Australian Government

National Anti-Scam Centre

# Targeting scams

## Report of the National Anti-Scam Centre on scams activity 2023

April 2024

## Acknowledgment of country

The ACCC acknowledges the traditional owners and custodians of Country throughout Australia and recognises their continuing connection to the land, sea and community. We pay our respects to them and their cultures; and to their Elders past, present and future.

Australian Competition and Consumer Commission
Land of the Ngunnawal people
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601



ACCC 04/24_24-23

www.accc.gov.au

# Contents

# Foreword

This is the first annual report on scams activity released by the National Anti-Scam Centre since it was established on 1 July 2023. This report provides insight into scams reported by Australians in 2023 and highlights the impact of government and private sector initiatives to combat scams.

Scammers are opportunistic and agile financial criminals. They use sophisticated technology and psychology to steal Australians' money and personal information.

In early 2023, it was anticipated Australians would report losing significantly more than the **$3.15 billion reported in 2022**[1] given the year-on-year growth in financial losses and increasing scam activity globally. However, based on data from Scamwatch, ReportCyber, the Australian Financial Crimes Exchange, IDCARE, and the Australian Securities and Investments Commission the **combined losses** reported in **2023 were $2.74 billion** (a 13% decrease in losses).

In 2023, Australians made over **601,000 scam reports** compared to the 507,000 in 2022 (an 18.5% increase in reports). It is encouraging to see the amount of financial loss decreased despite the increase in scam reports. This is a result of the concerted efforts of government (including through the establishment of a National Anti-Scam Centre), the private sector, law enforcement, and community organisations. These results demonstrate that coordinated scams prevention, detection and response initiatives can stem the flow of funds to criminals and protect Australians.

While we are cautiously optimistic that our combined efforts will see this downward trend in scam losses continue, we know that behind the losses remain real people who have lost money, often their life savings, to scams. Trust, relationships, and well-being are also negatively impacted.

This is why we remain committed to identifying and removing weak links that scammers could otherwise exploit.

Over the next two years the National Anti-Scam Centre will continue a technology build that will coordinate intelligence and distribute information to those who can act on it – such as banks to freeze accounts, telcos to block calls or SMSs and digital platforms to take down websites or accounts. We will partner with other organisations to tackle the most harmful scams and we will continue to raise scams awareness with the people who are most at-risk.

While cooperation can achieve a great deal, it is not enough. We need all parties at the table – not just the volunteers. This is why we continue to work with Treasury in its development of a Scams Code Framework with mandatory and enforceable obligations on banks, telecommunications providers, and digital platforms.

This important work cannot be done without the significant efforts of the organisations who engage with us every day. This report is a testament to their valued contributions. We also acknowledge the efforts of consumer advocates, financial counsellors and victim services that support Australians to recover from the emotional and financial impact of scams.

Our sincere thanks to those working towards our common goal of making Australia a much harder target for scammers.

Catriona Lowe
Deputy Chair, ACCC

1 ACCC, *Targeting scams: Report of the ACCC on scams activity 2022* (April 2023).

# About the National Anti-Scam Centre

The Australian Government established the National Anti-Scam Centre in the Australian Competition and Consumer Commission (ACCC) on 1 July 2023. The National Anti-Scam Centre and its partners in government, industry, law enforcement, and consumer organisations are collectively committed to making Australia a harder target for scammers and reducing the devastating financial and emotional harm caused by scams.[2]

The National Anti-Scam Centre was a key part of the Government's commitment to fight scams. In the 2023–24 budget the Government provided $86.5 million in funding to:

- establish a National Anti-Scam Centre as a world leading partnership between Government agencies and industry
- establish Australia's first SMS Sender ID registry to help prevent scammers imitating trusted industry or government brands in text messages
- boost work by the Australian Securities and Investments Commission to identify and take down investment scam websites.

The National Anti-Scam Centre has 3 key domains of activity:

- collaboration (technology and intelligence sharing)
- disruption
- awareness and protection.

### Collaboration

The National Anti-Scam Centre is developing technology to facilitate fast intelligence gathering and information sharing through an Actionable Scam Intelligence Service. This new digital capability will enable the near real time exchange of scam intelligence to organisations that can block and stop scams. In the second half of 2024, more government agencies and key businesses will be connecting and exchanging data through the National Anti-Scam Centre.

### Disruption

The National Anti-Scam Centre is scaling up a website takedown capability to ensure that scam websites are taken down before they cause widespread harm. The Scamwatch reporting service is being improved to make it easier to report a scam so that from July 2024 Australians can quickly report a scam website or scam advertisement that can be shared with a takedown service or digital platform and blocked.

Businesses, community organisations, law enforcement and technology services will have opportunities to work with the National Anti-Scam Centre to develop tools and processes to target specific scams. They will also be able to access scam information relevant to them through a Partner Portal. Fusion cells run by the National Anti-Scam Centre are bringing together expertise and information to inform innovative solutions. The outcomes of the first fusion cell focussing on investment scams are discussed further below. The National Anti-Scam Centre is partnering with the Australian Financial Crimes Exchange on a scam intelligence loop to further support sharing of actionable intelligence with those best placed to act on that intelligence to disrupt scams.

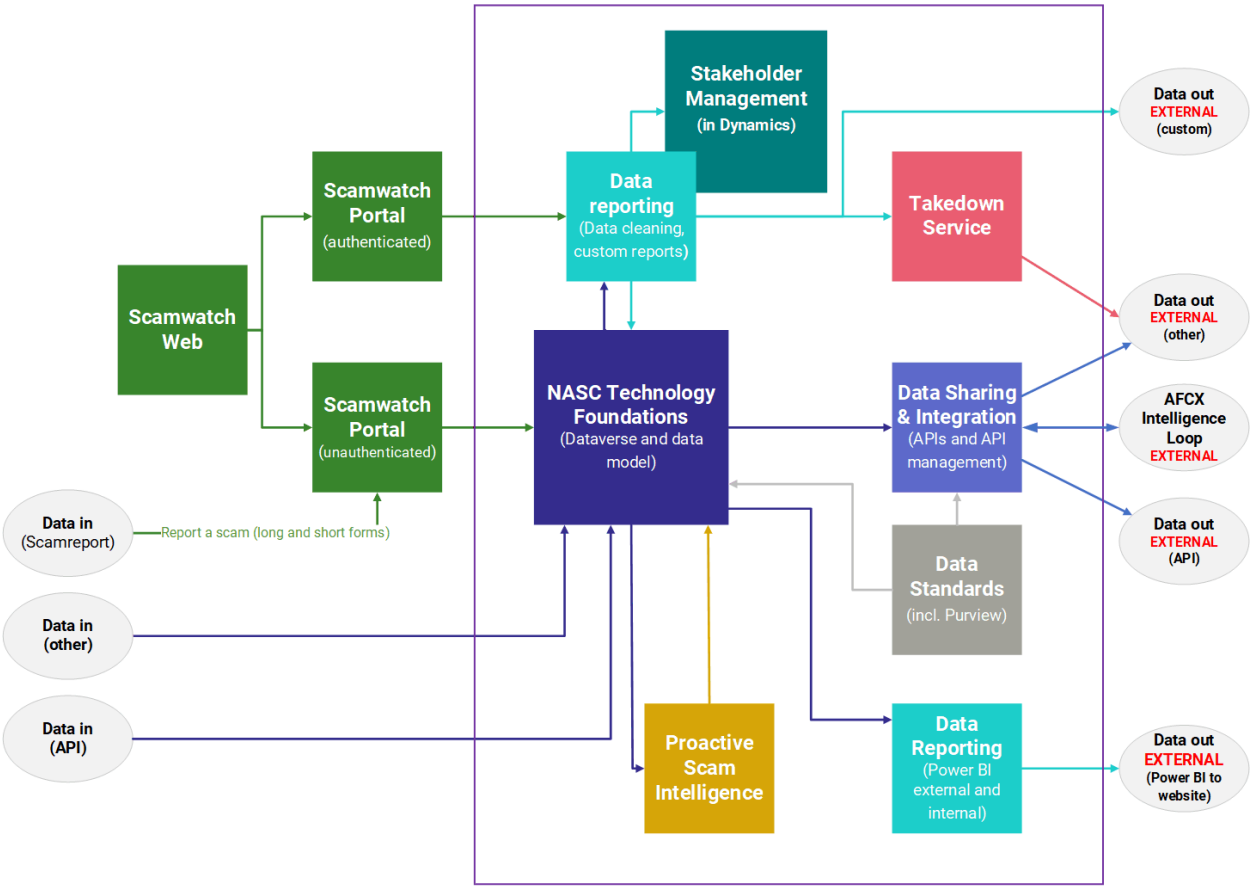
2 The National Anti-Scam Centre publishes updates each quarter available at: https://www.accc.gov.au/about-us/publications/serial-publications/national-anti-scam-centre-quarterly-update.

### Awareness and protection

With these changes, reporting and support services will also be more integrated. Victims of scams will have faster access to the support they need and confidence that information is being shared with law enforcement. Australians will also benefit from more frequent and consistent information about scams targeting them and how to avoid them. The National Anti-Scam Centre will coordinate scam awareness campaigns to ensure consistent messaging and undertake effective outreach with at-risk communities.

By harnessing expertise across all parts of the ecosystem and working together, the National Anti-Scam Centre will be a world leading initiative that makes Australia less attractive to scammers and protects citizens from their criminal enterprises.

**Figure 1:** National Anti-Scam Centre data and technology model



# At a glance

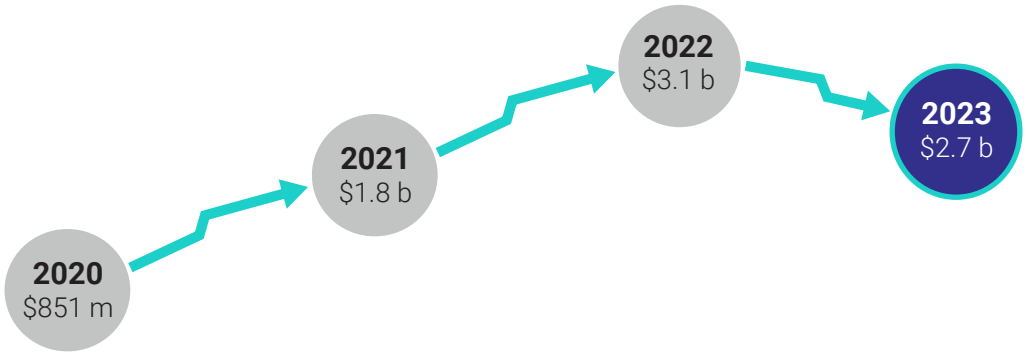
## Losses

**$2.74 billion in losses**

Total combined losses reported to Scamwatch, ReportCyber, IDCARE, Australian Financial Crimes Exchange (AFCX) and Australian Securities and Investments Commission (ASIC)

**601,000+**
**scam reports**
**▲18.5%**

## Combined losses over last 4 years




## Top 5 scams by loss (combined data)

| Investment | Remote access | Romance | Phishing | Payment redirection |
|---|---|---|---|---|
| **$1.3 b** | **$256.0 m** | **$201.1 m** | **$137.4 m** | **$91.6 m** |

## Successful scam disruption pilots

Government, law enforcement, banks, telcos and digital platforms contributed to:

| Sharing data and intel | Scam websites and ads | Scam diversion and victim support | Scam payments |
|---|---|---|---|
| • Data sharing of scam phone numbers and bank accounts to disrupt scams.<br>• Banks using data and intel to enhance detection. | • Over 3,500 investment scam websites taken down. | • Diverting victims who call scam numbers to warnings and assistance.<br>• Automatic referral of scam victims to IDCARE. | • Stopping payments to crypto exchanges used by scammers.<br>• Stopping scam transactions through added frictions.<br>• First bank payee verification. |

# Key statistics

Australians report scams to many organisations depending on the type of scam and level of awareness about the role of reporting agencies and private organisations. The National Anti-Scam Centre has commenced work to bring together the most common data sources to provide a more accurate picture of the level of scam activity in Australia. This work is ongoing over the next 12 months and will lead to a stronger evidence base to better target initiatives to limit the harm caused by scams. The National Anti-Scam Centre and its partners continue to encourage Australians to report scams. Reports help identify trends which in turn can alert others and support disruption activity.

This report incorporates data from the following sources: Scamwatch, ReportCyber, Australian Financial Crimes Exchange (AFCX), IDCARE, and the Australian Securities and Investments Commission (ASIC). More detailed analysis and observations of Scamwatch data is contained in **Appendix 1**. Further information about data sources, adjustments and data cleaning is contained in **Appendix 2**.

In 2022, Australians made over 500,000 reports and reported combined losses of over $3.1 billion. In 2023, Australians made a combined[3] total of over **601,000 reports** (an 18.5% increase), with reported losses of over **$2.74 billion in 2023** (a 13% decrease).

Table 1 below sets out the breakdown of combined scam reports and losses including some adjustments to account for duplication.

**Table 1:** Combined losses and reports

| Organisation | Reports | Losses (m) |
|---|---|---|
| **Scamwatch** | 301,778 | $476.8 |
| **ReportCyber** | 69,393 | $793.5 |
| **AFCX**[4] | 217,284 | $1,182.4 |
| **ASIC** | 1,373 | $87.8 |
| **IDCARE** | 30,553 | $366.7 |
| **Adjustments** | -18,578 | -$165.3 |
| **TOTAL** | **601,803** | **$2,741.9** |

3 Data sources: Scamwatch, ReportCyber, AFCX, IDCARE, and ASIC.

4 AFCX included data for National Australia Bank (NAB), Australia and New Zealand Banking Group (ANZ), Commonwealth Bank of Australia (CBA), Westpac, Bendigo Bank, Macquarie Bank, Customer Owned Banking Association (COBA) and Cuscal. COBA and Cuscal contribute less than 2% to the totals for the AFCX.

Table 2 below sets out the top 5 scam categories by financial loss and highlights the decrease in reported losses to investment scams from $1.5 billion in 2022 to $1.3 billion in 2023.

**Table 2:** Combined losses (m) by category[5]

| Scam type | Scamwatch | ReportCyber | AFCX | ASIC | IDCARE | Adjusted total[6] | 2022 total[7] |
|---|---|---|---|---|---|---|---|
| **Investment** | $291.9 | $393.4 | $409.8 | $85.1 | $216.4 | $1,300.0 ▼ | $1,500.0 |
| **Remote access** | $15.5 | $1.6 | $235.4 | N/A | $5.6 | $256.0 ▲ | $229.2 |
| **Romance** | $34.3 | $66.1 | $77.9 | N/A | $48.5 | $201.1 ▼ | $210.2 |
| **Phishing** | $25.9 | $0.1 | $90.2 | N/A | $58.0 | $137.4 ▼ | $157.6 |
| **Payment redirection** | $16.2 | $75.4 | N/A | N/A | N/A | $91.60 ▼ | $224.9 |
| **Other**[8] | $92.9 | $256.9 | $369.2 | $2.7 | $38.3 | $755.9 ▼ | $784 |

### Unreported losses

Not all Australians report scams. Despite the existence of several reporting platforms, we know the extent and impact of scams is under-reported and some cohorts[9] are markedly underrepresented in official reporting figures. The National Anti-Scam Centre is conducting more work to encourage reporting from all communities, and to reduce the stigma of scams so that more people are comfortable to report them.

The Australian Bureau of Statistics (ABS) Personal Fraud data[10] shows that in the 2022–23 financial year, 2.5% of Australians (514,300) experienced a scam. A person is considered to have experienced a scam if they have responded to a scam and sought further information, provided money or personal information, or accessed links associated with the scam. 69% of people who experienced a scam notified (or were notified by) an authority. This means that approximately 30% of people who experienced a scam did not report it. It is likely many of those who did not report incurred a small or no direct financial loss and consequently this under reporting does not mean the $2.74 billion in reported losses would be 30% higher if those people reported.

There are also Australians who lost money to a scam in 2023 and did not know they were being scammed. Investment and romance scams are long term scams where scammers maintain relationships for months or years before the person is aware it is a scam. They may be detected only after a bank account is identified as containing scam funds and banks or law enforcement identify victims who have sent money to the scam bank account.

5 Totals for each organisation may differ slightly from totals in Table 1 due to rounding of scam type in Table 2. Organisations label scam types differently however efforts have been made to align categories as much as possible.

6 These totals have been adjusted to recognise there may be some duplication in the data sets. Further information on this is available in Appendix 2.

7 Data source: *Targeting scams: Report of the ACCC on scams activity 2022*; Table 2.2.

8 'Other' refers to all other scams which were not part of the top 5 scams causing the highest losses.

9 Research by Fiftyfive5 (part of Accenture) commissioned by The Treasury in 2023 indicates people from First Nations communities and Culturally and Linguistically Diverse communities may be less likely to report scams. It found First Nations people are notably less likely to trust banks and government.

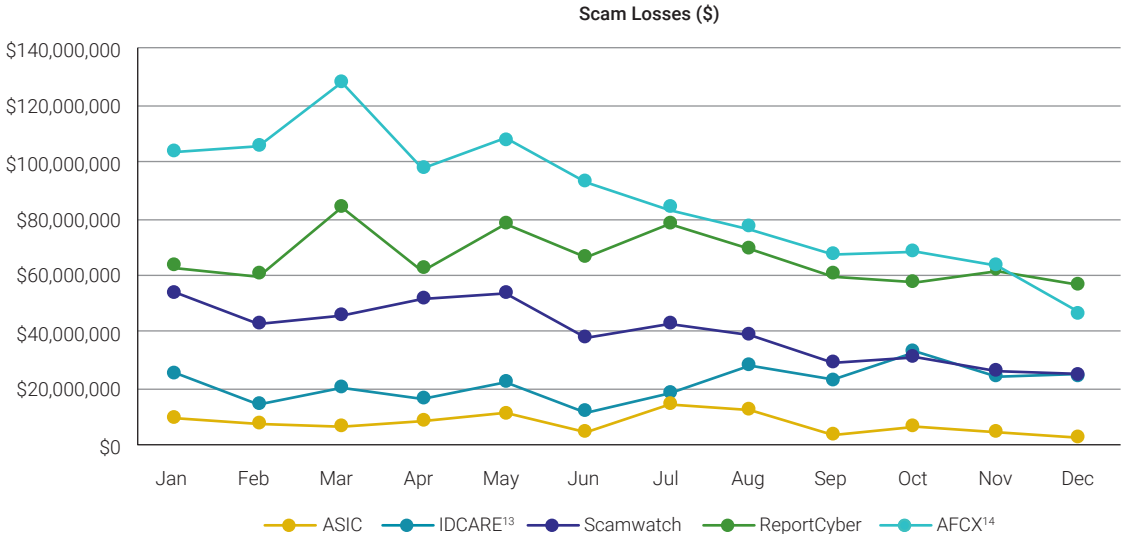
10 Reference: https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release.

Reporting scams provides critical intelligence for the National Anti-Scam Centre and its partners to detect and disrupt scam activities. As one of the focuses of the National Anti-Scam Centre has been increasing consumer awareness of scams and how to report them, it is likely the number of unreported scams is decreasing. This is supported by data showing that while reported losses have decreased, the number of scam reports has increased. The National Anti-Scam Centre will continue to encourage consumers to report scams, which will drive up the number of reports.

# Observations on declining losses in 2023

Financial losses decreased in the second half of 2023 by 21% compared to the first half of the year.[11] Several organisations observed a downward trend, despite some fluctuations in reported losses throughout the year for organisations like IDCARE.[12] The most significant decreases were evident in AFCX financial transaction data as demonstrated in Figure 2 below.

**Figure 2:** Scam losses by month for Scamwatch, ReportCyber, AFCX, ASIC and IDCARE




When all sources from Figure 2 are added together, a consistent trend emerges of a 21% reduction in scams losses in the latter half of 2023 compared to the first.

11 The combined loss data was analysed from Jan–June and July–Dec. July–Dec combined losses across all data contributors were 21% less than Jan–June.

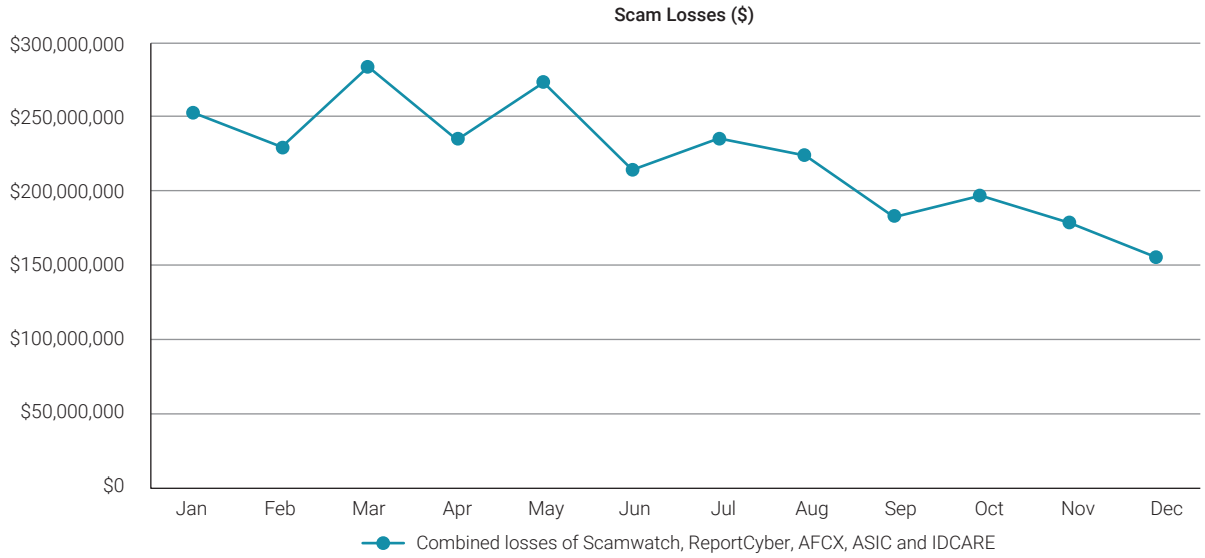
12 IDCARE receives a high number of referrals from other organisations compared to direct reporting from the public.

13 The ACCC commenced an automated referral process to IDCARE from May 2023, so ACCC referrals have been removed from IDCARE data in this graph. Other duplicates with the AFCX and ReportCyber have not been removed in this graph. High-value losses to ReportCyber of over $1m have been reviewed and unreliable reports removed.

14 Large outliers in May 2022 were removed from AFCX losses for this chart; they were not removed from total loss figures in Table 1 as they are verified losses.

Figure 3 shows the decrease when data points in Figure 2 are combined.

**Figure 3:** Scam losses by month for all sources (combination of trendlines from Figure 2)




The reduction in reported losses is likely the result of a range of complex factors. However, key Government and industry initiatives in 2023 appear to have led to significant decreases in reported losses for investment scams and payment redirection scams, as well as smaller decreases for romance scams and phishing scams. These initiatives are outlined below.

## Launch of the National Anti-Scam Centre

The National Anti-Scam Centre was launched in July 2023.

A key aim of the National Anti-Scam Centre is to enable the sharing of scams intelligence across government, law enforcement and the private sector to enable near real time identification of scam phone numbers, bank accounts and social media accounts – leading to timely intervention when scammers try to contact potential victims, or when victims unknowingly attempt to make payments to scammers.

The increase in collaboration between government, law enforcement and industry including information sharing arrangements with the AFCX and other organisations has likely prevented financial loss for Australians. As the National Anti-Scam Centre finalises the technology build to enable real time data sharing of scams between key organisations, it is expected to increase capability to prevent, detect, disrupt, and respond to scams earlier.

The National Anti-Scam Centre and ASIC led investment scam fusion cell resulted in disruption initiatives detailed below.

The National Anti-Scam Centre also worked with State and Federal police to provide information and referrals for scam investigations in Australia and overseas and partnered on scams disruption initiatives.

## Announcement of a Scams Code Framework

In late 2023, the Government released consultation for a mandatory Scams Code Framework.

The impact of proposed regulation is likely to have motivated businesses to proactively address underlying risks and may have led to an increased focus by potential regulated entities on scam prevention initiatives.

## Bank action on cryptocurrency exchanges

AFCX data from the end of the 2022–23 financial year indicated nearly half of all scam losses were processed through cryptocurrency exchanges.[15] From mid–2023, Westpac, CBA, NAB and ANZ and other banks have taken steps to limit transactions to 'high risk' cryptocurrency exchanges.

This has likely reduced both direct scam payments particularly for investment scams, as well as reduced the incentives for some criminals to operate in Australia as transferring financial crime proceeds becomes more difficult.

## ASIC's website takedown service

As part of the Government's 'Fighting Scams' initiative, ASIC established an investment scam website takedown capability and worked with the National Anti-Scam Centre and partners through the investment scam fusion cell to identify and remove websites hosting malicious phishing and investment scam information.

During the investment scam fusion cell, over 3,500[16] websites were taken down or made inaccessible to Australians.

ASIC also launched a new investor alert list[17] in November 2023 which provides warnings to potential investors about scam businesses and websites.

## 'Call Stop' initiative

Optus, along with banking members of the AFCX developed a 'Call Stop' initiative[18] to counter bank impersonation SMS scams by diverting Australians who call back a number in a scam SMS message to a scam warning message. The National Anti-Scam Centre worked with investment scam fusion cell participants to expand this initiative to divert confirmed investment scam numbers.

Diverting telephone contact can play a crucial in de-legitimising scammers operating complex investment scams that result in very high (~$264k) average losses.

During the fusion cell period, 113 calls were diverted, potentially saving millions of dollars in scam losses.

15 AFCX data as reported in: https://www.afr.com/companies/financial-services/crypto-platforms-a-getaway-for-half-of-scam-proceeds-20230810-p5dvhc.

16 https://asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-037mr-asic-shuts-down-nearly-3-500-scam-websites-steps-up-surveillances-in-push-to-protect-consumers/.

17 https://moneysmart.gov.au/check-and-report-scams/investor-alert-list.

18 https://www.optus.com.au/about/media-centre/media-releases/2023/07/optus-call-stop-to-fight-off-sms-scams.

## Scam indicator tool and payment prompts

In mid–2023, Telstra and CBA announced[19] a pilot program to help detect and prevent phone scams for joint customers. Scam Indicator enables CBA to confirm if a customer is on a phone call while transacting with the CBA which is an indicator that a scam could be occurring, potentially doubling the bank's success rate of phone scam detection.

The NAB also introduced payment prompts in digital banking to help customers see potential red flags leading to customers saving more than $50 million worth of payments to suspected scammers in eight months.[20] Similarly, a number of banks introduced additional security controls to detect fraud and scams throughout 2023.[21]

## Telecommunications initiatives

As part of the Government's 'Fighting Scams' initiative, the Australian Communications and Media Authority (the ACMA) is implementing an SMS sender ID registry. The registry will protect the alphanumeric message headers (such as 'ATO', 'MyGov' or 'NAB') of brands and government agencies from SMS impersonation. In December 2023, the ACMA commenced a pilot phase of the registry, which will consolidate existing sender ID protections with some well-known brands and agencies.

Pursuant to the Telco Code,[22] between October and December 2023, telecommunications providers reported blocking over 246.7 million scam calls and over 106.7 million scam SMS.[23]

During 2023, the ACMA directed multiple telecommunication providers to comply with the Telco Code. Once a provider is directed to comply, future enforcement – including civil penalties – is easier if breaches are found.

## Payee verification technology and the Scam Safe Accord

In 2023, several banks announced[24] the roll out of confirmation of payee technology. Confirmation of payee helps reduce scams by ensuring people can confirm they are transferring money to the person they intend to. This can reduce the number of people impacted by payment redirection scams and impersonation scams.

In November 2023, the Australian Banking Association and the Customer Owned Banking Association announced[25] a Scam Safe Accord between community owned banks, building societies, credit unions and commercial banks with a set of anti-scam measures to apply across the industry.

The Accord outlines a $100 million investment by industry in a new confirmation of payee system to be rolled out across all Australian banks. When implemented across all banks, confirmation of payee will have a significant impact in driving down scam losses.

19 https://www.telstra.com.au/exchange/keep-snitching-on-scammers--how-our-new-7226-reporting-number-is.

20 https://news.nab.com.au/news/nab-payment-alerts/.

21 https://www.itnews.com.au/news/anz-plus-to-add-scam-safe-features-602287 and https://www.mpamag.com/au/news/general/westpac-introduces-new-scam-prevention-features/458337.

22 ACMA registered Reducing Scam Calls and Scam SMS Industry Code.

23 https://www.acma.gov.au/publications/2024-02/report/action-telco-consumer-protections-october-december-2023.

24 https://www.commbank.com.au/support/security/namecheck.html and https://www.westpac.com.au/about-westpac/media/media-releases/2023/5-March/.

25 https://www.ausbanking.org.au/new-scam-safe-accord/.

## Next Steps

Key activities planned to drive down financial losses to scams in 2024 include:

- The development of mandatory and enforceable obligations requiring banks, telecommunications providers, and digital platforms to prevent, detect, disrupt, and respond to scams.
- The National Anti-Scam Centre will pilot the take down of a broader range of scam websites and develop a simple process for Australians to report scam websites and advertisements.
- A second fusion cell to disrupt a specific type of scam.
- The National Anti-Scam Centre will have 10 partners participating in data sharing arrangements and use its actionable intelligence service to disrupt scams and issue real time scam alerts.
- The banking sector will progress a confirmation of payee system which is expected to drive down losses to payment redirection scams and impersonation scams.
- The ACMA will expand the SMS Sender ID Registry pilot focusing on brands that have been the target of impersonation scams.
- ASIC will takedown more websites by working with the National Anti-Scam Centre to automate referrals of investment scam websites for takedown.
- Data sharing between the National Anti-Scam Centre and the AFCX anti-scam intelligence loop will lead to faster action to block scam bank accounts and better intelligence to inform detection and blocking of scams across participating organisations.
- Working with the private sector, community organisations and support services, the National Anti-Scam Centre will raise awareness about scams through activities such as Scams Awareness Week (August 2024), and education and community outreach activities. This will include empowering at-risk groups to recognise and avoid scams and increase reporting behaviour.

# Appendix 1: Scamwatch data and observations

## Report and loss statistics

Scamwatch is a rich data source that includes information about scam types, victims affected, communication and payment methods used by scammers, and some information about the backgrounds of reporters and victims. This data enables further exploration of trends in scam categories, methodologies, and impacted communities. However, this data is a subset of total losses and reports and therefore caution should be exercised in making definitive statements about total losses based on Scamwatch data alone.

Scamwatch received 301,778 reports in 2023 (a 26.1% increase compared to 2022). Over 29,000 reports (9.7%) involved a financial loss. Reported losses declined for the first time in 7 years with total reported losses of $477 million in 2023 (a 6.1% decrease from 2022).[26] The median loss in 2023 was $500, which is a 50% decrease from the median loss of $1000 in 2022.[27]

### Losses reported to Scamwatch

Scamwatch data shows a decrease in reported losses in the second half of 2023. The scam prevention and disruption initiatives outlined earlier are likely to have contributed to this trend.

**Table 3:** Scamwatch data, losses by month, 2022 compared with 2023

| Month | 2022 Losses (m) | 2023 Losses (m) | 2022 to 2023 % change [28] |
|---|---|---|---|
| January | $33.1 | $53.3 | 61.1% ▲ |
| February | $37.9 | $43.2 | 14.0% ▲ |
| March | $34.4[29] | $45.3 | 31.7% ▲ |
| April | $37.1 | $51.5 | 38.6% ▲ |
| May | $51.3 | $53.3 | 3.9% ▲ |
| June | $37.6 | $38.1 | 1.3% ▲ |
| July | $42.8 | $42.4 | -1.0% ▼ |
| August | $44.7 | $38.6 | -13.7% ▼ |
| September | $43.5 | $29.0 | -33.3% ▼ |
| October | $49.2 | $31.3 | -36.4% ▼ |
| November | $51.7 | $25.7 | -50.3% ▼ |
| December | $43.3 | $25.1 | -42.0% ▼ |

26 For accuracy in reporting comparative data, an outlier report was removed from the 2022 data. The 2022 financial loss total used for comparative purposes was $507.9 million.

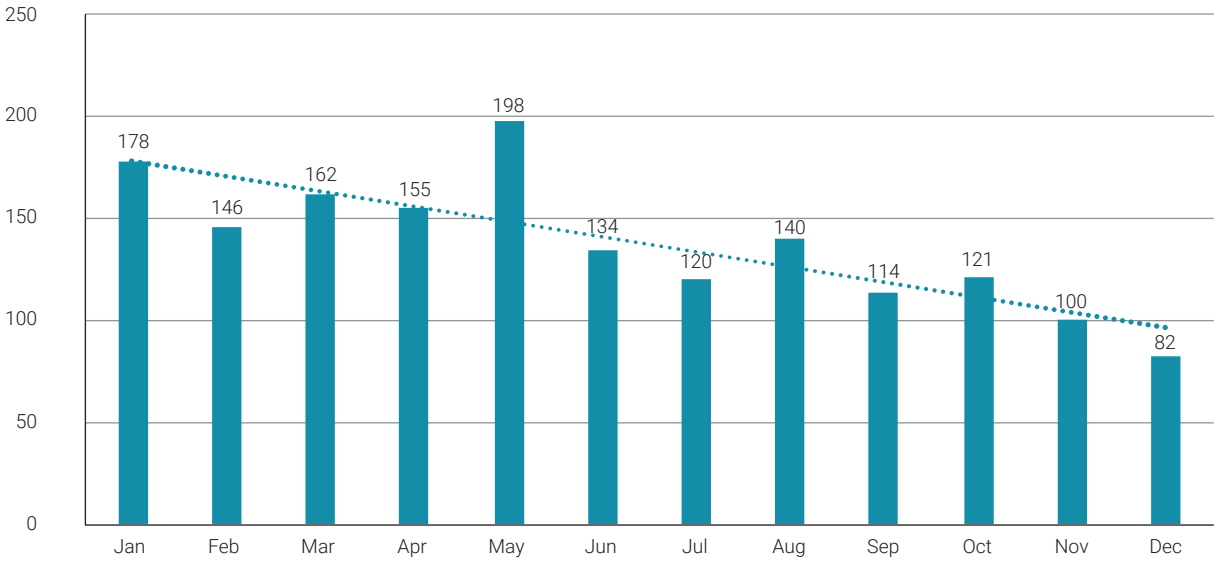
27 All medians calculated in this appendix are based on reports with a financial loss.

28 Percentages were calculated from the actual values and not the rounded values presented in the table.

29 There was a high loss outlier report in March 2022. It has been removed to avoid artificially inflating a large comparative decrease in losses.

Closer analysis identified an overall decrease in the number of Scamwatch reports of losses of $50,000 or higher. Figure 4 below presents the number of reports each month where the loss amount reported was $50,000 or higher. This is consistent with fusion cell and industry disruption initiatives focussed on high loss investment scams and improved scam detection techniques by banks in relation to large transactions.

**Figure 4:** Number of reports in 2023 by month, where losses per report were $50,000 or higher




## Scam categories reported to Scamwatch

**Table 4:** Top 10 scam categories in 2023 by highest losses

| Category | Losses (m) | Number of reports | % change in losses from 2022 |
|---|---|---|---|
| **Investment scams** | $291.9 | 8,159 | -7.8% ▼ |
| **Romance scams** | $34.3 | 3,652 | -15.6% ▼ |
| **False billing** | $28.0 | 39,588 | 10.6% ▲ |
| **Phishing** | $25.9 | 108,636 | 5.2% ▲ |
| **Jobs scams** | $24.4 | 4,831 | 151.2% ▲ |
| **Remote access scams** | $15.5 | 8,975 | -28.6% ▼ |
| **Online shopping**[30] | $14.9 | 32,886 | -15.7% ▼ |
| **Threats based scams**[31] | $13.9 | 5,607 | -0.5% ▼ |
| **Identity theft** | $8.6 | 19,896 | -19.9% ▼ |
| **Rebate scams** | $8.2 | 7,125 | 151.4% ▲ |

Although decreasing from 2022, investment scams continued to be the source of most reported losses in 2023, at $292 million compared to the $316.5 million in 2022 (a 7.8% decrease). The National Anti-Scam Centre's investment scam fusion cell, ASIC's website takedown service and bank-initiated frictions among other things contributed to decreases in reports and losses in the second half of 2023. In December 2023, Scamwatch received 436 reports about investment scams compared to 733 reports in December 2022 (a 40.5% decrease).

30 Online shopping includes 'classified scams'.

31 Category on Scamwatch is 'threats to life, arrest or other'.

In 2023, egregious scams targeting culturally and linguistically diverse (CALD) communities, new migrants, and international students were at similar levels to 2022 contributing to a total of $13.9 million in reported losses for threat-based scams. Research suggests CALD communities have a reduced ability to detect scams and protect themselves and this may explain the increased susceptibility to some scams.[32] This is further exacerbated by the challenges in reaching some communities with traditional scam prevention approaches.

There was an increase in reports and losses to job scams which tend to impact CALD communities and those looking for part-time work or to supplement their income and ease cost of living pressures. In 2023, losses to job scams increased by 151.2% to $24.4 million. These scams attempt to lure younger Australians and digital natives by using gamification in their methodology. For example, they provide a tiered 'level-based' reward system with promised payouts increasing proportionally with the amount invested and/or the number of other people the victim refers into the system. Susceptibility may be higher for younger Australians where this methodology may not appear as unusual or a 'red flag.' These scam methodologies demonstrate the agility of scammers to capitalise on local conditions such as economic circumstances.

The other significant increase in reported losses was to rebate scams at $8.2 million in 2023 (a 151.4% increase). This was caused by increases in money recovery scams and discount bill scams. Over the last few years there has been an increase in money tracing and recovery services. Some of these services are follow up scams but others are services that charge victims large amounts of money to analyse the scam and attempt to recover money or cryptocurrency. In most instances they are unable to recover the money. Unfamiliarity with digital currencies may lead more victims to believe these services offer good prospects of financial recovery – but this is rarely the case.

## Contact methods reported to Scamwatch

**Table 5:** Contact methods by loss and reports[33]

| Contact Mode | 2022 losses (m) | 2023 losses (m) | 2022 reports | 2023 reports |
|---|---|---|---|---|
| **Phone call** | $141.0 | $116.0 ▼ | 63,816 | 55,418 ▼ |
| **Social media**[34] | $80.2 | $93.5 ▲ | 13,427 | 17,542 ▲ |
| **Email** | $77.3 | $80.0 ▲ | 52,159 | 85,941 ▲ |
| **Internet** | $73.5 | $69.7 ▼ | 13,692 | 17,568 ▲ |
| **Mobile apps** | $71.7 | $64.8 ▼ | 10,057 | 8,101 ▼ |
| **In person** | $30.6 | $21.5 ▼ | 2,186 | 3,614 ▲ |
| **Text message** | $28.5 | $26.9 ▼ | 79,835 | 109,621 ▲ |

Australians made more reports to Scamwatch in 2023 than any other year with over 301,700 reports made. Reports peaked at 29,000 in each of February and March largely driven by significant increases in phishing scam reports such as toll scams and government impersonations.[35] In December reports decreased to just over 21,000.

Text message was the most reported contact method in 2023 with 109,621 reports (37.3% increase from 2022).

32 Fiftyfive5, *Supporting Australians to Combat Scams*, research commissioned by The Treasury in 2023.

33 This table excludes mail, other and fax which were each $3m or less in losses and under 3,000 reports.

34 This contact method is called social networking/online forums on the Scamwatch website.

35 Over 10,000 phishing scam reports received in both February and March 2023.

Reports about scam calls decreased 13.2% to 55,418, however scam calls nevertheless resulted in the highest reported losses at $116 million, a 17.7% decrease from the $141 million in 2022.

Scams where contact occurred via social media[36] resulted in the second highest in reported losses, increasing by 16.5% to $93.5 million. There was also a 30.6% increase in reports about scams on social media. Many job scams and investment scams rely on advertisements and posts on social media as well as direct engagement using WhatsApp. With many disruption initiatives focused on phone and SMS it is expected that reports of losses and scams via social media will increase. This highlights the need for digital platforms to take proactive steps to disrupt scammer misuse of their platforms.

Scams by email also increased from 52,159 reports in 2022 to 85,941 reports in 2023 (64.8% increase). While there have been several initiatives in 2023 focused on phone scams and scam websites, there has been less attention on email scams. This may mean scammers are increasing the use of email as a contact method.

## Payment methods reported to Scamwatch

The 2 most common payment methods used by scammers are bank transaction and cryptocurrency.

- Bank transfer was the most reported payment method with 12,252 reports totalling $212.9 million in reported losses. This is consistent with 2022.
- 3,195 reports involved cryptocurrency as the payment method with $171.1 million reported lost (an increase of 6.5% from 2022).
- Payment by credit card decreased 14% with $10.4 million reported lost.

To address the use of cryptocurrency in scams, the National Anti-Scam Centre will continue engagement with digital exchanges to share actionable intelligence over the coming year. The Scamwatch form has been updated to collect better intelligence (wallet addresses) to combat scams.

## Observations on Scamwatch report demographics

Information about the impact of scams on parts of the population that face greater challenges reporting or recovering from a scam is important to assist government, community organisations, private sector, and support services to develop effective scam prevention initiatives. The data below highlights opportunities for more effective:

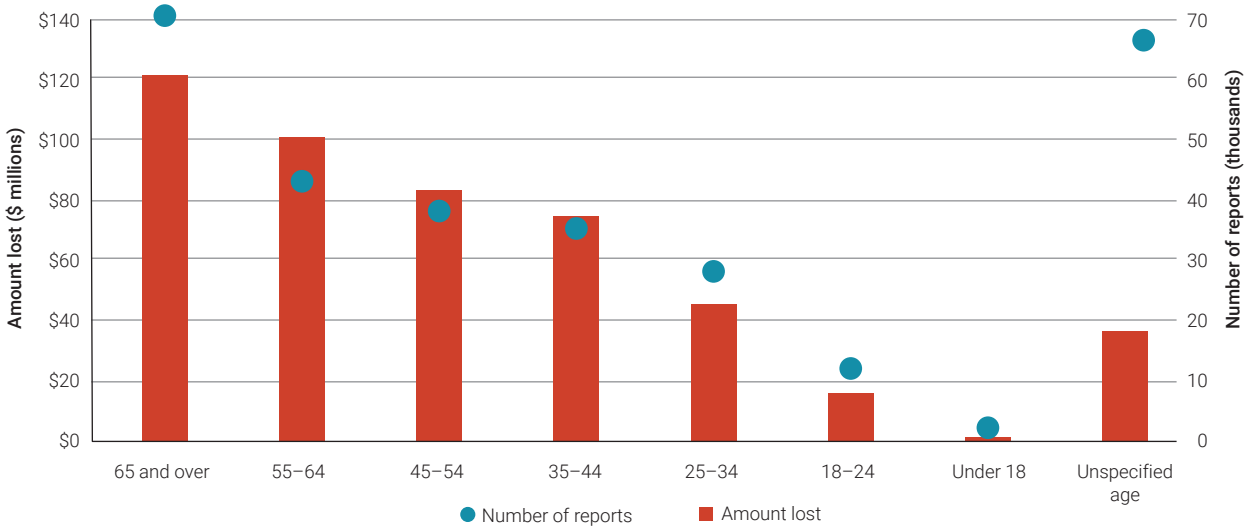
- engagement with at-risk groups
- culturally informed, tailored, and widespread scams campaigns and messaging
- tools and resources to support people to recognise and avoid scams
- research to understand information preferences and reporting behaviours.

For example, there is a clear need to raise awareness among CALD communities about steps to recognise, avoid and report threat-based scams and job scams. Scams prevention initiatives for people with disability should target social media and email scams.

36 Scamwatch report form lists the contact method as social networking or online forums.

Despite the overall decrease in losses in 2023, **Australians aged 65 and over** experienced almost no change in reported losses in 2023 compared with 2022. People over 65 lost more money than other age groups, with $121 million reported lost. Older Australians were the only age group that did not experience a decrease in reported losses. Some older Australians are more likely to have considerable retirement savings and be looking to invest. While there were decreases in reported losses for people 65 and over from September 2023 (coinciding with scam prevention initiatives) the significant investment scam losses in February ($13.7 million) and May ($11.2 million) led to an overall increase in reported investment scam losses for older Australians of 13.3%.

**Figure 5:** Scam reports and losses by age group




**First Nations people**[37] reported more scams in 2023 with 6,192 reports compared to 3,889 in 2022. Reported losses decreased by 26.1% to $3.8 million. This decrease should be considered with caution as research suggests First Nations people who lose money may be reluctant to report.[38] The National Anti-Scam Centre will be undertaking work to better understand scams impacting First Nations communities and the most effective and empowering scams prevention strategies. This work will be undertaken with First Nations communities.

**Table 6:** Top 5 scams with highest total losses for First Nations people

| Scam types | Losses | % change from 2022 losses | Median loss |
|---|---|---|---|
| **Investment scams** | $1,275,326 | -50.7% ▼ | $3,522 |
| **Identity theft** | $728,049 | 218.0% ▲ | $855 |
| **Online shopping**[39] | $458,931 | 10.9% ▲ | $250 |
| **Jobs and employment** | $353,971 | 27.3% ▲ | $3,864 |
| **Dating and romance** | $350,698 | -54.2% ▼ | $681 |

37 Scamwatch invites reporters to indicate whether they identify as 'Indigenous' when they complete a webform. This information helps identify the types of scams that may be impacting First Nations people and target warnings to the relevant communities.

38 Fiftyfive5 (part of Accenture) research commissioned by The Treasury 2023.

39 Includes 'classified' scams.

In 2023, people from **CALD communities**[40] made up only 4.8% of total reports to Scamwatch and almost 12.7% of reported losses. They collectively made 14,396 reports (increase of 26.1%) with $60.5 million in total reported losses (increase of 6.9%). The median and average reported losses are higher for CALD communities than for all Scamwatch reporters.[41] People from CALD communities were over-represented in the losses for some scam types, accounting for:

- 6.2% of reports but 54.4% of losses to scams involving threats to life, arrest or other
- 3.8% of reports but 27.1% of losses to scams involving inheritance and unexpected money
- 10.9% of reports but 16.4% of losses to jobs and employment scams.

**Table 7:** Top 5 scams with highest losses for CALD reporters

| Scam type | Losses | % change from losses in 2022 | Median loss |
|---|---|---|---|
| **Investment scams** | $38,515,781 | 29.5% ▲ | $14,133 |
| **Threats to life, arrest or other** | $7,549,288 | 24.0% ▲ | $57,500 |
| **Jobs scams** | $3,988,575 | 92.2% ▲ | $7,900 |
| **Romance scams** | $2,292,273 | -65.5% ▼ | $4,000 |
| **Phishing** | $1,612,887 | 67.3% ▲ | $2,500 |

Scamwatch received 22,080 reports (7.3% of total reports) from **people with disability**,[42] with financial losses of $30.8 million (6.5% of total losses) reported. Reports increased 34.0% and losses decreased 8.5%. The most common contact methods where people with disability lost money were social media ($7.5m) and email ($6.0m).

**Table 8:** Top 5 scams with highest losses for reporters with disability

| Scam Type | Losses | % change in losses from 2022 | Median loss |
|---|---|---|---|
| **Investment scams** | $16,647,632 | -11.1% ▼ | $8,000 |
| **Romance scams** | $4,126,471 | -10.6% ▼ | $1,900 |
| **Phishing** | $3,326,608 | 269.7% ▲ | $2,500 |
| **Rebate scams** | $991,385 | 205.8% ▲ | $2,500 |
| **Inheritance and unexpected money** | $917,495 | 249.4% ▲ | $2,800 |

**Businesses**[43] submitted 4,933 scam reports in 2023, a 27.9% increase from 2022. Businesses reported losses of $29.5 million, a small increase on losses reported in 2022. Small and micro businesses reported $17.3 million of the total lost.[44] The scams causing high losses for small business were false billing scams, remote access scams and investment scams.

40 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 to report on scams that impact CALD communities. Scamwatch does not collect data on the specific languages spoken or cultural backgrounds of reporters from a non-English speaking background.

41 The median loss for CALD reporters was $1,000 and the average loss was $25,298.

42 When people report to Scamwatch, they can indicate if they identify as a person with disability on the report form. This helps identify scams that may be targeting or impacting people with disability so that we can ensure our warnings are relevant and effective. The Scamwatch reporting form does not ask people to specify the type of disability.

43 Scamwatch receives reports about scams from businesses and they are invited to indicate whether they are large (over 200 staff); medium (20–199); small (5–19) or micro (0–4).

44 Small and micro businesses (0 to 19 employees).

**Table 9:** Losses and reports by business size

| Business size by staff | Reports | Losses (m) | Loss percentage change from 2022 | Median loss |
|---|---|---|---|---|
| **Micro (0–4)** | 1,358 | $13.2 | 64.9% ▲ | $3,225 |
| **Small (5–19)** | 1,132 | $4.1 | -27.8% ▼ | $4,234 |
| **Medium (20–199)** | 766 | $5.2 | 42.7% ▲ | $4,394 |
| **Large (over 200)** | 666 | $1.7 | 71.7% ▲ | $3,198 |
| **Size not provided** | 1,011 | $5.3 | 7.9% ▲ | $1,998 |

Table 10 below highlights the scam types leading to the most reported losses for businesses.

**Table 10:** Top 5 scams for businesses

| Scam type | Losses (m) | % change from 2022 | Median loss |
|---|---|---|---|
| **False billing** | $11.8 | 37.0% ▲ | $7,000 |
| **Investment scams** | $6.2 | -37.7% ▼ | $49,787 |
| **Remote access** | $4.9 | 478.6% ▲ | $20,000 |
| **Phishing** | $3.5 | 186.5% ▲ | $10,500 |
| **Rebate scam** | $1.4 | 2,234.9% ▲[45] | N/A |

The National Anti-Scam Centre will continue to raise awareness about scams impacting small business. In December 2023, the National Anti-Scam Centre held an industry forum to raise awareness about payment redirection scams. This was attended by over 140 representatives from medium and small businesses impacted by these scams including car dealerships and the construction sector. More of these forums will be held in 2024.

# More information on scam activity

The annual Targeting Scam report series is available at www.scamwatch.gov.au.

Scamwatch data is regularly published via the public dashboard available on Scamwatch. A public beta version of an improved dashboard which allows additional filtering, including by state or territory, is also available.

Updates about the National Anti-Scam Centre and its partners are available through its Quarterly Report series and regular media releases.

45 This percentage increase in losses to rebate scams was largely due to a single report and is considered an outlier in terms scam reports by businesses.

# Appendix 2: About the data used in this report

The data in this report is for the calendar year 1 January to 31 December 2023.

Reference to **combined reports** or **combined losses** include data from Scamwatch, ReportCyber,[46] IDCARE, ASIC, and the AFCX.[47] These are the primary places that hold data relating to both scam losses and reports.

ReportCyber, Scamwatch and ASIC data has been adjusted to remove duplicate reports about the same incident from the same reporter where they could be identified, and unreliable[48] high loss reports have been removed from these data sets. Adjustments have been made to account for potential duplication across Scamwatch, the AFCX and IDCARE.[49]

Due to the aggregate nature of the data provided, there will be some duplication remaining in the data sets. However, to some extent this is balanced by the gaps[50] in the data sets.

In future, through National Anti-Scam Centre data sharing arrangements, there will be more opportunities to de-conflict data. Future reports will also include additional data sets to produce a more accurate picture of scam activity in Australia.

The National Anti-Scam Centre thanks all contributing organisations for their participation and cooperation in the production of this report.

## Scamwatch data

This report includes a section analysing scams reported to the National Anti-Scam Centre's Scamwatch service. Scamwatch is a rich data source that includes information about scam types, victims affected, communications and payment methods used by scammers, and some information about the backgrounds of reporters and victims. Over the next twelve months the National Anti-Scam Centre technology build will integrate information from many of the reporting services and data sources to provide a more consolidated data set.

Scamwatch data may be adjusted throughout the year due to quality assurance processes, or changes to categories or the Scamwatch report form. Most high loss reports are verified, but many lower loss reports are unverified.

When comparing this report with data published on the Scamwatch website there are minor discrepancies in report numbers. This is a result of a data migration of 2.2 million records into a new National Anti-Scam Centre data system. The variability is statistically insignificant. The National Anti-Scam Centre team are always working to improve the data quality and understanding of scams affecting Australians.

46 This report only includes ReportCyber data relating to 'scams' and not cyber security incidents, hacking, malware or data breaches, online image abuse or cyberbullying.

47 The 2023 combined data does not include data from the ACMA, ATO and Services Australia. In 2022 this data made up less than 6% of the report data and less than 0.00254% of loss data. ACMA provided 2023 telemarketing and spam data which was not easily aligned with scam categories and did not contain losses. Total telemarketing scams were 3,411; total spam scams were 1,420, both were decreases on 2022.

48 Unreliable losses are those that do not appear to have any connection to Australia; those that appear to be prank reports; reports where loss is not direct loss but loss of anticipated gain; and exaggerated loss, for example claims of $1 trillion.

49 This approach recognises the potential duplication from referrals to IDCARE coming from contributing data sources.

50 AFCX data does not include data for all financial institutions in Australia. Data has not been obtained from cryptocurrency exchanges or superannuation firms. The combined data has not been adjusted to account for any unreported losses.

# Data sources

## National Anti-Scam Centre – Scamwatch scam report service

Scamwatch (www.scamwatch.gov.au) is run by the National Anti-Scam Centre. Established in 2002 by the ACCC, it provides a place to report scams and provides information about how to recognise and avoid scams. Scamwatch intelligence is used by the National Anti-Scam Centre to disrupt scams and to inform the activities of government, law enforcement, industry and community organisations to prevent scams. Scamwatch takes reports direct from the public.

## Australian Signals Directorate – ReportCyber cybercrime report service

ReportCyber (www.cyber.gov.au) is a cybercrime reporting platform hosted by the Australian Cyber Security Centre of the Australian Signals Directorate. It was developed as a national policing initiative with State and Territory police, the Australian Federal Police and the Australian Criminal Intelligence Commission. Australians can report a cybercrime, cyber security incident or vulnerability. Some of the reports made to ReportCyber are scams. The National Anti-Scam Centre has access to these reports.

## Australian Financial Crimes Exchange (AFCX) – financial services information exchange

The AFCX (www.afcx.com.au) is an independent, non-profit platform that enables the exchange of intelligence primarily by financial services to combat financial and cybercrime. The AFCX is not a public reporting platform. The information shared and data collected is based on financial services transaction data. This data is sourced from or reported via members of the AFCX. The National Anti-Scam Centre is working with the AFCX to integrate data and intelligence in 2024.

## IDCARE – Identity theft and cyber support service

IDCARE (www.idcare.org) is Australia and New Zealand's national identity and cyber support service. It is a registered charity that receives some government funding and is funded by subscribers[51] that use its services. The public can also contact IDCARE to receive free advice and support. IDCARE provides support for scam victims as well people who have experienced identify takeover, lost or stolen credentials, data breaches, hacking or cyber security concerns. The National Anti-Scam Centre has had automated referral processes with IDCARE since its commencement in July 2023. This ensures victims who lose money or identity information are referred in real time to IDCARE for support. Other organisations such as most banks, law enforcement agencies and many other organisations refer their customers to IDCARE for support.

51 A list of organisations that use IDCARE services: https://www.idcare.org/about-idcare/our-subscribing-organisations.

## Australian Securities and Investments Commission (ASIC) – investment scam intelligence

ASIC (www.asic.gov.au) is Australia's corporate, markets, financial services and consumer credit regulator. ASIC receives reports about investment scams. The National Anti-Scam Centre set up new data sharing arrangements in 2023, which simplifies the process for reporting and deconflicting reports between ASIC and Scamwatch services. Since November 2023, ASIC has redirected investment scam reporters from ASIC to Scamwatch via an embedded link on its Moneysmart website.[52]

52 https://moneysmart.gov.au/check-and-report-scams/report-an-investment-scam.


Australian Government


National
Anti-Scam
Centre