave of scams involved victims receiving a text message with a link inviting them to set up their covid passport. The link took victims to a site that mimicked the Medicare website and would ask for personal and banking details. For example, 'Your digital version of Covid-19 Passport is available: https://cutt.ly/be-safe'.

The second wave of vaccine scams involved scammers sending messages informing recipients they were eligible for their 'third dose' prior to the announcement of the booster program. These messages contained a link to a webpage which contained malware.

Scamwatch continued to receive reports of individuals losing money and identity information to scam websites selling fake proof of vaccination certificates, COVID-19 passports or that create falsified check-in pages.

The public were often confused about what was real or fake and reported several legitimate text message, phone call and emails from health facilities and government agencies throughout 2021.

Case studies: Vaccine scam reports

$300 lost

Kamala reported a scammer selling digital vaccine passports, certificates, and exemption cards on Facebook. The scammer pushed people to pay for the passports on Blockchain.com.

$390 lost

Emily reported a doctor who used the Telegram app and said he would give people a covid vaccination certificate without giving the jab.

Pet scams

Pet scams increased in 2020 as a result of lockdowns, but despite lockdowns easing, Scamwatch continued to see pet scam reports increase by 48% in 2021.

Scamwatch received 3,332 pet scam reports with over $4 million in reported losses. The most common contact method reported was email which also had the highest losses. The most common pets used in scams were puppies followed by kittens. Scamwatch also received reports about a wide range of animals including snakes, goats and ferrets. Some pet scams can lead to significant loss as people feel emotionally attached.

'All I wanted was the puppy to be safe and healthy but that never happened'

($90,000 lost)

Pet scams will generally advertise on fake websites, social media or classified sites. People won't be able to see the pet and after its paid for victims will be asked for more money because of a range of problems including transport issues, illness and need for vaccines. The scammers go to a lot of effort to convince people that the pet is being delivered.

Case study: Pet scam (ferret)

$800 lost

'I reached out to Gary from a ferret page group on Facebook as he had ferrets for sale. I sent him a deposit of $100 and he was going to send it via courier. But I had not heard of the courier, so I did not agree. He said he would deliver to me in person, but I said that would be hard because he would need a COVID permit to come from NSW to Victoria. I sent him $150 for vaccinations and he messaged a photo that they were at the vets getting vaccinated. He kept me up to date as he travelled and then said his car had broken down. I sent him money for it and then he said he got pulled over by animal control and that he needed $200 so he could continue. He said he should be there by 10pm. After 10pm I checked on Facebook and noticed he had blocked me on Facebook. I've requested my money back from PayPal which they are refunding, but this guy should be caught for scamming people'.

$1,200 lost

'I saw ferrets for sale on Facebook and reached out. I had to organise delivery from Sydney to Melbourne through a courier. They told me PayPal wasn't working so they sent bank details to pay the $300. Then they said to pay with Payld email details for an additional $300 for a crate to deliver the ferret. They sent me a tracking number. Then they asked for an additional $600 to pay for vaccine at the airport with a different BSB and account number. Once I made the payment I didn't receive anything further and no one answered at the shipping company. The shipping company was fake. The person on Facebook would not refund me. I told them I was going to police and they then blocked me from Facebook'.

3.5 Agriculture scams

In 2021, Australian farmers and agriculture businesses lost over $1.5 million to scammers targeting the agriculture industry. The most reported category was classified scams, with over $686,000 in reported losses, closely followed by online shopping scams with over $676,000 reported lost.

The most common agriculture scam reported was fake online sales for heavy machinery/tractors. This was a trend that became prominent during the beginning of the COVID-19 pandemic in 2020.

There were also significant losses to agriculture businesses from false billing scams. Scammers issued counterfeit invoices under real business names to farmers who purchased agricultural inputs, such as fertiliser. In one case, a small business owner lost over $200,000 by transferring money to a scammer's bank account listed on a false invoice.

Scammers also sought to obtain personal information, such as driver licences, passports, Medicare details and addresses from agriculture businesses and farmers.

Tractor scams

Scamwatch received 313 reports about scams involving the sale of tractors and other agricultural machinery such as backhoes, bobcats and excavators. The total losses from agricultural machinery scams in 2021 was $1.4 million.

These scams targeted people looking to purchase both new and second-hand machinery.

The new tractor scams involved setting up fake tractor websites offering a range of agricultural machinery. To make these websites look more legitimate, scammers will:

- use the name of another legitimate business
- use the ABN of another business
- include a physical business address which are vacant blocks, or belong to another business.

Scammers would also give the purchaser a 15-day trial period for the machinery before going through with the sale. The scammers would say the money is to be deposited to an escrow service while the trial period is running. However, the escrow business is part of the scam and is not legitimate.

The agriculture machinery scams also appear on legitimate platforms such as Gumtree and Facebook Marketplace. These ads often request that all communication be made over email to get people off the platform where the scam could be detected.

Livestock scams

In 2021, Scamwatch received 41 reports about livestock scams, with total reported losses over $31,000. The amount lost from each scam varied between $200 and $10,000.

These scams involved people looking to purchase livestock such as cattle, sheep, donkeys, horses, etc. via online marketplace platforms such as Gumtree and Facebook. These scammers would post ads on these marketplaces and communicate with the person via the messaging platforms.

Once the victim makes contact with the scammer, the scammer would ask for a deposit to secure the purchase and to pay for transport of the livestock, with the rest to be paid when the livestock is delivered. Once the deposit has been paid, communication stops with the scammer either 'blocking' the victim or deleting their social media account.

- ***'I enquired to purchase 2 miniature highland calves. I had multiple discussions over messenger and transferred $1000 deposit from my account to their nominated account. Amount was $1200 per calf plus $400 delivery. Calves were to be delivered Saturday but never were. They closed their Facebook account when I tried to send message.'***

4. The people reporting scams

4.1 The demographics

People who report to Scamwatch differ in gender, age, location and ethnicity.[26] Some people report on behalf of a relative and some report on behalf of a business or community organisation. Scamwatch collects demographic data to help it and other agencies understand who is most impacted by scams and provide warnings and information to people in an effective way. This section of the report explores who reported and lost money (and often personal information) to scams in 2021.

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.

Gender

In 2021, men reported losing more money than women. Men lost a total of $190 million and women reported losses of $131 million.

Table 4.1 Gender and scam reports and losses

Gender	Number of reports	Reports with loss	Losses
Women	142,092	12,736	$131m
Men	138,591	12,499	$190m
Non-specified	5,939	176	$2m
Total	**286,622**	**25,411**	**$324m**

Men reported losing twice as much as women to investment scams ($118.4 million compared with $58.1 million) in 2021. However, women reported losing more to romance scams when compared to men ($32 million compared with $24 million). While women lost a higher total amount of money than men to romance scams men were more likely to report losing money. In the younger age groups, men and women tend to lose similar amounts.

Table 4.2 Scam types reported by men and women by highest loss

Scam type	Women		Men	
	Reports	Losses	Reports	Losses
Investment scams	3,349	$58m	6,073	$118m
Dating and romance scams	1,636	$32m	1,715	$24m
False billing	10,378	$7m	10,767	$10m
Remote access	7,765	$8m	7,694	$8m
Threats to life, arrest or other	15,986	$7m	15,870	$4m

Women lost more money than men to remote access scams and to threats to life arrest or other.

26 Scamwatch does not collect data about specific ethnicity – reporters can identify in the report form as a person who speaks a language other than English.

Age

In 2021, people aged 65 and over made the most reports to Scamwatch (46,286) and reported the highest losses of almost $82 million. The clear trend emerged in 2021 with losses increasing with age.

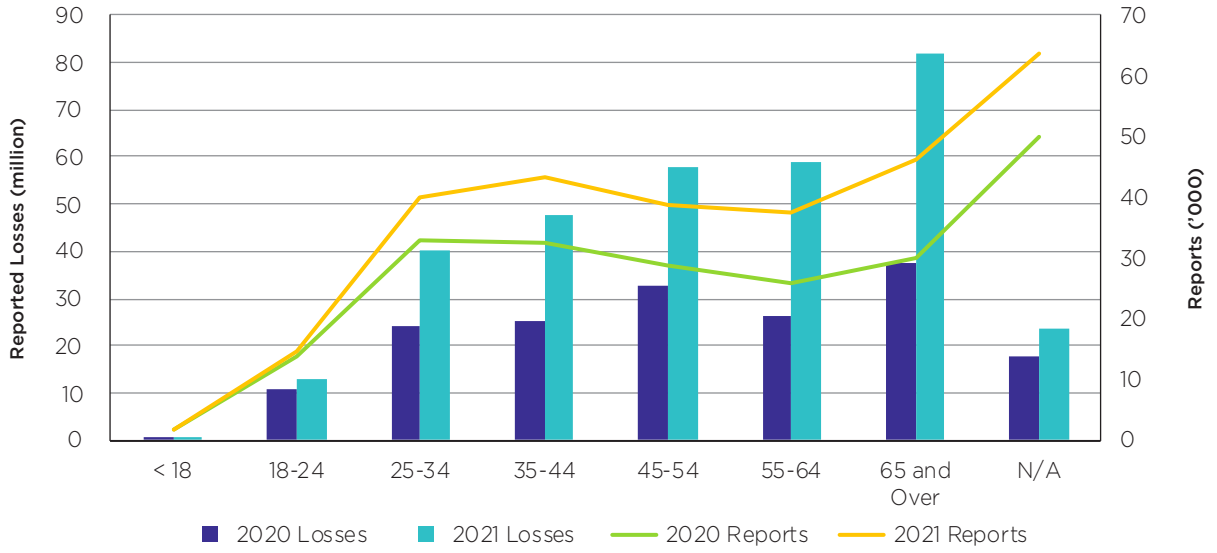


Table 4.3 Number of Scamwatch reports by age group – 2021 compared with 2020

Age group	2021 Reports	2021 Reports with loss (% of total reports in age group)	2021 Losses	2020 Reports	2020 Losses
Under 18	1,984	372 (18.8%)	$366,592	1,810	$496,156
18–24	14,834	3,038 (20.5%)	$13m	13,781	$11m
25–34	39,954	5,299 (13.3%)	$40m	33,122	$24m
35–44	43,527	4,837 (11.1%)	$48m	32,727	$25m
45–54	38,893	3,751 (9.6%)	$58m	28,908	$33m
55–64	37,644	3,010 (8.0%)	$59m	25,836	$26m
65 and over	46,286	3,055 (6.6%)	$82m	30,053	$38m
Age not provided	63,500	2,049 (3.2%)	$24m	49,850	$18m

Case study: Payment redirection scam targeting an older Australian over $370,00 lost

Janine was assisting her elderly grandmother who had sold her home to pay the deposit required to move into aged care. Janine received an email from the aged care home with the bank details so the payment could be made. The email contained the breakdown of fees and confirmed the bank account details for payment.

Janine provided the account details to the property settlement agent so that the proceeds from the sale of the house could be paid to the aged care home at settlement.

The settlement agent confirmed they processed the payment and requested confirmation of receipt from the aged care home.

Janine received a phone call from the aged care home saying that the funds were not received. Janine requested confirmation of account details and then realised that the ones she had paid were incorrect. She spoke to the manager of the aged care home, her bank, the recipient bank and concluded it had been a payment redirection scam. The email of the aged care home had been hacked. Her grandmother lost over $370,000.

Location

Scamwatch receives reports from people all across Australia and from overseas.[27] Generally the number of reports and losses is consistent with population size and this was the case in 2021 with people from New South Wales making the most reports (92,122) and reporting the highest losses ($110 million). In 2020, Victorians reported the highest losses and reports, and this was attributed to the impact of the pandemic on Victoria.

Table 4.4 Location of scam activity

State	Loss Total	Report Total
NSW	$110m	92,122
VIC	$74m	74,599
QLD	$59m	52,057
WA	$22m	25,416
SA	$19m	20,336
ACT	$7m	9,414
TAS	$4m	5,346
Overseas	$24m	4,308
NT	$2m	2,770
Blank	$2m	254

The amount lost to scams increased across Australia. The table below shows losses compared to population size.

Table 4.5 Losses by state compared with population

State	Loss Total	Census population on 30 September 2021
NSW	$110,080,190	8,186,800
VIC	$74,288,969	6,643,100
QLD	$58,559,252	5,240,500
WA	$22,175,130	2,685,200
SA	$19,363,369	1,722,800
ACT	$7,088,500	430,500
TAS	$4,417,723	540,800
NT	$1,589,956	245,900

The Australian Capital Territory has just 1.7% of the Australian population. However, ACT residents were overrepresented in terms of loss in 2021. This means that people in the ACT lost a proportionally higher amount to scams of all states. A full breakdown of the scam category of each Australian State and Territory is available in Appendix 2.

4.2 Scams affecting Indigenous Australians

Scamwatch invites reporters to indicate whether they are Indigenous[28] when they complete a webform. This information helps Scamwatch to identify the types of scams that may be impacting Indigenous Australians and target our warnings to the relevant communities.

27 Scamwatch includes losses where there is a connection to Australia in the scam report.

28 Scamwatch reports may include reporters who identify as 'Indigenous' in other countries (eg. New Zealand; USA; Canada etc).

In 2021, reports to Scamwatch from Indigenous people rose 44% to **4,958** and losses increased 142% to **$4.8 million** compared to 2020. Indigenous people reported a median loss of $650 which was an almost 18% increase on 2020.

Table 4.6 Top 5 scams with the highest losses for Indigenous reporters

Scam type	Losses	% from 2020	Median loss
Investment	$1.5m	371%	$3,092
Phishing	$1.1m	4301%	$500
Romance	$518,192	-12%	$900
Betting & Sports investment	$419,827	8424%	$1,120
Online shopping	$197,733	-28%	$284

Indigenous people represented:

- 43% of losses for betting and sports investment scams
- 41% of losses for health and medical products
- 26% of losses for phishing scams.

Indigenous people aged 45–54 lost the most money, followed by those aged 35–44 indicating that scams tend to impact younger Indigenous people compared to the trend in losses for all reporters. Indigenous people pay scammers in different ways to other Scamwatch reporters with the most losses reported as 'other payment' rather than bank transfer.

Indigenous people in NSW made the most reports (1,799) but those in Queensland reported losing the most money with over $2 million reported lost.

Case study: In-person scam in remote Australia

'I just want my money back. I got kids and paying rent myself. How can I get my money back please? I'm struggling. Cause we had no breakfast all day and my house has got no power.'

Marli, a sole parent of young children lived in a remote community. She was in financial hardship and was visited by a couple who were going door to door getting people to sign up for books and DVDs. The couple convinced Marli to enter into a long term contract without an assessment of family income or capacity to pay. She wanted to cancel but they would not let her.

Indigenous Australians also lost large amounts of money to investment scams including cryptocurrency.

Case study: Bitcoin investment scam – $180,000 lost

Over 5 months, Nora a retiree from Northern Australia invested all of her superannuation with a scam broker from 500 investments[29] who encouraged her to invest in Bitcoin. It started with a $200 investment and then she was pressured by Luke to add more to the online wallet which was performing well. The plan was to draw a monthly income of $5,000 but when she asked to withdraw the money Luke stopped responding to calls, texts or emails. She could see she still had $140,000 in the wallet and kept trying to withdraw but they cancelled each time. Eventually she saw her money was down to $15,000 and she had lost everything.

In 2021 Scamwatch received reports from at least 6 Indigenous Australians reporting shipping container scams with total losses exceeding $26,800.

29 Warnings by FCA (UK) https://www.fca.org.uk/news/warnings/500-investments-cabsy-holdings-ltd , Austrian FMA and Italian CONSOB.

Case study: Shipping container scam

'I purchased 4 shipping containers in 3 separate transactions. I received invoices paid by EFT, however the delivery date passed with no containers received. Now I cannot contact them as phones have been disconnected and not answering emails.'

The report noted the website responsible was: www.boxesandcontainers.com. This website was one of a series of websites facilitating these scams. The ACCC's Scamwatch notified the hosting provider about the Scamwatch reports and the web host removed the website.

4.3 Scams affecting culturally and linguistically diverse communities

People reporting to Scamwatch can identify as a person from a 'non-English speaking background' when lodging an online report. This is used as a proxy by Scamwatch to report on scams that impact culturally and linguistically diverse communities (CALD communities). Scamwatch does not collect data on the specific languages spoken or cultural backgrounds of reporters from a non-English speaking background.

In 2021, people from CALD communities made up 5% of reports and almost 13% of the total losses. There was a 20% increase in reports to Scamwatch from CALD communities to 14,060 and an 88% increase in financial losses up to almost $42 million compared to 2020.

The median loss for CALD reporters was $1,200 which was higher than for non-CALD reporters ($845). Reports from CALD communities made up 13% ($42 million) of all reported losses.

Table 4.7 Top 5 scams with the highest losses for CALD Communities

Scam type	Losses	Percentage change from 2020	Median loss
Investment	$20m	224%	$4,100
Romance	$7m	28%	$10,000
Threats to life, arrest or other	$4m	-32%	$6,000
Identity theft	$4m	852%	$1,288
Phishing	$1m	336%	$600

For CALD communities the contact method resulting in the highest losses was Mobile Apps with $10.2 million reported lost. Many people in these communities were impacted by the ponzi/pyramid scheme Hope Business scam which utilised apps. People from CALD communities made up 19% of the reports about Pyramid schemes in 2021.

Case study: Pyramid schemes and CALD communities – lost $20,000 each

Sharman invested money in the Hope Business app in the hope of getting a 2–3% return. He had to buy products which the app on-sells. He lost $20,000.

Riaan received a referral from a friend and invested in the Hope Business app losing $20,000.

Women from CALD communities reported losing more money (almost $21 million) than men (almost $20 million), but men made more reports. The age group 45–54 lost the most money ($11.5 million) followed by those aged 35–44 ($9 million) and 25–34 ($8 million). Younger CALD people were far more likely to lose money to threat based scams with the 18–24-year-old group losing the most ($2.8 million).

People from CALD communities were over-represented in the losses for some scam types, accounting for:

- 19% of reports and 38% of losses for pyramid schemes
- 5% of reports but 37% of losses for threats to life arrest and other
- 6% of reports but 37% of losses for identity theft
- 4% of reports but over 30% of the losses for phishing scams.

Case study: Threat based scam $300,000 lost

Xiu had just finished university in Australia and received a phone call from Zihan (a scammer) who said she was from China Communications Group Co. which Xiu thought might be a fake business. Zihan said that there was a phone number registered under Xiu's name which was sending scam messages. Zihan told Xiu to contact the Chinese police on a phone number Zihan provided. After calling the number Xiu was told that there was a bank account with money missing and was shown documents purporting to be evidence of this loss.

Xiu trusted that they were the real police and was asked to do verification of voiceprint and handwriting. Xiou participated in a video call and saw them wearing the police uniform. They told Xiu that the person responsible worked for the Commonwealth Bank. Xiu was instructed to send money to an ANZ account belonging to Hong Kong prosecutors whose names she was given. She transferred 2 amounts totalling $300,000. Xiu was told some of the money was for bail while she was in Australia otherwise the police said they would repatriate her back to China.

The contact went on for over a week and during that time Xiu was told she was not allowed to tell anyone about it. They said that after a few days she could tell her family and they would transfer the money back. When Xiu told her family, they said it was a scam and she should report to the police.

Government impersonation scams can impact vulnerable people from CALD backgrounds especially those who may be refugees or new migrants.

Case study: Visa scam targets vulnerable family – $410,000 lost

Sayeed (a scammer) offered to assist Prisha with her family's Australian Visa applications. Sayeed said he was from Melbourne and presented to the family as a lawyer and a security worker. He started to assist Prisha's family with their visas. Sayeed generated a fake video and Australian passport and took money from all the family members in cash. When confronted Sayeed refused to return the money and threatened the family members. He created false paperwork and disrupted their visa applications.

Sayeed threatened Prisha that if the matter was reported he would tell the police that Prisha's family were pretending to be police and were threatening rape, death and theft. Prisha and her family were frightened and left with no money.

Sayeed pressured Prisha's brother to sign a false statutory declaration and pay money to get a specialist lawyer for him. Prisha reported that this all became too much, and her brother tried to commit suicide. Prisha's entire family was stressed as Sayeed had all of her family's personal information which he obtained when pretending to process visas. Sayeed then started threatening Prisha's family in India as well. He got their passport details and other documents.

Prisha stated that it took her family a lot of courage to come forward and report it and they did because they did not want Sayeed to fraud and rob any other families.

4.4 Scams affecting people with disability

When people report to Scamwatch, they can indicate if they identify as a person with disability on the report form. This helps Scamwatch identify scams that may be targeting or impacting people with disability so that we can ensure our warnings are relevant and effective. Scamwatch received 15,387 (about 5% of all reports) reports from people with disability with financial losses of $19.6 million (6% of total losses).

In 2021 there was a 104% increase in reports from people with disability and a 102% increase in financial losses reported to Scamwatch. The median loss was $700.

Table 4.8 Top 5 scams with the highest losses from people with disability

Scam type	Losses	Percentage change from 2020	Median loss
Investment	$8m	202%	$5,000
Romance	$4.3m	-23%	$2,568
Identity theft	$2.7m	3,223%	$1,079
Remote access scams	$1.2m	480%	$3,800
Threats to life, arrest or other	$1.1m	548%	$2,750

Older people with disability lost more money, with those over 65 losing almost $7 million.

Case study: Remote access $40,000 lost

Susan, an older Australian with disability received a call from Owen (a scammer) who said he was from NBN asking about her internet and home phones. Owen said that someone was trying to take money from Susan's accounts. Owen said they were going to set up a dummy account to catch the people responsible. Owen said that no money would come from Susan's account but to make it look legitimate they would make it appear to come from Susan's account. Owen told Susan to press on something called 'AnyDesk'. This was remote access software that meant that Owen was then able to get into Susan's phones and tablet. He set up 3 transactions and said when the bank calls everything will be ok. Susan started to get suspicious, and Owen said all the money would be put back in their account. Susan looked up the cyber-crime department but somehow Owen knew she did this. Owen also accessed Susan's credit card. At the time of reporting to Scamwatch the scammers continued to call Susan. They had told her not to tell anyone about it.

People with disability were over-represented in the losses for some scam types, making up:

- 6% of reports but 38% of losses for ransomware and malware
- 5% of reports but 26% of losses identity theft
- 8% of reports but 25% of losses for unexpected prize & lottery scams
- 8% of reports but 15% of the losses for inheritance scams.

Case study: Health & medical scam from reporter with disability

Elana, an aged pensioner, saw an article advertised on Facebook which brought up an offer to buy 2 and get 2 free for health products. Then a yellow box popped up and said to put delivery details and name and it was a one time offer for $78 that would run out in so many minutes for a product that would help with her arthritis and diabetes. Elana put her credit card details to take up the offer. Elena checked her bank online and was horrified to see 2 amounts had been taken out for a total of $500.

Reports of losses to unexpected prize and lottery scams were also higher for reporters with disability. Many of these scams related to COVID-19 social support payments from the Federal Government. These scams were spread as links in emails or contact on social media by compromised accounts leading individuals to believe they were being directed to the program by friends.

4.5 The Businesses losing money to scams

The scam that impacts business the most is payment redirection, also known as business email compromise. Combined losses to payment redirection were **$227 million** in 2021 with most reports made to banks and ReportCyber. Scamwatch received 1,363 reports about payment redirection scams[30] with $12.5 million reported lost.

Scamwatch receives reports about scams from businesses and they can advise whether they are large (over 200 staff); medium (20–199); small (5–19) or micro (0–4) or not provide their size. While total losses went down for small businesses, the median loss for small business was higher than other business sizes.

In 2021, Scamwatch received 3,624 reports from businesses[31] with $13.4 million reported lost. This represents a 13% decrease in reports and a 27% decrease in losses.

Table 4.9 Losses and number of reports by business size

Business size	Reports	Losses	Percentage change in losses from 2020	Median loss
micro (0–4 staff)	1,093	$3.5m	71% increase	$1,550
small (5–19 staff)	890	$3.5m	28% decrease	$3,812
medium (20–199 staff)	551	$4.2m	170% increase	$2,772
large (over 200 staff)	319	$421,000	95% decrease	$1,601
size of business not provided	771	$1.7m	117% increase	$2,398

The highest losses were to false billing scams which includes many payment redirection scams. Businesses reported losses of $6.7 million to false billing scams with a median loss of $4,200. However, for small businesses the median loss was $8,000. The second highest losses were investment scams with over $5 million reported lost and a median loss of almost $40,000.

The most common contact method for reports and losses was email, which is not surprising given the scam that causes the highest losses involves scammers emailing invoices with a change of payment details.

Table 4.10 Top 5 scams by loss – business

Scam type	Losses	Percentage change in losses from 2020	Median loss
False billing	$6.7m	-50%	$4,200
Investment	$5.1m	205%	$39,273
Classified scams	$0.6m	202%	$2,250
Online shopping scams	$0.3m	-32%	$916
Identity theft	$0.2m	205%	$1,531

Case study: False Billing report from business – $90,000 lost

An Australian Engineering company's emails was somehow intercepted and redirected from the same email address but had .com instead of .com.au. It contained a request to change bank account details and had an attached letter with the legitimate company's logo. A payment was then made to the fraudulent account and was not discovered until the supplier queried their unpaid invoices.

30 Scamwatch does not have a category for payment redirection or business email compromise. Most people report under false billing but others are under phishing; other scams; identity theft and hacking. These will include reports by both individuals and businesses.

31 This includes all businesses that specified a business size: large, medium, small or micro.

5. The fight against scams

Scamwatch sent more than **150 disseminations** of scam reports on high risk or current scam trends to law enforcement and government. This intelligence assisted state and federal police to investigate and, in some instances, prosecute scammers. Police investigated, charged and/or arested individuals involved in money muling rings; roofing scams; puppy scams; identity theft; investment scams and phone scams impersonating law enforcement or banks.

Scamwatch provided Flubot URLs to the Australian Cyber Security Centre to facilitate website removal requests on 18 occasions.

5.1 ACCC identifies Flubot scam and collaborates to disrupt the scam

In August 2021 the ACCC received some of the first complaints of the 'Flubot' scam when it hit Australia. It was the largest phone malware campaign ever seen in Australia. Scamwatch received close to 26,500 reports by the end of the year.

Flubot was one of the fastest spreading mobile malware known to date emerging in Europe and the US before hitting Australia. It steals passwords, online banking details and other sensitive information from smartphones around the world.

The ACCC wrote to Australian banks to alert them to the risk of mobile banking compromise. We set out our expectations that banks would immediately take steps to minimise the ability for scammers to compromise consumer accounts and that they will support affected consumers to minimise losses and recover access to their accounts.

In mid-September we wrote to more than 27 banks and credit providers and notified the Australian Banking Association and the Australian Financial Complaints Authority that we had contacted banks to make them aware of our concerns relating to Flubot.

Scmawatch worked with the Australian Cyber Security Centre and their partners to ensure websites hosting 'Flubot' reported to Scamwatch were rapidly removed from the internet. We uploaded Australian strains of Flubot for ingestion into anti-virus tools and safe browsing engines.

We provided phone numbers associated with phone scams including Flubot to the telecommunications industry.

Direct financial loss to these scams remained low (just under $11,000). Although an unknown number of people may have experienced loss of personal information.

We shared the scam reports about Flubot with the Australian Federal Police to assist it in law enforcement efforts. In June 2022, The EU announced that an international police cooperation including the AFP was successful in taking down the FluBot criminal infrastructure. Europol's European Cybercrime Centre brought together the national investigators in the affected countries to establish a joint strategy, provide digital forensics support and facilitate the exchange of operation information. The operation included relevant Australia (AFP); Belgium; Finland; Hungary; Ireland; Romania; Sweden; Spain; Netherlands and the United States.

5.2 ACCC and the Scams Awareness Network improve outcomes for victims of identity compromise

During 2021 the ACCC continued its work with Department of Home Affairs and IDCARE in advocating for the state and territory licencing authorities and State Ministers to seek a nation-wide practical solution that will enable the use of a unique identifier (UID) number on each new licence card issued. A UID would enable licencing authorities to replace lost or stolen licences more-readily without re-issuing a new driver licence number.

This resulted in agreement from States to enhance security measures around identity verification and driver licences and the ACCC is continuing to work alongside the Department of Home Affairs and state and territory authorities to implement these improvements.

This will make it more difficult for criminals to use lost or stolen driver licences and easier for victims to recover from identity crime.

5.3 Stronger measures introduced in telco sector to tackle phone scams

Since about 2017 the ACCC has highlighted concerns about the use of phone services to perpetrate scams and the harms caused by mobile porting fraud.

In December 2018 the ACMA established the Scam Technology Project to tackle phone scams. Since its inception, the ACCC has worked alongside the ACMA and the Australian Cyber Security Centre, other government agencies, such as the ATO, and telecommunications providers.

Key outcomes of the project include:

- the introduction of the *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020* which has reduced the level of porting fraud
- the registration of the *Reducing Scam Calls Industry Code* in December 2020 and the increased use of call blocking to disrupt phone scams
- ongoing development of measures to prevent sim swap fraud
- work on regulatory measures to require telcos to monitor and block malicious scam SMS messages.

The ACCC continued to play an important role in the Scams Telecommunications Action Taskforce which provides government and industry coordination and oversight of telecommunications scam minimisation strategies.

We work closely with telecommunications providers and the ACMA to understand the actions they are taking to meet their requirements under the Reducing Scam Calls Code and the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020.

In 2021, over 100,000 scam reports advised that the scammer made contact in a phone call.

Telecommunications providers blocked over 357 million scam calls *in the first 12 months of the code's operation (2 December 2020 to 30 November 2021), limiting opportunities for criminals to scam Australians.*

Each week the ACCC provides a report of telephone numbers that have been reported to Scamwatch to Communications Alliance members including Telstra, Vodafone, Optus, Vocus, Pivotel, Aussie Broadband, MNF Group and NetSip. Its important to report scam calls so this information can be used to disrupt the scams.

At the time of publishing this report, phone scams reported to Scamwatch in 2022 had decreased 48% compared to 2021.

The Australian Communications and Media Authority flags additional rules for telcos

Phone scams remained a key priority[32] for the Australian Communications and Media Authority (ACMA) throughout 2021. The ACMA engaged with industry and government agencies and international counterparts to disrupt scams on Australia's telco networks, promote compliance obligations to industry, and educate consumers about how they can identify scams and protect themselves. Building on the successes of the *Reducing Scam Calls* industry code and SMS Sender ID solution, the ACMA

32 ACMA 2021, *ACMA compliance priorities 2021–22*, viewed 24 January 2022.

is working with Communications Alliance to develop enforceable obligations on telecommunications providers to identify, trace and block or disrupt SMS scams. The ACMA anticipate making new rules in the first half of 2022.

The ACMA is also developing new rules to require telecommunications providers to undertake enhanced identity verification prior to engaging in customer interactions with a high risk of fraud, for example, SIM swap, billing enquiries or account change requests.[33]

The ACMA-led Scam Telco Action Taskforce met in March, August, and early December 2021. Issues discussed included scam reduction initiatives, new telco technology to identify and block scam calls and trials of trusted organisation impersonation scam reduction initiatives. The Taskforce will continue to meet in 2022.

In December 2021, the ACMA renewed its scams consumer awareness resources[34], targeting key findings from its consumer research into the Australian experience of unsolicited communications.

The ACMA also issued formal warnings to 3 telcos for failing to protect customers against identity theft (following rules[35] introduced in early 2020 which require telcos to have more rigorous customer verification processes in place, such as multifactor or in-person identification).

5.4 ACCC advocates with finance sector and regulators to address scams

Most payments to scammers were via traditional bank transfer. In 2021 $129 million was reported to Scamwatch as paid via bank transfer. Financial firms are in a unique position to identify fraud risk and invest in capability to mitigate risks.

The ACCC has communicated expectations to the finance sector about its role in preventing scams. The ACCC appreciates that the finance sector is increasing its effort to combat scams but is of the view that more is required to increase the effectiveness of scams prevention. The ACCC is seeing more scam victims losing larger amounts of money with devastating consequence often to those who can least afford it.

Case study: Payment redirection in property settlement – over $700,000 lost

'We were about to settle on a home we purchased only to find out the mortgage broker's email had been compromised by a hacker or scammer. This person pretended to be our mortgage broker by intercepting emails and assuring me where to transfer my funds of over $700,000 to ensure a smooth settlement process. Turns out the account was not where the bank wanted the money to go, and our broker knew nothing about his email (and many threads) being written by the scammer and not him.

***We had no idea it wasn't him and now we've lost our life savings and cannot settle on our new home. Devasted**'.*

In 2021 ASIC continued its review of the ePayments Code and amended the Code to exclude scams from the mistaken payment and unauthorised transactions provisions. While the ACCC recognised that the Code was not set up to protect consumers from scams, in its submissions to ASIC, the ACCC highlighted the need for the banking and payment sector to consider some regulatory initiatives that have been implemented in comparable jurisdictions overseas.

The ACCC also advocated in its submission to the Review of Australian Payments Systems for the adoption of initiatives similar to the UK's Confirmation of Payee which would match the account number to the intended recipient to reduce scam losses occurring by bank transfer.

33 ACMA, 2021, *Proposal to make Telecommunications Service Provider (Customer Identity Verification) Determination 2021*, viewed 24 January 2022.

34 ACMA 2021, *Phone scam educational resources | ACMA*, viewed 25 January 2022.

35 *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020*, viewed 24 January 2022.

Case study: Scam prevention measures in financial sectors overseas

Confirmation of payee (UK)

Confirmation of Payee (CoP) is a tool in reducing certain types of scams and accidentally misdirected payments. It checks the name of the payee's account against the other details given by the payer.

Introduced in the UK in 2019, the 6 largest banks in the UK and 92% of transactions in the UK Faster Payments system are covered. The UK is working on expanding to cover 99% (a further 50 payment providers to be brought under the scheme). The first full year of CoP led to a 35% fall in mistaken payments.[36]

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. Better processes could be developed in Australia to alert customers when an account number does not match a name. This would be useful in disrupting payment redirection scams and would also provide limited protections for consumers from other types of fraud and mistaken payment.

'CoP has been a game changing innovation in the battle against fraud and scams in the UK... not only will this detect fraudulent and misdirected payments, but CoP is also proven to reduce operating costs and improve the digital journey for customers' (NatWest Group, UK).[37]

IBAN Name check (the Netherlands)

In 2017 Dutch banks introduced the IBAN-name check service which led to an 81% drop in reported fraud/scams.[38] From 2020 customers will also be refunded if a scam occurs through telephone number spoofing.

Contingent Reimbursement Code (UK)

In 2020 the UK implemented the *Authorised Push Payment Contingent Reimbursement Model Code*. This Code requires banks to implement CoP and issue effective warnings to customers; delay or stop payments; act quickly when a scam is reported and stop scammers opening bank accounts. It also requires banks to reimburse scam victims in certain scenarios, to identify higher risk payments and customers who are vulnerable.

Voluntary initiatives

The ACCC is aware of a bank in the UK that has made voluntary commitments to refund scam victims who have been tricked by a scam. It provides refunds for an honest mistake including accidentally clicking on something they shouldn't.[39] The bank considers this is the lowest cost option that doesn't result in a higher level of fraudulent claims or customers being less careful.[40]

Scamwatch sets up API with Australian Financial Crimes Exchange (AFCX)

To enable the banks to better combat scams, the ACCC shares scam reports with the AFCX for provision to NAB, CBA, Westpac, ANZ, Bendigo Bank and Macquarie Bank. This provides the banks with close to real time information about scams and often includes the account numbers of the scammers. We expect the banks to act on this information to stop scammers. The ACCC is looking to expand the scammer intel it shares with the AFCX across all the members on the platform.

The ACCC also meets regularly with the Australian Banking Association, AusPayNet, the New Payments Platform and RBA on initiatives to reduce scams.

36 PSR CP22/2 Confirmation of payee: requirements for fourth participation in CoP 2022, p 24.

37 30 May 2022, Gaurav Gaur, NatWest Group UK https://www.finextra.com/newsarticle/40344/natwest-launches-confirmation-of-payee-api-for-business-customers.

38 SurePay 2020 report: https://www.surepay.nl/en/surepay-year-report-2020/.

39 https://www.tsb.co.uk/fraud-prevention-centre/fraud-refund-guarantee/.

40 TSB Bank: https://www.tsb.co.uk/news-releases/tsb-marks-three-years-of-fraud-refund-guarantee/ and https://committees.parliament.uk/writtenevidence/18464/html/.

The ACCC shares information with the Australian Financial Complaints Authority to assist their determinations when assessing the banks handling of scam complaints.

ACCC works with banks and tech companies to combat remote access scams

In 2021, reports of remote access scams increased by 85% compared to 2020 and losses increased by 94% to over $16 million.

Scamwatch in collaboration with NBN Co identified scammers using TeamViewer software to remotely steal money from victims. The ACCC met with TeamViewer to understand how we might collaborate to reduce these scams.

TeamViewer proposed a number of technical solutions to reduce scams and we facilitated a roundtable with the ABA, NAB, CBA, Westpac, ANZ, Suncorp, HSBC, Macquarie, BoQ, Bendigo Adelaide and ING to discuss these in May 2021.

As a result of these initiatives reports of remote access scams involving TeamViewer reduced significantly in the second half of 2021. Between January and June 2021 the ACCC received 960 reports about scams using TeamViewer with losses of over $2 million. After this initiative from July to December 2021 reports decreased by 69% to 292 and losses reduced by 71% to $591,000.

The ACCC's next step is to undertake similar steps with other remote software companies being used in scams.

5.5 The ACCC shares scammer intel with the US Federal Trade Commission

In 2021 the ACCC commenced sharing scammer intelligence through the US Federal Trade Commission (FTC) Consumer Sentinel Network (approximately 32 countries) adding to the global intel on scams and consumer fraud.

5.6 ACCC focuses on digital platforms and commences proceedings against Meta

Financial loss to scams over social networking and online forums increased almost 107% in 2021 to $56 million. The ACCC expects Digital Platforms to use their own tools to monitor platforms, educate users and remove scammers.

Since 2017 the ACCC sends a daily dissemination of Scamwatch reports involving Facebook to Facebook to take appropriate action.

The ACCC has advocated for digital platforms to take more action to address scams. This has been covered in the ACCC's inquiries into various aspects of digital platforms including the final report, which included 2 specific recommendations to address scams.

ACCC action against Meta for publishing scam celebrity crypto ads on Facebook

In March 2022 the ACCC commenced proceedings in the Federal Court against Facebook owner Meta Platforms Inc and Meta Platforms Ireland Limited alleging that they engaged in false, misleading or deceptive conduct by publishing scam advertisements featuring prominent Australian public figures.

The ACCC alleges the ads, which promoted investment in cryptocurrency or money making schemes were likely to mislead Facebook users into believing the advertised schemes were associated with well-known people featured in the ads. The ACCC alleges the schemes were in fact scams, and the people featured in the ads had never approved or endorsed them.

The ACCC alleges that Facebook failed to prevent the publication of the scam ads even after public figures around the world reported similar ads to Meta. In one instance that the ACCC is aware of, a consumer lost more than $650,000.

5.7 Scamwatch increases the scam report data it shares with the private sector

Over the last 2 years the ACCC has sent tens of thousands of scam reports and met regularly with the private sector to combat scams.

Some of the organisations and platforms we shared scams intel or collaborated with included:

- Gumtree
- MoneyGram
- Western Union
- LinkedIn
- TeamViewer
- NBN Co
- Seek
- Afterpay
- CarsGuide
- Facebook
- Autotrader
- CoinSpot
- Amazon
- Microsoft.

The ACCC meets with representatives of these platforms and businesses to discuss emerging scam trends and to identify opportunities to prevent and disrupt scams. As an example, Scamwatch identified a new scam targeting Gumtree users whereby scammers were claiming to have organised for couriers to collect or deliver goods. Gumtree who regularly engages with us to address scams on the platform, now has a pop-up embedded into their site, warning users about this scam as soon as they enter the platform.

5.8 Scams Awareness Network

The ACCC Chairs the Scams Awareness Network, which is comprised of government regulatory agencies and departments with responsibility for consumer protection and policing in the areas of scams, cyber safety and fraud.

The core purpose of the Scams Awareness Network is for members to share information about scams regularly and to deliver a coordinated awareness campaign for consumers. It has 40 government agencies and IDCARE as members (a list is available here).

The ACCC shares updates with government agencies about each agency's activities and the Network meets annually.

5.9 Scamwatch media, social media and awareness raising

From 8–12 November the ACCC led the Scams Awareness Week campaign which was supported by over 350 partner organisations. The campaign encouraged the public to 'Stop Scams. Speak Up' and reached an estimated 15 million people.

By the end of 2021, Scamwatch had 127,972 subscribers to its email alert service and published 9 media releases warning the public about scams.

The Scamwatch website had over 8 million page views in 2021, and the ACCC's Little Black Book of Scams was viewed 21,910 times and downloaded 12,391 times. We distributed 91,413 hard copies.

In 2021 the Scamwatch Twitter account (@Scamwatch_gov_au) posted 261 tweets and by the end of 2021 had a following of over 35,000.

In June 2021, the ACCC released its 2020 Targeting Scams report which was viewed 7,507 times and downloaded 5,222 times.

In 2021 there was an increase in demand for information about scams and trends. We responded to hundreds of media requests. 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.

The ACCC's indigenous outreach teams visited Bagot Community, Belyuen Community, Knuckey Lagoon and Palmerston Indigenous village in 2021 where among other things staff provided information and responded to concerns about scams.

The ACCC issued 9 media releases on a scams related topic.

Date	Media release
8 Nov 2021	Stop Scams Speak Up – scams awareness week
27 Sep 2021	Losses reported to Scamwatch exceed $211, phone scams exploding
12 July 2021	Computer takeover scams on the rise
10 June 2021	CALD community lose $22 million to scams in 2020, reports form Indigenous Australian up by 25%
9 Jun 2021	Payment redirection scams cost Australian businesses $128 million in 2020
7 Jun 2021	Scammers capitalise on pandemic as Australians lose record $851 to scams
27 Apr 2021	Losses to car ad scams climbing
30 Mar 2021	Payment redirection scams cost Australian businesses $14 million
12 Feb 2021	Romance baiting scams on the rise

5.10 Scams Awareness Week – 350+ government and private partners

The ACCC runs Scams Awareness Week in November each year, and also involves private sector and community partners.

Scams Week was held in the week 8–12 November 2021. The campaign encouraged everyone to start a conversation about scams to reduce stigma and help people recognise a scam sooner, or prevent scams from happening in the first place. The ACCC produced 4 short videos which ran on social media throughout the week and also has dedicated campaign activities and resources to start discussions about scams which are available on the Scamwatch website.

Over 350 partners supported Scams Awareness Week 2021 under the theme ‘Stop scams. Speak up’. The campaign aimed to encourage conversation about the often-stigmatised topic of scams. A series of short videos, a crossword, quiz, and a game of scam bingo helped promote the Scams Awareness Week message and spark conversations about scams. The campaign was a success and **reached an estimated 15 million people**. More information about Scams Awareness Week and a list of campaign partners is available on the Scamwatch website.

Global Anti-Scams Alliance – Scamwatch wins international award

The ACCC attends a range of international forums and working groups to discuss scams and share information about trends. Scamwatch is a member work with the international Law Enforcement Anti-scams Group run via the Global Anti Scam Alliance headquartered in the Netherlands.

Scamwatch was honoured as Scamfighters of the year in early 2022. Scamwatch was awarded the best scam fighting organisation for its role in ‘providing excellent and comprehensive information about how

to recognise, avoid and report scams'[41] and for 'taking a lead role in the combat against online fraud globally.'[42]

ATO campaigns & Partnership

In 2021 the ATO worked with Services Australia to publish a joint media release about the first phishing scam targeting mygovID.

The ATO shared information and in-language resources about scams and identity protection through its Community Leader Network. This forum provides a forum to talk with Culturally and Linguistically Diverse representatives about tax and super scams and generate ideas on how the ATO can engage better with these audiences. The ACCC also presented to the network about scams more broadly, including how to report to Scamwatch and support services.

The ATO continued partnership with government agencies and financial institutions to promote best practice for scam management through representation at the Inter-regulatory scam network facilitated by ASIC.

The ATO continued to represent the ATO at the Australian Communications and Media Authority Scam Technology Action Taskforce. The STAT focussed its attention on SMS scams with the industry body (Communications Alliance) working to identify an industry wide framework to prevent scammers impersonating the SMS alpha-tags[43] of well-known brands and organisations. The ATO has worked with a vendor partner to implement an alpha-tag blocking pilot across all telecommunications companies to block selected SMS alpha-tags unless it comes from an ATO approved point of origin. This mirrors the successful pilot conducted by Services Australia to protect the 'myGov' alpha tag.

The ATO participated in the ACCC's Scams Awareness Week, by publishing a range of external and internal communications. Taking a storytelling approach for Facebook and LinkedIn in line with the 'Stop Scams. Speak Up' theme, the ATO described a scam report where a cashier had helped someone avoid buying gift cards for a fake tax debt scam. This approach performed well in terms of engagement and commentary.

In November, the ATO ran their annual internal Security, Integrity and Fraud Awareness week event, which gives staff the opportunity to reflect on their approach to security, integrity and fraud awareness and affirm we're making good decisions. An internal webinar on 'a partnership for scam prevention' was presented by ATO Cyber Director Fiona Homan and Delia Rickard, ACCC Deputy Chair.

The ATO facilitated the quarterly Cyber Security Stakeholder Group (CSSG) that brings together key stakeholders from tax professional, government and industry bodies to discuss emerging scam and cyber risks and promote effective mitigation strategies.

The ATO has continued work on a targeted, innovative campaign working with retailers to address scams using particular payment methods, which will launch in 2022.

Services Australia

Services Australia was able to prevent its impersonation in sender IDs in text messages by using the blocking functionality in Telstra's 'Cleaner Pipes'[44] initiative. Through this initiative it expanded the protection for mutual Services Australia and Telstra customers, with Optus, TPG Telecom (Vodafone) and Pivotel also applying similar technological solutions in March 2021. These organisations collectively blocked 738 attempts to impersonate a Services Australia sender ID in 2021. Services Australia remains active members of the Scams Technology Action Taskforce and contribute to other technological solutions to scams.

---

41 Cindy Liebes, Cybercrime Support Network.

42 Mitchel Chang, Trend Micro.

43 An alpha tag provides the ability to give SMS messages a unique 'sender' name which can include digits, text and some special characters using an alphanumeric sender ID.

44 Cleaner Pipes is an initiative of Telstra which was designed to prevent theft of personal information like logins, block the spread of malware and prevent customers passing infections onto their own contacts. It commenced in 2020 and involved the filtering of malware communications and blocking them as they try to cross Telstra infrastructure.

Services Australia updated its 'Beware of Scams' factsheet, which is now available in 28 languages. An additional language was added to assist with the arrival of Afghan evacuees in late 2021.

Services Australia raised awareness of scams via in-language SBS radio segments to assist culturally and linguistically diverse customers. These segments were aimed at geographical areas where specific communities were being targeted by scam activity. Multicultural Service Officers worked to help raise scam awareness in these communities.

In February 2021, the Services Australia launched a Current Scams Alert page on their public website to support individuals to identify or determine if they received scam contact. Since February 2021 this page has been visited over 30,000 times.

WA Scamnet

In 2021, WA ScamNet reported and removed the following:

- 416 Bank Accounts
- 109 Social Media Pages
- 258 Websites
- 12 Email accounts.

WA ScamNet assisted 10 victims to recover $349,634 in funds lost to scammers.

Case study: WA ScamNet – Shipping Container Sales scam

Victims responded to advertisements for shipping containers through Facebook Marketplace and Gumtree where they were then directed to a website which claims to be selling shipping containers at discounted prices.

Victims were presented with ABN information of legitimate businesses on the website and in correspondence and were directed to pay via bank transfer.

Once payment was received, minimal updates were provided on the arrival of the container. Victims also reported further demands for funds due to issues with the delivery, such as paying custom fees, insurance fees etc.

Websites identified by WA ScamNet were using stolen ABN details within the content of the websites and on invoices provided to victims to build trust that the purchase was legitimate.

WA ScamNet sent letters to ABN holders to inform them that their details were used on a scam website selling shipping containers and encouraged them to warn consumers. WA ScamNet reported the scam websites to the domain and web hosts to have them shutdown. They also reported the bank accounts used in the scam to limit the impact on consumers and assist those who had sent funds to potentially obtain a refund. The scam websites were also listed on the ScamNet website and an email warning sent to subscribers.

Examples of Law Enforcement

Actions from law enforcement in Australia include:

- In December 2021 the AFP arrested 2 people in Sydney in connection with a money laundering operation that worked through cryptocurrency exchanges. Australian police also led an operation to combat a money laundering scheme by working with police in 25 countries. They charged 17 Australians with money laundering and blocked $1.85 million from being cleaned.[45]
- In May 2022, 3 men were jailed for conning more than $434,000 out of vulnerable elderly Victorians as part of an elaborate roofing scam from 2020. The County Court ordered them to spend over 4 years in prison after they scammed more than 40 people. Some of the victims were victims of identity theft as their identities were used by the scammers to facilitate the scam activity.[46]
- In August 2021 Victoria Police arrested and charged a woman from Blairgowrie, Victoria with 5 counts of obtaining property deception in relation to an online puppy scams. The woman advertised French Bulldog puppies for sale through online marketplaces asking 5 victims to pay substantial deposits. The victims lost $31,000 collectively. Once the victims paid the deposit the woman allegedly requested transport and veterinary costs leaving victims without a puppy or their money back.[47]
- In April 2022 a Victorian man was charged after more than 100 people were allegedly defrauded of almost $300,000 through a string of puppy scams, false advertising on online marketplaces and scams where the person claimed to be from the ATO or a mobile phone company. The man is alleged to have used stolen identities to obtain bank accounts to transfer money into. He was charged with obtaining property by deception, possessing proceeds of crime and using a fraudulent document.[48]
- In October 2021 NSW police charged a man after he allegedly conducted an elaborate phone scam worth $30,000. He made fake phone calls pretending to be law enforcement or a financial institution. He demanded money and threatened violence or arrest for non-compliance.[49]

45 https://www.occrp.org/en/daily/15626-australian-police-continue-money-mule-arrests-confiscate-cash.

46 https://www.abc.net.au/news/2022-05-17/victoria-trio-jailed-over-roof-scam/101073914.

47 https://www.miragenews.com/mornington-peninsula-police-pounce-on-puppy-scam-621406/.

48 https://www.canberratimes.com.au/story/7716113/victorian-puppy-scam-suspect-to-face-court/.

49 https://www.9news.com.au/national/man-arrested-over-allegedly-pretending-to-be-law-enforcement-in-elaborate-phone-scam/2df42057-b979-44aa-9ddc-1e7d89bd447d.

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

Reports by losses

Scam type	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in losses since 2020
Investment scams	$177,184,295	9,664	4,068 (42.1%)	▲169.2%
Dating & romance scams	$56,175,428	3,424	1,379 (40.3%)	▲44.4%
False billing	$17,303,665	21,545	1,881 (8.7%)	▼-6.3%
Remote access scams	$16,412,258	15,698	1,330 (8.5%)	▲94.4%
Threats to life, arrest or other	$11,077,551	32,426	658 (2.0%)	▼-6.4%
Identity theft	$10,159,930	22,354	951 (4.3%)	▲230.7%
Online shopping scams	$8,074,469	20,694	7,436 (35.9%)	▲9.3%
Classified scams	$7,114,830	9,561	3,080 (32.2%)	▲28.7%
Phishing	$4,324,128	71,308	861 (1.2%)	▲156.0%
Hacking	$3,041,484	15,141	547 (3.6%)	▲114.3%
Jobs & employment scams	$2,697,500	3,453	308 (8.9%)	▲112.6%
Travel, prizes and lottery scams	$1,984,215	4,976	322 (6.5%)	▲1.0%
Pyramid Schemes	$1,341,389	487	215 (44.1%)	▲368.8%
Ransomware & malware	$1,172,034	3,623	54 (1.5%)	▲1,482.2%
Rebate scams	$1,145,112	2,046	132 (6.5%)	▲63.3%
Betting & sports investment scams	$976,214	328	125 (38.1%)	▼-1.0%
Inheritance and unexpected money	$923,256	1,831	150 (8.2%)	▼-60.0%
Overpayment scams	$841,060	2,027	315 (15.5%)	▲19.9%
Other scams	$690,788	40,970	1,018 (2.5%)	▲80.8%
Health & medical products	$372,014	1,588	289 (18.2%)	▼-90.5%
Psychic & clairvoyant	$358,501	187	89 (47.6%)	▲55.7%
Fake charity scams	$188,457	835	101 (12.1%)	▲41.5%
Mobile premium services	$165,139	2,456	102 (4.2%)	▲16.7%
Grand Total	**$323,723,717**	**286,622**	**25,411 (8.9%)**	**▲84.3%**

Reports by number of reports

Scam type	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in reports since 2020
Phishing	$4,324,128	71,308	861 (1.2%)	▲61.8%
Other scams	$690,788	40,970	1,018 (2.5%)	▲30.3%
Threats to life, arrest or other	$11,077,551	32,426	658 (2.0%)	▲0.7%
Identity theft	$10,159,930	22,354	951 (4.3%)	▲6.8%
False billing	$17,303,665	21,545	1,881 (8.7%)	▲64.2%
Online shopping scams	$8,074,469	20,694	7,436 (35.9%)	▲35.2%
Remote access scams	$16,412,258	15,698	1,330 (8.5%)	▲85.3%
Hacking	$3,041,484	15,141	547 (3.6%)	▲74.2%
Investment scams	$177,184,295	9,664	4,068 (42.1%)	▲32.5%
Classified scams	$7,114,830	9,561	3,080 (32.2%)	▲20.6%
Travel, prizes and lottery scams	$1,984,215	4,976	322 (6.5%)	▲3.0%
Ransomware & malware	$1,172,034	3,623	54 (1.5%)	▼-6.7%
Jobs & employment scams	$2,697,500	3,453	308 (8.9%)	▲17.7%
Dating & romance scams	$56,175,428	3,424	1,379 (40.3%)	▼-7.7%
Mobile premium services	$165,139	2,456	102 (4.2%)	▲61.3%
Rebate scams	$1,145,112	2,046	132 (6.5%)	▲12.0%
Overpayment scams	$841,060	2,027	315 (15.5%)	▲22.3%
Inheritance and unexpected money	$923,256	1,831	150 (8.2%)	▼-19.0%
Health & medical products	$372,014	1,588	289 (18.2%)	▲8.8%
Fake charity scams	$188,457	835	101 (12.1%)	▼-41.4%
Pyramid Schemes	$1,341,389	487	215 (44.1%)	▲20.0%
Betting & sports investment scams	$976,214	328	125 (38.1%)	▼-26.8%
Psychic & clairvoyant	$358,501	187	89 (47.6%)	▼-18.7%
Grand Total	**$323,723,717**	**286,622**	**25,411 (8.9%)**	**▲32.6%**

Appendix 2: Scam losses by State or Territory

Australian Capital Territory

Scam type	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in losses since 2020
Investment scams	$3,122,171	299	126 (42.1%)	▲227.8%
Dating & romance scams	$1,938,272	80	40 (50%)	▲254.0%
Remote access scams	$487,893	442	42 (9.5%)	▲181.0%
Threats to life, arrest or other	$325,846	1,317	27 (2.1%)	▲29.2%
Phishing	$263,229	2,788	26 (0.9%)	▲520.1%
Overpayment scams	$213,852	66	13 (19.7%)	▲461.5%
False billing	$196,924	623	47 (7.5%)	▼-48.1%
Online shopping scams	$182,282	597	234 (39.2%)	▼-27.6%
Classified scams	$163,468	232	84 (36.2%)	▼-28.1%
Identity theft	$92,939	650	19 (2.9%)	▲172.1%
Hacking	$20,346	329	12 (3.6%)	▲37.0%
Pyramid Schemes	$18,400	13	4 (30.8%)	▲30,566.7%
Other scams	$17,182	1,251	33 (2.6%)	▲16.4%
Jobs & employment scams	$13,599	105	7 (6.7%)	▲30.1%
Rebate scams	$10,305	117	2 (1.7%)	No losses in 2020
Inheritance and unexpected money	$5,851	37	3 (8.1%)	▼-96.1%
Travel, prizes and lottery scams	$5,421	138	7 (5.1%)	▼-44.3%
Mobile premium services	$4,352	73	5 (6.8%)	No losses in 2020
Psychic & clairvoyant	$1,820	4	2 (50.0%)	▲574.1%
Health & medical products	$1,779	35	5 (14.3%)	▼-31.7%
Betting & sports investment scams	$1,520	9	4 (44.4%)	▼-86.2%
Fake charity scams	$900	34	2 (5.9%)	▲153.5%
Ransomware & malware	$149	175	1 (0.6%)	▼-99.1%
Total	**$7,088,500**	**9,414**	**745 (7.9%)**	**▲127.0%**

New South Wales

Scam type	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in losses since 2020
Investment scams	$61,144,819	2,869	1,126 (39.2%)	▲276.1%
Dating & romance scams	$15,912,178	1,055	422 (40%)	▲19.0%
False billing	$8,542,655	6,794	606 (8.9%)	▲166.3%
Remote access scams	$5,672,547	5,369	408 (7.6%)	▲105.5%
Identity theft	$3,656,950	7,674	299 (3.9%)	▲337.0%
Online shopping scams	$2,750,482	6,896	2,546 (36.9%)	▲34.8%
Classified scams	$2,207,310	3,088	993 (32.2%)	▲47.5%
Threats to life, arrest or other	$2,132,956	10,468	159 (1.5%)	▼-27.4%
Hacking	$1,993,070	5,063	166 (3.3%)	▲444.9%
Ransomware & malware	$1,038,714	1,077	16 (1.5%)	▲3,991.5%
Phishing	$1,019,458	22,754	306 (1.3%)	▲219.9%
Jobs & employment scams	$1,019,262	872	83 (9.5%)	▲63.4%
Betting & sports investment scams	$726,134	83	30 (36.1%)	▲340.6%
Travel, prizes and lottery scams	$646,832	1,396	85 (6.1%)	▲124.9%
Rebate scams	$392,014	606	45 (7.4%)	▲68.5%
Pyramid Schemes	$313,073	114	43 (37.7%)	▲444.8%
Other scams	$225,240	13,122	304 (2.3%)	▲100.6%
Inheritance and unexpected money	$213,693	513	37 (7.2%)	▼-72.8%
Overpayment scams	$177,381	691	102 (14.8%)	▲0.8%
Psychic & clairvoyant	$96,149	48	27 (56.3%)	▲211.3%
Mobile premium services	$71,442	866	33 (3.8%)	▲34.8%
Fake charity scams	$70,615	244	28 (11.5%)	▲11.9%
Health & medical products	$57,216	460	91 (19.8%)	▼-55.6%
Total	**$110,080,190**	**92,122**	**7,955 (8.6%)**	**▲137.6%**

Northern Territory

Scam type	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in losses since 2020
Investment scams	$997,085	86	58 (67.4%)	▲187.9%
Remote access scams	$189,350	122	9 (7.4%)	▲1,103.1%
Dating & romance scams	$136,593	39	20 (51.3%)	▼-59.2%
Online shopping scams	$92,801	195	64 (32.8%)	▲77.6%
Classified scams	$49,489	93	29 (31.2%)	▲70.1%
Threats to life, arrest or other	$40,488	316	6 (1.9%)	▼-4.2%
False billing	$19,005	242	19 (7.9%)	▲54.3%
Phishing	$15,841	704	12 (1.7%)	▼-15.5%
Identity theft	$14,591	193	8 (4.1%)	▲78.0%
Overpayment scams	$9,200	23	3 (13.0%)	▼-67.4%
Hacking	$6,714	110	11 (10.0%)	▲282.3%
Pyramid Schemes	$6,400	5	2 (40.0%)	▲782.8%
Travel, prizes and lottery scams	$4,053	63	5 (7.9%)	▼-38.0%
Inheritance and unexpected money	$3,700	28	3 (10.7%)	▼-49.0%
Other scams	$3,269	444	9 (2.0%)	▼-53.4%
Jobs & employment scams	$800	25	1 (4.0%)	▼-79.7%
Health & medical products	$309	10	2 (20.0%)	▼-87.9%
Fake charity scams	$175	10	1 (10.0%)	▼-93.0%
Betting & sports investment scams	$93	1	1 (100.0%)	▼-84.9%
Rebate scams	-	14	0.0%	▼-100.0%
Psychic & clairvoyant	-	2	0.0%	▼-100.0%
Ransomware & malware	-	28	0.0%	No losses in 2020
Mobile premium services	-	17	0.0%	▼-100.0%
Total	**$1,589,956**	**2,770**	**263 (9.5%)**	**▲71.0%**

Queensland

Scam type	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in losses since 2020
Investment scams	$38,195,447	1,532	664 (43.3%)	▲261.6%
Dating & romance scams	$6,703,480	634	220 (34.7%)	▼-33.8%
Remote access scams	$3,335,618	2,754	245 (8.9%)	▲9.3%
Threats to life, arrest or other	$1,866,857	6,207	121 (1.9%)	▼-38.2%
False billing	$1,828,166	4,337	360 (8.3%)	▲26.9%
Phishing	$1,684,825	12,606	134 (1.1%)	▲684.1%
Classified scams	$1,493,390	1,847	507 (27.4%)	▲44.6%
Online shopping scams	$1,211,562	3,549	1192 (33.6%)	▼-15.1%
Identity theft	$463,913	3,774	148 (3.9%)	▲37.7%
Travel, prizes and lottery scams	$261,027	1,020	74 (7.3%)	▼-50.4%
Jobs & employment scams	$239,007	423	49 (11.6%)	▲437.6%
Hacking	$223,682	2,923	89 (3.0%)	▼-30.0%
Inheritance and unexpected money	$201,108	314	22 (7.0%)	▼-76.4%
Health & medical products	$181,114	267	52 (19.5%)	▲533.3%
Overpayment scams	$138,931	356	66 (18.5%)	▲19.3%
Other scams	$135,302	7,751	196 (2.5%)	▲115.1%
Rebate scams	$107,151	361	20 (5.5%)	▲28.8%
Pyramid Schemes	$103,319	88	34 (38.6%)	▲1.8%
Betting & sports investment scams	$72,526	51	15 (29.4%)	▼-47.4%
Fake charity scams	$42,715	154	18 (11.7%)	▲213.3%
Ransomware & malware	$39,744	704	9 (1.3%)	▲803.3%
Mobile premium services	$22,098	383	15 (3.9%)	▲16.9%
Psychic & clairvoyant	$8,270	22	7 (31.8%)	▼-49.8%
Total	**$58,558,252**	**52,057**	**4,257 (8.2%)**	**▲82.0%**

South Australia

Scam type	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in losses since 2020
Investment scams	$10,447,134	647	195 (30.1%)	▲183.3%
Dating & romance scams	$3,622,288	195	76 (39%)	▲122.4%
Threats to life, arrest or other	$903,805	2,232	36 (1.6%)	▲320.8%
Remote access scams	$903,258	1,034	98 (9.5%)	▲117.9%
Identity theft	$653,374	1,566	68 (4.3%)	▲75.8%
False billing	$505,883	1,562	121 (7.7%)	▲102.6%
Online shopping scams	$502,804	1,323	428 (32.4%)	▲37.4%
Jobs & employment scams	$496,706	174	21 (12.1%)	▲3,524.0%
Classified scams	$388,013	696	206 (29.6%)	▲4.8%
Travel, prizes and lottery scams	$262,404	403	33 (8.2%)	▲163.0%
Hacking	$239,392	1,089	50 (4.6%)	▲143.4%
Phishing	$145,538	5,290	55 (1.0%)	▼-5.8%
Rebate scams	$58,500	150	8 (5.3%)	▼-50.0%
Inheritance and unexpected money	$56,586	166	9 (5.4%)	▲29.7%
Other scams	$44,534	2,881	84 (2.9%)	▲119.8%
Pyramid Schemes	$32,952	14	7 (50.0%)	▼-6.1%
Overpayment scams	$28,738	128	12 (9.4%)	▼-44.6%
Mobile premium services	$20,492	160	10 (6.3%)	▲249.4%
Ransomware & malware	$14,192	273	6 (2.2%)	▲358.0%
Psychic & clairvoyant	$12,030	9	5 (55.6%)	▲2,213.5%
Fake charity scams	$11,360	66	12 (18.2%)	▲48.2%
Health & medical products	$10,836	252	29 (11.5%)	▲40.9%
Betting & sports investment scams	$2,550	26	3 (11.5%)	▼-89.5%
Total	**$19,363,369**	**20,336**	**1,572 (7.7%)**	**▲142.5%**

Tasmania

Scam type	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in losses since 2020
Investment scams	$2,461,272	121	48 (39.7%)	▲356.9%
Dating & romance scams	$670,903	61	22 (36.1%)	▲49.5%
Threats to life, arrest or other	$363,821	611	18 (2.9%)	▲205.6%
Remote access scams	$268,308	256	31 (12.1%)	▲229.1%
False billing	$234,531	460	48 (10.4%)	▼-0.7%
Classified scams	$133,476	193	77 (39.9%)	▲25.0%
Online shopping scams	$94,598	394	112 (28.4%)	▼-35.6%
Identity theft	$54,235	380	25 (6.6%)	▼-43.8%
Hacking	$50,865	276	13 (4.7%)	▲58.5%
Jobs & employment scams	$21,400	45	3 (6.7%)	▲2,979.1%
Betting & sports investment scams	$16,860	25	5 (20.0%)	▲155.1%
Phishing	$14,172	1,323	12 (0.9%)	▼-24.0%
Travel, prizes and lottery scams	$10,184	116	9 (7.8%)	▼-96.2%
Other scams	$6,975	823	20 (2.4%)	▼-2.7%
Overpayment scams	$6,015	36	4 (11.1%)	▼-29.5%
Rebate scams	$4,350	34	3 (8.8%)	▲4,250.0%
Mobile premium services	$2,500	38	2 (5.3%)	▲8,233.3%
Health & medical products	$1,298	29	8 (27.6%)	▼-15.7%
Psychic & clairvoyant	$1,260	2	1 (50.0%)	No losses in 2020
Pyramid Schemes	$400	5	1 (20.0%)	▼-76.5%
Ransomware & malware	$300	75	1 (1.3%)	No losses in 2020
Inheritance and unexpected money	-	25	0.0%	▼-100.0%
Fake charity scams	-	18	0.0%	▼-100.0%
Total	**$4,417,723**	**5,346**	**463 (8.7%)**	**▲108.0%**

Victoria

Scam type	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in losses since 2020
Investment scams	$39,403,669	2,057	866 (42.1%)	▲91.9%
Dating & romance scams	$12,392,933	684	351 (51.3%)	▲67.0%
Threats to life, arrest or other	$4,817,296	8,423	200 (2.4%)	▼-0.3%
Remote access scams	$4,088,136	4,345	352 (8.1%)	▲39.9%
Identity theft	$3,376,205	6,072	283 (4.7%)	▲244.5%
Online shopping scams	$2,460,811	5,516	1,948 (35.3%)	▲39.9%
False billing	$2,201,105	5,319	451 (8.5%)	▼-26.7%
Classified scams	$1,705,524	2,396	818 (34.1%)	▲0.8%
Phishing	$713,250	19,359	194 (1.0%)	▲3.8%
Pyramid Schemes	$594,165	157	89 (56.7%)	▲4,103.2%
Travel, prizes and lottery scams	$475,086	1,180	65 (5.5%)	▼-12.0%
Rebate scams	$415,952	553	37 (6.7%)	▲63.7%
Hacking	$380,597	3,986	141 (3.5%)	▼-9.4%
Inheritance and unexpected money	$366,930	363	33 (9.1%)	▼-1.9%
Jobs & employment scams	$224,883	718	65 (9.1%)	▲59.5%
Other scams	$135,040	10,711	233 (2.2%)	▲42.3%
Betting & sports investment scams	$110,389	65	28 (43.1%)	▼-81.7%
Psychic & clairvoyant	$106,892	41	17 (41.5%)	▼-4.5%
Overpayment scams	$103,052	508	63 (12.4%)	▼-51.6%
Health & medical products	$87,336	286	64 (22.4%)	▼-95.9%
Ransomware & malware	$60,685	981	14 (1.4%)	▲277.7%
Fake charity scams	$38,018	193	17 (8.8%)	▲12.0%
Mobile premium services	$31,015	686	22 (3.2%)	▼-19.8%
Total	**$74,288,969**	**74,599**	**6,351 (8.5%)**	**▲51.3%**

Western Australia

Scam type	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in losses since 2020
Investment scams	$11,868,515	859	333 (38.8%)	▲148.0%
Dating & romance scams	$2,720,039	244	114 (46.7%)	▲32.5%
False billing	$2,193,645	2,087	177 (8.5%)	▲149.7%
Remote access scams	$1,387,979	1,290	120 (9.3%)	▲300.1%
Classified scams	$884,499	907	312 (34.4%)	▲132.6%
Threats to life, arrest or other	$574,491	2,737	80 (2.9%)	▲129.4%
Online shopping scams	$573,383	1,692	574 (33.9%)	▲23.8%
Phishing	$404,140	6,051	82 (1.4%)	▲109.4%
Identity theft	$357,779	1,889	85 (4.5%)	▲213.0%
Travel, prizes and lottery scams	$221,213	516	26 (5.0%)	▲9.2%
Pyramid Schemes	$171,198	35	17 (48.6%)	▲243.4%
Rebate scams	$145,124	189	12 (6.3%)	▲3,889.1%
Overpayment scams	$136,386	159	23 (14.5%)	▲248.8%
Psychic & clairvoyant	$117,729	25	11 (44.0%)	▲974.3%
Hacking	$114,648	1,261	46 (3.6%)	▼-22.4%
Other scams	$105,796	3,681	89 (2.4%)	▲192.3%
Jobs & employment scams	$72,079	850	22 (2.6%)	▼-70.3%
Inheritance and unexpected money	$31,150	137	8 (5.8%)	▲152.2%
Health & medical products	$25,216	211	29 (13.7%)	▲187.5%
Betting & sports investment scams	$21,335	28	8 (28.6%)	▲3.0%
Fake charity scams	$20,592	75	15 (20.0%)	▲405.7%
Ransomware & malware	$16,900	282	5 (1.8%)	▲125.7%
Mobile premium services	$11,294	211	10 (4.7%)	▼-42.3%
Total	**$22,175,130**	**25,416**	**2,198 (8.6%)**	**▲115.1%**

Appendix 3: Scam Reports from Businesses

Scam type	Reported losses 2021	Number of reports 2021	Number of reports with loss	Percentage change in losses since 2020
False billing	$6,747,148	763	227 (29.8%)	▼-50.1%
Investment scams	$5,100,761	86	20 (23.3%)	▲204.6%
Classified scams	$606,353	207	76 (36.7%)	▲201.8%
Online shopping scams	$335,822	281	97 (34.5%)	▼-32.4%
Identity theft	$174,293	297	21 (7.1%)	▲205.1%
Phishing	$166,635	752	27 (3.6%)	▲220.1%
Remote access scams	$90,504	115	8 (7.0%)	▲778.7%
Hacking	$49,754	166	10 (6.0%)	▲84.9%
Rebate scams	$41,200	23	2 (8.7%)	▲100.7%
Overpayment scams	$38,083	43	6 (14.0%)	▲64.1%
Ransomware & malware	$31,350	54	3 (5.6%)	▲683.8%
Other scams	$13,872	542	30 (5.5%)	▼-12.9%
Fake charity scams	$13,296	56	10 (17.9%)	▲265.2%
Jobs & employment scams	$11,175	50	6 (12.0%)	▼-93.8%
Health & medical products	$9,205	16	1 (6.3%)	▼-99.6%
Threats to life, arrest or other	$5,965	90	4 (4.4%)	▼-89.4%
Betting & sports investment scams	$4,000	2	2 (100.0%)	No losses in 2020
Travel, prizes and lottery scams	$100	42	1 (2.4%)	No losses in 2020
Dating & romance scams	-	2	-	▼-100.0%
Pyramid Schemes	-	1	-	▼-100.0%
Inheritance and unexpected money	-	23	-	▼-100.0%
Mobile premium services	-	13	-	▼-100.0%
Total	**$13,439,516**	**3,624**	**551 (15.2%)**	**▼-27.0%**

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.

Flubot

Flubot is malicious software (malware) that sends text messages to both Androids and iPhones. The content of the text messages varies but all messages contain a link. The link may ask the recipient to download an app to track or organise a time for a delivery, hear a voicemail message, or view photos that have been uploaded. Downloading the app downloads Flubot onto the user's device.

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.

Hope Business/Wonderful World scams

These scam businesses were the first of their kind for which Scamwatch received significant reporting. In these scams, victims are encouraged to sign up for a 'work from home' job with the premise of earning a significant amount of money. The specifics of the job vary but the scam always moves to include the transfer of the victim's own money to bank accounts specified by the scammers. The scams often involve professional-seeming online support, live chats and social media discussion forums with other people participating in the scheme. Many of the other users are in fact placed there by the scammer.

In the Hope Business scam, victims thought they were purchasing items from online merchants to increase their traffic on online marketplaces but in fact were sending money directly to the scammers' bank accounts. Initially, victims would receive a full refund of the money they sent plus a 'commission'. Victims received referral bonuses for signing up friends and family members. Scammers eventually stopped allowing participants to withdraw any funds and encouraged them to send more money to allow funds withdrawal.

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 and unexpected money scams

These scams offer victims the false promise of money via an inheritance or other unexpected opportunity to claim a large sum of money in their name 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 2-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.

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

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.

Pet scams

Scammers create a fake website claiming to sell in-demand dog breeds or other animals. 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 animal.

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.

Ponzi scheme

Ponzi schemes are investment scams relying on referrals of new victims. Initially, participants who have deposited money received promised profits or commissions on their investment and are able to withdraw funds. Eventually the scammers stop allowing victims to withdraw funds.

Psychic and clairvoyant scams

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

Pyramid schemes

Pyramid schemes are illegal and risky get-rich-quick schemes. In a typical pyramid scheme, a member pays to join. If the only returns from a scheme are entirely or substantially reliant on the member convincing other people to join, 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.

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, prizes and lottery scams

Travel, prizes and lottery scams are a combination of the previous categories of 'travel prize scams', 'scratchie scams' and 'unexpected prize and lottery scams'. All of these categories involved attempts to trick people into parting with their money to claim a free reward. These rewards come either from a competition or lottery they had not entered, or through a winning freely provided scratchie for a holiday or large sum, often sent via the mail.

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.

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.

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 gift cards and Steam Wallets

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

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.


ACCC
AUSTRALIAN COMPETITION
& CONSUMER COMMISSION