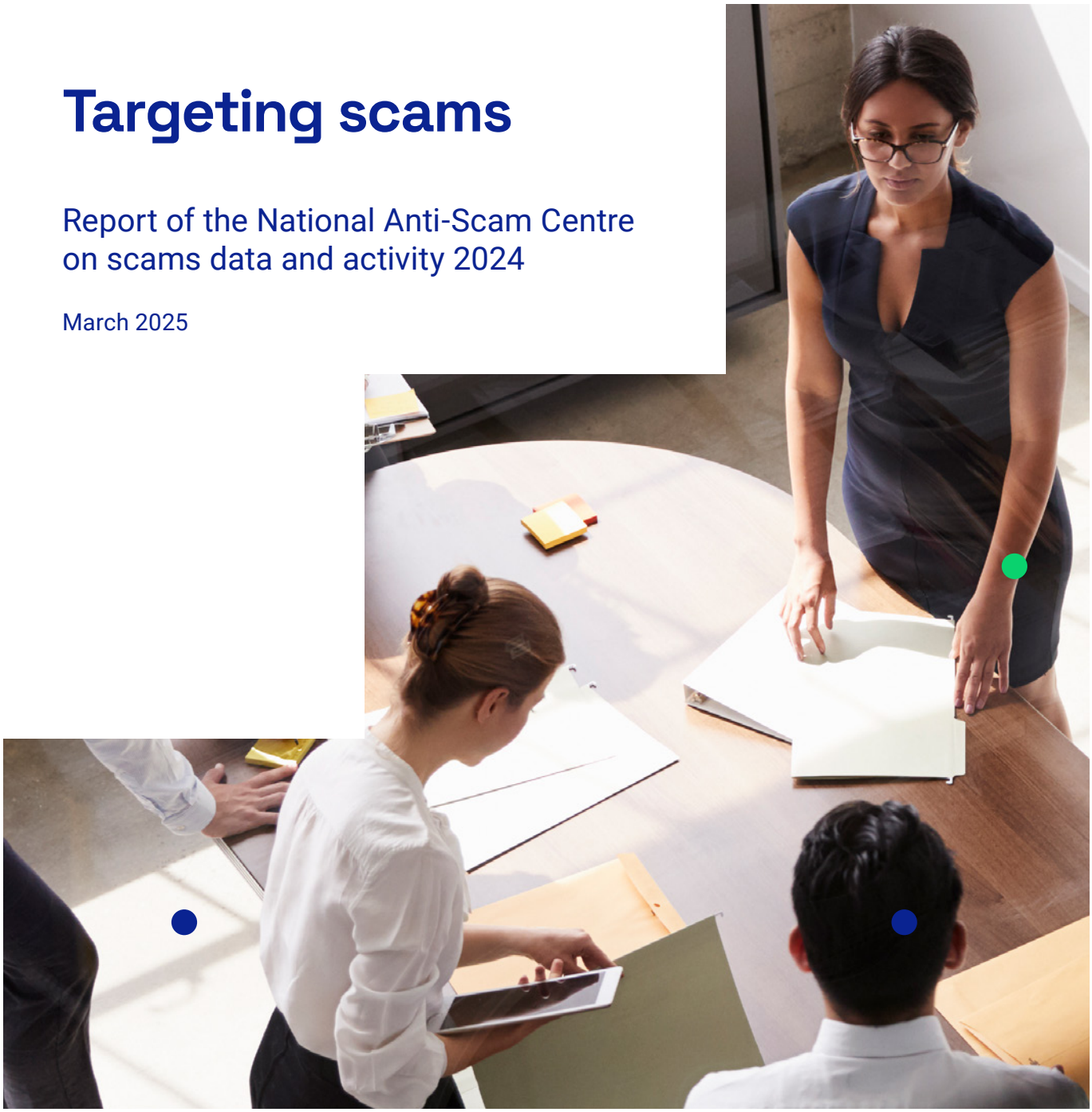
Australian Government

National Anti-Scam Centre

Targeting scams

Report of the National Anti-Scam Centre on scams data and activity 2024

March 2025



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 03/25_25–10

www.accc.gov.au

Contents

Foreword

This report provides insight into the scams targeting Australians in 2024 and highlights the impact of combined efforts by government, law enforcement, community sector and industry to combat these financial crimes. This is the second Targeting Scams Report produced by the National Anti-Scam Centre since its establishment on 1 July 2023.

Data from Scamwatch, ReportCyber, the Australian Financial Crimes Exchange (AFCX), IDCARE and the Australian Securities and Investments Commission (ASIC) shows **$2.03 billion** was the **combined reported losses to scams** in **2024**, a 25.9% decrease from 2023. Over the same period, Australians made **494,732** scam reports compared to 601,803 in 2023 (a 17.8% decrease in reports).

It is encouraging to see a continued decrease in reported losses in 2024. While we are cautiously optimistic that the combined efforts of government, law enforcement and industry will continue the downward trend, we note an increase in loss reports over the last months of 2024. Scammers are sophisticated and motivated criminals, and we can expect them to innovate even as we succeed in strengthening our defences.

This fact, together with the very real human and economic impact of scams, makes us more determined than ever to continue our important work. We are mindful that the harm caused by scams is not limited to financial loss. The impact on scam victims is all too often life changing, with negative effects on mental health and wellbeing.

One of the best weapons we have is the intelligence reported by Australians to us or our partners, including the reports provided by people who have identified and avoided a scam. In 2025, we commenced a national media campaign to raise scams awareness and help Australians feel supported to confidently identify, avoid and report scams. The campaign message, 'Stop. Check. Protect.', provides Australians with a simple and memorable set of actions to arm themselves against scams.

The National Anti-Scam Centre is committed to providing better protection for Australians against increasingly sophisticated scams by strengthening cooperation between government and industry. We will continue our technology build and the expansion of our data sharing with trusted partners to coordinate intelligence and provision of information to those who can act on it. In 2024 we established data sharing agreements, including with AFCX, ASIC and cryptocurrency exchanges, and expect to build on this in 2025.

Cooperation can, and has, achieved a great deal. But it is not enough. We need everyone at the table, not just the volunteers. Accordingly we very much welcome the enactment of the *Scams Prevention Framework Act 2025*.

The implementation of consistent, mandatory and enforceable obligations on designated sectors to take reasonable steps to prevent, detect, report, disrupt and respond to scams will provide better protection for consumers. The National Anti-Scam Centre will support stakeholders as they prepare for the Scams Prevention Framework.

The effort to combat scams is complex and cannot be done without the significant efforts of all the people and organisations who engage with us every day. This report is testament to their valued and ongoing contributions. Our sincere thanks to those working towards our common goal of providing better protection for Australians against scams.

Catriona Lowe

Deputy Chair, ACCC

At a glance

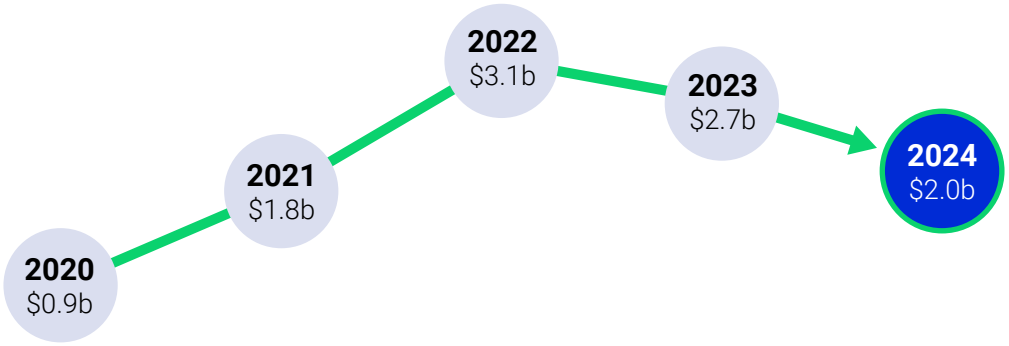
Losses

$2.03 billion lost ▼25.9%

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

494,732
scam reports
▼17.8%

Combined losses over last 5 years



Top 5 scam types by loss 2024 (combined data)

Investment	Romance	Payment redirection	Remote access	Phishing
$945.0m	$156.8m	$152.6m	$106.0m	$84.5m

The losses from the Top 5 scam types accounted for 71% of total losses in 2024.

Top 5 scams types by loss 2023 (combined data)

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

The losses from the Top 5 scam types accounted for 74% of total losses in 2023.

Key statistics

Depending on the type of scam and the level of awareness about the role of reporting agencies and private organisations, Australians may report scams to a range of sources. The National Anti-Scam Centre is working to bring together these data sources to provide a more complete picture of the level of scam activity in Australia.

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

In 2024, Australians made a combined total of **494,732 reports** (a 17.8% decrease), of which 207,605 report losses of over **$2.03 billion** (a 25.9% decrease). This compares with a combined total of 601,803 reports and combined reported losses of over $2.7 billion in 2023.

Table 1: Combined losses and reports 2023 and 2024[1]

	2023		2024		% change in loss from 2023
Organisation	Number of Reports	Losses	Number of Reports	Losses	%
Scamwatch	301,778	$476.8m	249,448	$318.8m	-33.1% ▼
ReportCyber	69,393	$793.5m	64,682	$734.2m	-7.5% ▼
AFCX[2]	217,284	$1,182.4m	169,184	$812.3m	-31.3% ▼
ASIC	1,373	$87.8m	965	$93.4m	6.4% ▲
IDCARE[3]	30,553	$366.7m	42,193	$513.6m	40.1% ▲
Adjustments[4]	-18,578	-$165.3m	-31,740	-$445.6m	
TOTAL	**601,803**	**$2.7b**	**494,732**	**$2.0b**	**-25.9%** ▼

1 Table 1 highlights the variance number of reports and reports with loss across the data sets. This variance is in part a reflection of where scam victims are more likely to report, depending on the circumstances. For example, victims may be more likely to report high-loss cyber related scams to ReportCyber, financial loss incurred through bank transfers to a bank (appearing in AFCX data), and more altruistic reporters without financial loss may report to Scamwatch. Bringing these data sets together provides a more complete picture of the scams landscape.

2 Institutions that reported data to AFCX for the full 2024 calendar year were: ANZ, Bendigo Bank, CommBank, Customer Owned Banking Association (on behalf of some members), Cuscal, Macquarie Bank, NAB and Westpac. Institutions that contributed data for part of the 2024 calendar year were: Suncorp (since September), Rabobank (since October) and Bank of Queensland (since December). For further information regarding AFCX data refer to Appendix 2.

3 IDCARE saw an increase in both the number of scam reports and loss in 2024 when compared to 2023. The increase in reports may be due to heightened community awareness regarding IDCARE's role in providing support to scam victims and an increase in referrals to IDCARE from other entities. IDCARE also advise the average amount for IDCARE clients who experienced a financial loss in 2024 was $40,000, up from $36,000 in 2023.

4 There can be duplication where the same scam is reported by a consumer multiple times or to multiple organisations, and adjustments are made to reflect to the extent possible (see Appendix 2 for further information on adjustments). Reports without loss hold intelligence value as they inform disruption activities, and add to understanding of scam methodology, thereby reducing the likelihood of others falling victim to the scam.

Table 2: Combined reports with loss 2023 compared with 2024

Organisation	2023			2024		
	Reports	Reports with loss	% of Reports with loss	Reports	Reports with loss	% of Reports with loss
Scamwatch	301,778	29,191	10.0%	249,448	22,408	9.0%
ReportCyber	69,393	39,091	56.3%	64,682	34,562	53.4%
AFCX	217,284	N/A	N/A	169,184	136,719	80.8%
ASIC	1,373	923	67.2%	965	N/A[5]	N/A
IDCARE	30,553	9,223	30.2%	42,193	13,916	33.0%

While investment scams continue to result in the most significant financial harm to Australians with combined losses of $945.0 million in 2024, financial losses across all scam categories, except payment redirection, decreased in 2024 as outlined in Table 3 below.

Table 3: Combined losses by category 2024[6]

Scam category	Scamwatch	Report Cyber	AFCX	ASIC	IDCARE	Adjustments	Total 2024*[7]	% change from 2023	Total 2023
Investment	$192.3m	$349.4m	$292.0m	$71.1m	$290.7m	$250.5m	**$945.0m**	-27.3% ▼	$1,300.0m
Romance	$23.7m	$66.1m	$55.5m	N/A	$69.1m	$57.9m	**$156.8m**	-22.0% ▼	$201.1m
Payment redirection	$9.5m	$90.8	$52.3m	N/A	$12.5m	$13.1m	**$152.6m**	66.6% ▲[8]	$91.6m
Remote access	$7.6m	N/A	$97.0m	N/A	$4.8m	$3.5m	**$106.0m**	-58.6% ▼	$256.0m
Phishing	$20.5m	N/A	$48.9m	N/A	$93.0m	$77.9m	**$84.5m**	-38.5% ▼	$137.4m
Other[9]	$65.2m	$227.8m	$266.6m	$22.2m	$43.3m	$42.8m	**$582.3m**	-23.0% ▼	$755.9m

5 In 2024 ASIC data was provided in aggregate form, consequently, reports with loss are not available.

6 Totals adjusted for potential duplication of reporting – see Appendix 2 for further information.

7 Totals for each organisation may differ slightly from totals in Table 1 due to rounding of scam types in Table 3.

8 AFCX data did not specify which scams were payment redirection scams in 2023. Payment redirection scams continue to be an issue for both Australian consumers and businesses but the 66.6% increase is a result of it not being included last year. Comparing 2024 and 2023 datasets on a like for like basis, i.e. Scamwatch, ReportCyber and IDCARE data only, shows a modest increase in losses to these scams of 9.0% in 2024.

9 "Other" includes all other scams which are not part of the top 5 scams causing the highest losses.

Observations on losses in 2024

Combined losses have decreased since 2023 as shown in Table 1. This downturn reflects key government, industry and consumer advocacy initiatives in 2024. These include the work of the National Anti-Scam Centre in bringing together participants from across the scams ecosystem to identify, disrupt and prevent scam activity, along with specific measures from industry and consumer groups. The case studies throughout this report highlight a range of industry and consumer advocacy measures from 2024 that have disrupted scams and raised awareness of scam activity.

IDCARE saw an increase in both the number of scam reports and losses in 2024 when compared to 2023. The increase in reports may be due to heightened community awareness regarding IDCARE's role in providing support to scam victims and an increase in referrals to IDCARE from other entities. IDCARE also advise the average amount for IDCARE clients who experienced a financial loss in 2024 was $40,000, up from $36,000 in 2023.[10]

10 Refer to Appendix 2 for how overlap between the IDCARE data set and the other datasets was identified and addressed when preparing the 2024 Targeting Scams Report.

National Anti-Scam Centre in action

This section of the report focuses on key initiatives that have protected Australians and reduced the harm caused by scams.

Disruption

The National Anti-Scam Centre and partners' disruption activity focuses on preventing contact between scammer and victim, breaking contact where it has already occurred, and preventing the transfer of money or personal information.

In 2024 the National Anti-Scam Centre:

- referred more than 6,000 non-investment scam URLs for assessment and takedown, with 92.0% of those subsequently removed
- referred more than 2,000 investment scam URLs to ASIC for assessment and appropriate further action including potential takedown
- identified 134 websites via the AFCX's Intel Loop for takedown disruption activity
- referred 10,355 suspected Facebook scam URLs to Meta for further investigation
- referred more than 1,000 phone numbers and sender IDs (on average more than 50 per fortnight), to telecommunications partners for disruption.

Consistent with the whole of ecosystem approach to combating scams, in 2024 the telecommunications sector played an important role in protecting Australians from scams. The National Anti-Scam Centre invited the Australian Communications and Media Authority (ACMA) and peak industry body, Communications Alliance,[11] to highlight significant anti-scam initiatives in 2024. Their contributions are set out below.

Anti-Scam initiatives: The Australian Communications and Media Authority[12]

The Australian Communications and Media Authority (ACMA) continues to disrupt telco scams before they reach Australians. In 2024, the ACMA focused on enforcing the Reducing Scam Calls and Scam SMS Industry Code (Scam Code), exploring new scam disruption initiatives, supporting the National Anti-Scam Centre, educating consumers, and collaborating with key stakeholders domestically and internationally.

Telcos reported blocking over 455.9 million scam calls and over 413.9 million scam SMS under the obligations in the Scam Code in 2024. The ACMA provided de-identified complaint data to telcos to help facilitate the identification and blocking of these scams.

11 Communications Alliance is the primary telecommunication industry body in Australia. For information refer to https://www.commsalliance.com.au/ (accessed 16 February 2025).

12 ACMA provided content for this information box.

The ACMA finalised 6 investigations into telco compliance with the Scam Code and gave 4 directions to telcos to comply with obligations. These actions closed gaps targeted by scammers to reach Australians and helped ensure telcos share intelligence across networks to assist in scam disruption.

As part of the Government's 'Fighting Scams' initiative, the ACMA is implementing a mandatory SMS Sender ID Register to protect the alphanumeric message headers (alpha tags) of brands and government agencies from SMS impersonation. At the end of 2024, there were 71 alpha tags on the pilot Register, all of which are used by scammers in impersonation scams. The mandatory Register is expected to commence in late 2025.

Examples of communications sector scam prevention initiatives:

Communications Alliance[13]

Blocking calls and SMS

Telstra blocked an average of over 10 million scam calls and 14 million scam SMS every month through its 'Cleaner Pipes' initiative (in financial year 2024).

TPG Telecoms (TPG) implemented advanced machine learning technology that adapts to current network conditions and subscriber behaviour to detect and block attempted illicit activity. In 2024, TPG blocked over 46 million scam calls and 109 million scam SMS.

Optus Call Stop intercepts calls to known impersonation scam numbers in partnership with the National Anti-Scam Centre and the AFCX.

Partnerships and preventing spoofing

Telstra partnered with CommBank on 'Scam Indicator' to enable real-time detection and prevention of scams by indicating whether a customer might be on a phone call while making a bank transaction – a key indicator of a scam taking place.

Optus SMS Sender ID Registry prevents specified SMS Sender IDs from being spoofed by unauthorised entities. The Optus Do Not Originate registry is a list of numbers used by Optus corporate and government customers for inbound calls only, blocking the numbers from entering the Optus network for outbound calls.

Reporting scam activity

Optus Scam Wise, a tool that tells customers how to spot scams and stay safe online, enables the reporting of scam activity and alerts users to the latest, most prevalent scams.

Telstra introduced a reporting number (7226 / SCAM) so customers can report SMS and MMS scams.

Sharing intelligence

Every week, the National Anti-Scam Centre provides all suspect phone numbers reported more than once in alleged SMS or phone call scams to 11 telecommunication services providers and the Australian Communications and Media Authority (ACMA). Providers are TPG (Vodafone), Pivotel, MNF Group, Symbio Networks, ATOM, Aussie Broadband, Netsip, Optus, Telstra, Bandwidth, and Vocus.

13 Communications Alliance provided content for this information box.

Data and intelligence sharing with stakeholders

The National Anti-Scam Centre has built technology and continued to establish data sharing partnerships in 2024. Sharing scams data enables increased visibility across government, law enforcement and the private sector about scam activity, providing organisations with better capability to identify and disrupt scams. The National Anti-Scam Centre plays a critical role in collecting and assessing data from across the scams ecosystem, actioning intelligence to support disruption and sharing intelligence with entities best placed to act on it.

Key National Anti-Scam Centre partnerships and data sharing in 2024 included:

- Daily sharing of investment scam URLs identified in Scamwatch reports with ASIC. The automated sharing of these reports means that ASIC can more efficiently assess and refer the websites for takedown, if suitable.
- Data from the National Anti-Scam Centre sent every two hours providing suspected scammer bank details to the AFCX, for sharing with relevant banks. The data supports banks to investigate suspected scammer accounts for further disruption activity. Suspected scam website URLs sent to the National Anti-Scam Centre from banks and telecommunications providers, via the AFCX Intel Loop, enabled 134 websites to be actioned for takedown disruption activities.
- Phone numbers reported in alleged text or phone call scams are provided weekly to 11 telecommunications providers and the ACMA.
- Meta provided with daily suspect scam URLs on the Meta platform identified in Scamwatch reports.
- Gumtree provided with daily suspected scam advertisement IDs, with 310 referred for further investigation.
- Through enhanced information sharing capabilities, the National Anti-Scam Centre now receives near real-time scam reports made by the public to law enforcement through ReportCyber.

In 2024 the banking sector played an important role protecting Australians from scams. The National Anti-Scam Centre invited banking industry bodies, the Australian Banking Association (ABA) and the Customer Owned Banking Association (COBA), to highlight significant anti-scam measures implemented in 2024. Their contributions are set out below.

Examples of banking sector scam prevention initiatives:

Australian Banking Association (ABA)[14]

The Australian banking sector developed the Scam-Safe Accord, aiming to disrupt, detect and respond to criminal scam activity. Examples are described below:

Bank impersonation scams

The CommBank implemented In-app CallerCheck technology to assist customers to verify it is CommBank calling, and avoid bank impersonation scams (February 2023).

ANZ introduced CallSafe, a feature that provides secure authentication, enabling ANZ Plus customers to verify they are speaking to ANZ staff, and staff to authenticate the customer's identity.

NAB collaborated with telcos by placing bank phone numbers on the 'Do Not Originate' list, making it harder for criminals to infiltrate bank phone numbers and text message threads (February 2023). Since July 2023 NAB no longer uses links in unexpected text messages to customers, to assist customers to recognise scam red flags.

Westpac added 94,000 phone numbers to the 'Do Not Originate' list preventing scammers from impersonating the bank's phone numbers.

Scams intelligence

In 2024, Bendigo and Adelaide Bank worked with Australian cybersecurity agencies, intelligence, and technology partners to detect malicious or abnormal behaviour. Several Australian banks integrated reporting into the AFCX's Anti-Scam Intelligence Loop, assisting it to report and respond to scams across digital platforms, telecommunications companies and banks.

Biometrics

Bank of Queensland enhanced onboarding controls in its digital bank and introduced new risk scoring and biometric technology. These measures assist to detect and intervene in suspected mule account applications. Bendigo and Adelaide Bank introduced biometric checks and other controls for new online accounts to prevent account misuse.

14 The ABA provided content for this information box. The ABA is an association of 20 member banks in Australia. For further information refer to https://www.ausbanking.org.au/about-us/the-aba/, (accessed 11 February 2025).

Confirmation of payee

CommBank introduced NameCheck technology giving customers an indication of whether the account details entered appear correct (March 2023). According to CommBank, NameCheck was used 57 million times in FY24, preventing scam payments estimated at more than $40 million. Bendigo and Adelaide Bank introduced a pilot of NameCheck, used to screen all payments made by Bendigo Bank and Up customers entering the BSB and account number for new payees.

Westpac introduced Verify, alerting customers when there is a potential account name mismatch when adding a new payee using a BSB and account number. Verify was recently introduced for St.George, Bank of Melbourne, and BankSA customers.

Warnings, payment delays and security questions

ANZ increased personalised warning messages on Internet Banking when a transaction or activity is considered high risk.

Bendigo and Adelaide Bank implemented warnings within the payment flow in e-banking, requires additional authorisation for payments to new payees and introduced risk-based delays for some New Payments Platform payments.

CommBank introduced interactive scam warnings for some first-time payments, assisting customers decide whether to proceed with the payment.

CommBank, ANZ, Westpac, NAB and Suncorp joined BioCatch Trust Australia, to pilot the sharing of information in real time before a payment is made, helping prevent money being sent to scammers.

NAB customers abandoned more than $211 million in payments in 2024 after the bank raised scam concerns. The bank introduced real-time payment alerts targeting common scam types in the NAB App and Internet Banking in March 2023.

Westpac introduced SaferPay technology that presents customers with a series of questions in instances where a payment is considered a high risk of being a scam.

Customer Owned Banking Association (COBA)[15]

COBA reports the customer-owned banking sector continues to progress and implement the Scam-safe Accord, including through access to scam intelligence for all COBA members. COBA report customer-owned banks are on track to meet due dates for Fraud Reporting Exchange participation, with members holding the equivalent of 95% of sector assets now participating. This assists in expediting recovery for scam victims. COBA reports that its members are continuing to work on increasing scam awareness and providing education for their communities on how to protect themselves from scams.

15 COBA provided content for this information box. COBA is the industry association for Australia's customer-owned banking institutions, see https://www.customerownedbanking.asn.au/ for further information (accessed 16 February 2025).

National Anti-Scam Centre Case study: From intelligence to action

In December 2024 the National Anti-Scam Centre identified a scam campaign which impersonated Australian universities. Students received emails asking for payment of overdue tuition fees. These emails:

- appeared to come from a legitimate university email address (because they were 'spoofed' by scammers)
- contained university branding and directions to send responses to an email address that was designed to appear like a legitimate university email account.

Within 3 days the National Anti-Scam Centre identified the issue through assessing Scamwatch data and then shared intelligence with industry, including financial institutions and digital media platforms, government and law enforcement. While sophisticated in nature, this was a short-lived scam and has not appeared in subsequent Scamwatch reports.

Website takedown service

The National Anti-Scam Centre and ASIC facilitate the takedown of scam websites.[16] In 2024 the National Anti-Scam Centre referred more than 8,000 websites for takedown, including 6,000 to the National Anti-Scam Centre's takedown service and over 2,000 investment related scams to ASIC. Disrupting scam websites assists consumers to identify a potential scam site as the longer a website remains active, the more legitimate it may appear to be. In taking down URLs, should scammers attempt to re-establish a scam site it will have limited history and therefore present a red flag to consumers.

Website takedown service

6,000+
URLs referred for takedown

92%
of URLs successfully removed

$36m
estimated avoided loss*

*based on average reported loss per reported URL

There are a range of other initiatives by government agencies to remove online scam content. Since 2019, ACMA has been taking down illegal gambling websites used in betting scams, as well as removing illegal gambling content from social media, online advertisements, and mobile applications. Services Australia removes scam content impersonating its brands such as myGov and Centrelink. In 2024, action was taken resulting in 13,000 Services Australia takedowns of scam content impersonating myGov/Centrelink. Different approaches counter the unique characteristics of different scam typologies. In 2024 the National Anti-Scam Centre collaborated with ASIC regarding investment scams.

ASIC collaboration

2,000+
URLs referred to ASIC

ASIC coordinated the removal of **6,270** phishing and investment scam websites

ASIC coordinated **64%** more URLs for removal via Scamwatch reports than in same period in 2023 (1 July to 31 December 2023)

16 The National Anti-Scam Centre commenced automatedly referring investment scams reported to its Scamwatch service to ASIC in March 2024.

Fusion Cells to combat scams

The National Anti-Scam Centre co-led the **Investment Scam Fusion Cell** with ASIC, publishing the final report on the Fusion Cell's work in May 2024.[17] Key outcomes include over 1,000 investment scam advertisements and videos removed, 220 investment scam websites disrupted and 113 attempted calls to scam phone numbers diverted.

The National Anti-Scam Centre launched the **Job Scam Fusion Cell** in August 2024; it is expected to publish a final report in May 2025.

In 2024 the ASIC played an important role in protecting Australians from investment scams. The National Anti-Scam Centre invited ASIC to highlight key anti-scam initiatives in 2024. Their contribution is set out below.

Anti-Scam initiatives: Australian Securities and Investments Commission[18]

ASIC is Australia's corporate, markets, financial services and credit regulator and combatting scams has been one of ASIC's core priorities for several years.

Investment scams cause significant harm to Australians.

In 2024, ASIC remained focused on reducing the incidence of investments scams in Australia and their impact on consumers. This is demonstrated through:

- coordinating the removal of an average of 120 investment scams and phishing websites per week, including those promoted by advertising on digital platforms
- listing, on average, 90 companies, businesses and websites per month suspected of being a scam on Moneysmart's Investor Alert List to warn consumers
- regularly publishing consumer and investor warnings about investment scams and scams in the financial services sector (for example: Share Sale Fraud)
- co-leading the IOSCO APRC Working Group on Scams and Online Harms where securities regulators build capability and cooperate on initiatives to mitigate and disrupt scams in the Asia-Pacific region.

While investment scam losses are decreasing, ASIC's reviews of the banking sectors have highlighted the need for a coordinated and increased effort to ensure the trend continues.

In 2024, ASIC published a report into the anti-scam practices of 15 banks outside the major four. Like the findings for the four major banks ASIC reported in 2023, this report highlights where banks needed to improve, particularly in response to poor customer experiences and outcomes.

The financial services sector has a critical role in scams prevention, detection and response along with all of corporate Australia including digital platforms, telecommunication providers and other organisations.

In 2024, an ASIC investigation into a sophisticated self-managed super fund (SMSF) scam led to criminal charges being laid against two individuals who allegedly perpetrated the scam. ASIC also commenced civil penalty proceedings against HSBC Australia alleging it failed to protect its customers from the risk of being scammed of millions of dollars and to fairly deal with those customers after they were scammed.

17 Refer to https://www.nasc.gov.au/reports-and-publications/fusion-cells.

18 ASIC provided content for this information box.

Consistent with the whole of ecosystem approach to combating scams, in 2024 the digital industry, including social media platforms and messaging applications, played an important role in protecting Australians from scams. The National Anti-Scam Centre invited peak industry body, Digital Industry Group Inc. (DIGI),[19] to highlight key anti-scam initiatives in 2024. Their contribution is set out below.

Examples of anti-Scam initiatives: Digital Industry Group Inc. (DIGI)[20]

On July 26 2024, DIGI launched the voluntary Australian Online Scams Code,[21] signed by Apple, Discord, Google, Meta, Snap, TikTok, Twitch, X and Yahoo as initial signatories, and is open to others in the digital industry. The code's commitments span nine key areas:

- Blocking: Measures to detect and block suspected scams.
- Reporting: A route for users to report possible scams.
- Takedowns: Action against verified scam content and scammers.
- Advertising: Measures to protect people from scam advertising.
- Email and messaging: Specific measures to protect people from scams in emails and private messages.
- Law enforcement: Engaging with law enforcement efforts to address scams.
- Intelligence sharing: Contribute to public-private and cross-sectoral initiatives to address scams.
- Communications: Provide information about scam risks and support counter-scam efforts.
- Future proofing: Contribute to strategy development and future proofing exercises.

Some examples of initiatives that signatories have implemented since the code was announced include:

- The Fraud Intelligence Reciprocal Exchange (FIRE), a scam reporting channel where banks share information about known scams with Meta, via the AFCX.[22]
- In October 2024, Google announced the Global Signal Exchange, a partnership with the Global Anti-Scam Alliance and DNS Research Federation, aiming to improve the exchange of abuse signals, enabling faster identification and disruption of fraudulent activities across various sectors, platforms and services.
- In December 2024, Meta commenced new verification requirements for advertisers wanting to promote ads of financial services and products to Australians on Facebook and Instagram.[23]

19 DIGI is a not-for-profit industry association for the digital industry in Australia, see https://digi.org.au/ (accessed 16 February 2025).

20 DIGI provided content for this information box.

21 The AOSC establishes consumer protections and a blueprint for combatting scams in the digital industry in advance of the Government's forthcoming reform agenda in relation to scams, where mandatory codes are intended for banking, telecommunications and digital platforms. The full measures signatories have committed to are outlined within the Australian Online Scams Code, which is available at digi.org.au/scams.

22 Meta released initial results from the program in October 2024; Between April and May 2024, 102 reports were provided by the AFCX on behalf of onboarded banks, enabling Meta to remove over 9,000 spam pages and over 8,000 AI-generated celeb bait scams across Facebook and Instagram.

23 As part of the requirements, advertisers will need to verify information about who is the beneficiary and payer of each financial services ad, including their Australian Financial Services Licence number, if applicable. This initiative takes full effect from the end of February 2025.

Collaboration with law enforcement agencies

The National Anti-Scam Centre works with the Australian Federal Police (AFP), including by staff secondment to the AFP-led Joint Policing Cybercrime Coordination Centre (JPC3), and AFP membership of the National Anti-Scam Centre Advisory Board and working groups. Participation in the JPC3 allows the National Anti-Scam Centre to rapidly share information across government, industry and law enforcement, supporting scams disruption and prevention efforts.

Significant law enforcement operations where the National Anti-Scam Centre provided support include:

- Operation NEBULAE: led by EUROPOL and the United Kingdom's Metropolitan Police, targeting LabHost, a suspected one-stop-shop for phishing services. LabHost enabled cybercriminals to replicate the websites of over 170 banks, government entities, and other businesses.[24] On 17 April 2024, the JPC3, AFP and state police, executed 22 search warrants across 5 states targeting users of LabHost's services. The same day, JPC3 partner agencies, including the National Anti-Scam Centre, provided real-time intelligence to officers in the field, ensuring operational decisions were shaped by up-to-date and accurate information. The operation led to 5 arrests as well as the takedown of LabHost's domain and 207 web servers hosting phishing websites.
- Operation FIRESTORM: an ongoing global operation led by the AFP to disrupt organised crime networks in Southeast Asia and Eastern Europe from large scale call centre scams targeting Australian consumers and business. The National Anti-Scam Centre continues to provide intelligence support to Operation FIRESTORM to generate leads and identify opportunities to disrupt scam networks.

The National Anti-Scam Centre also worked with ASIC and the AFP to develop processes for receiving and actioning large data sets provided by international law enforcement partners that contain information about Australian victims of scams.

- Since March 2024 the National Anti-Scam Centre has individually notified nearly 37,000 Australians via email and bulk SMS that they may have been impacted by investment and romance scams. The notification campaigns advised victims to cease investing further funds, seek support from their banks and referred victims to identity protection and crisis support services.

International engagement

As scams are a global threat, international cooperation and collaboration is an important enabler of scams disruption and prevention. In 2024, the National Anti-Scam Centre has continued to strengthen international partnerships with a focus on strategic and targeted international engagement.[25]

Highlights from 2024 include:

- With government and industry representatives, learning more about the Singapore Government's anti-scam activities and sharing with Singapore some of the lessons learned in Australia, including the operation of fusion cells.
- Participating in knowledge sharing opportunities such as the International Consumer Protection and Enforcement Network (ICPEN) annual conference.[26]

24 For further information regarding Operation NEBULAE refer to Case study: collaborating with law enforcement found in: ACCC, National Anti-Scam Centre in Action (November 2024) p. 18.

25 UK agencies include UK Finance, the National Economic Crime Commission, Stop Scams UK, and the Credit Industry Fraud Avoidance System (Cifas). The National Anti-Scam Centre has provided briefings to officials from Thailand, Vietnam, Philippines, Malaysia, Maldives, Ireland and New Zealand on how the centre was established, operations, scam trends, initiatives and innovations.

26 In September to hear from the Federal Trade Commission (FTC) on the 'human side' of scam conduct and the 'upstream' side of scams.

- Delivering an anti-scams workshops supporting the Association of Southeast Asian Nations (ASEAN) member states to uplift consumer protection efforts,[27] and with ASIC in Vietnam.[28]
- Presenting the National Anti-Scam Centre's work at the Global Anti Scam Summit in Singapore.

The National Anti-Scam Centre puts Australia at the forefront of the fight against scams. Through our international engagement, the National Anti-Scam Centre has shared insights and lessons learned from our first full year of operations, and gained knowledge from international partners, positioning Australia as a world leader in the anti-scam space. By contributing to these global initiatives, the National Anti-Scam Centre supports other nations to implement effective anti-scam measures thereby protecting Australians from scams.

Consumer awareness

Community engagement

The National Anti-Scam Centre is committed to increasing consumer awareness to empower Australians to identify, avoid and report scams. In 2024, the National Anti-Scam Centre updated the design of the Scamwatch website to improve the online experience for consumers and launched new Scamwatch Instagram and NASC LinkedIn channels.

National Anti-Scam Centre channels target government and business stakeholders while Scamwatch channels target consumers. The ACCC Facebook and Instagram channels are also leveraged to reach a broader consumer audience with high priority anti-scam messaging.

Engagement with Scamwatch/National Anti-Scam Centre websites

5,622,516 views^ of Scamwatch website
from 1,433,316 users^^ (approx)

81,468 views of National Anti-Scam Centre website*
from 48,766 users (approx)

^Views: The number of pageviews on the website. A single user can have multiple page views.
^^Users: The number of distinct users who visited the website.
*The National Anti-Scam Centre website launched on 30 July 2024.

Reach and impact of Scamwatch, National Anti-Scam Centre and ACCC social media[x]

500+ posts

1.5k shares/reshares

800k impressions

Almost **35k** engagements

x Includes Scamwatch Instagram, National Anti-Scam Centre LinkedIn and X, ACCC Facebook and Instagram.

27 This workshop was delivered in May as part of the ACCC's Consumer Affairs Program supporting Association of Southeast Asian Nations (ASEAN) member states. ASEAN member states in attendance included Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Thailand, and Vietnam.

28 This workshop was delivered in October jointly with ASIC.

Supporting people and communities to stay safe from scams

A principal objective of the National Anti-Scam Centre is to empower people who may face barriers or increased risk of harm to identify and avoid scams by developing high quality and accessible information. This approach focusses on First Nations communities, older Australians, youth and children, people from culturally and linguistically diverse backgrounds, those living with a disability, and small businesses.

Outreach initiatives focused on at-risk groups in 2024 include:

- Working in partnership with the Department of Employment and Workplace Relations to produce scams awareness material for participants in the Pacific Australia Labour Mobility (PALM) scheme.[29]
- A radio campaign, developed in partnership with First Nations radio stations. The campaign had a potential reach of more than 17,000 and was designed to uplift scams awareness among First Nations audiences living in remote communities.
- The National Anti-Scam Centre's flagship publication The *Little Book of Scams: How to spot and avoid scams* is now available in 17 languages other than English.[30] It is recognised internationally as an important tool for consumers and small businesses to learn about scams, including the most common scams for which to be vigilant, the warning signs and how to protect yourself against scams.

Community, consumer, and industry initiatives

72 Scams awareness community presentations

36 presentations to government and industry

Little Book of Scams distribution:

169,471 printed copies

3,756 downloads*

*Total downloads include: 2,792 in English, 283 In-Language and 681 Easy Read versions

In November 2024, the National Anti-Scam Centre engaged with some of Australia's largest retailers regarding gift cards and measures they could implement to improve consumer awareness of gift card scams. To ensure consistent public messaging, the National Anti-Scam Centre distributed Scamwatch branded point of sale signage to retailers for use in stores and are currently engaging with these retailers on further protective measures they could implement to reduce the impact of scams. Further measures include: placing restrictions on the number of gift cards purchased in a single transaction, sales warning prompts on both assisted and self-checkouts, audio scripts for in-store warning, internal communications for retail staff raising gift card scam awareness and training.

Scams Awareness Week and national media campaign

This year's Scams Awareness Week ran from 26 to 30 August with the theme, 'Share a story, stop a scam.' The theme aimed to reduce the stigma of being scammed and help empower people to identify, avoid and report scams. Scams Awareness Week was co-designed with members of the National Anti-Scam Centre Communications and Awareness Working Group Design Team.[31]

29 The aim of this work is to reduce the number of PALM workers targeted by scammers, particularly in-person scams in which personal information and bank details are stolen.

30 The Little Book of Scams is now available in: Arabic, Cantonese, Croatian, Dari, English, Farsi, German, Greek, Hindi, Indonesian, Italian, Korean, Macedonian, Mandarin, Spanish, Tagalog, Turkish, and Vietnamese. In-language videos are available in: Arabic, Cantonese, Croatian, Dari, English, Farsi, German, Greek, Hindi, Indonesian, Italian, Korean, Macedonian, Mandarin, Spanish, Tagalog, Turkish, and Vietnamese.

31 Members of the National Anti-Scam Centre Communications and Awareness Working Group Design Team include: Westpac, COBA, Pivotel, Services Australia, ATO, ASIC, ANZ, Digi, IDCARE and Monash University (Monash University neuropsychologist and scams researcher Dr Kate Gould).

Social and digital platforms, banks, telcos, law enforcement, government agencies and non-profit organisations supported Scams Awareness Week.

Scams Awareness Week

26–30 August:
'Share a story, stop a scam'

16m
estimated audience reach through television and radio

64%
higher engagements (shares, comments, reactions) with Scams Awareness Week social media posts

The Australian Government funded the National Anti-Scam Centre to develop the 'fighting scams campaign' to raise community awareness of scams and communicate protective behaviours to guard against scammers. The 'Stop. Check. Protect.' campaign seeks to tackle the threat of scams by educating the community about sophisticated scam tactics, reminding people that anyone can be vulnerable to scams, and empowering victims to report scams to Scamwatch. The campaign was developed in 2024 and is running during first half of 2025. The campaign focus is to drive behavioural change through heightened awareness, challenging optimism bias and helping consumers feel supported to confidently identify, avoid and report scams.

The National Anti-Scam Centre continues to invest in supporting publicly available scams data via the dashboard.[32] The dashboard provides access to transparent and up to date scams data and has been used by a number of stakeholders including media, government, community organisations, private sector and academic researchers.

In 2024 consumer research organisations played an important role ensuring consumer voices and perspectives inform and influence anti-scam efforts. The National Anti-Scam Centre invited CHOICE[33] to highlight important anti-scam initiatives in 2024. Their contribution is set out below.

Consumer research: CHOICE[34]

CHOICE advocates for stronger scam protections for consumers, including through representing the Consumers' Federation of Australia on the National Anti-Scam Centre Advisory Board, and through original research and consumer advocacy.

CHOICE conducted quantitative and qualitative research on the experiences of bank scam victims in Australia, surveying over 200 people who had money stolen via bank transfer or debit card scams. CHOICE's 'Passing the Buck' report, released in May, tracked the entire scam journey of victims, revealing how easy it is to become a victim. CHOICE's report noted inconsistent and inadequate responses from banks to detect, prevent and respond to scams, and how many victims were left feeling unsupported and suffering negative impacts on their lives.

In June, CHOICE delivered a petition signed by over 26,000 people calling on the Government to introduce strong rules to force businesses to detect and prevent scams – and require compensation for scam victims.

32 See https://www.nasc.gov.au/scam-statistics.

33 CHOICE is a leading consumer research and advocacy group, see https://www.choice.com.au/ (accessed 16 February 2025).

34 CHOICE provided content for this information box.

Victim support

Victim referrals and responses

In 2024 the National Anti-Scam Centre (through a data sharing arrangement) referred 7,670 Scamwatch reporters to IDCARE for tailored and timely scam recovery support.[35] The National Anti-Scam Centre also engaged with over 1,300[36] scam victims via tailored emails and phone calls; this is in addition to the bulk email and SMS alerts sent in collaboration with the AFP referenced in the Disruption section above. The tailored emails and phone calls:

- direct victims to support services to prevent further harm
- offer peace-of-mind to victims who feel threatened
- give advice to concerned friends or relatives to help them discuss scams with a victim they care about
- provide other advice unique to their situation.

In providing this support, the National Anti-Scam Centre recognises the impact on scam victims often goes well beyond financial loss and can inflict devastating emotional harm. Many Australians have experienced significant harm to their mental health after experiencing financial crime. Victims of scams may be referred to crisis support services such as **Lifeline – 13 11 14** and **Beyond Blue – 1300 22 4636** by National Anti-Scam Centre and the Scamwatch service. In many cases these victims need ongoing mental health support to recover.

Support for scam victims

Legislative reform: Scams Prevention Framework

The ACCC strongly supports the establishment of an ecosystem-wide, mandatory, consistent and enforceable regime to effectively address and reduce scam activity in Australia,[37] and so welcomed the *Scams Prevention Framework Act 2025*.

The Scams Prevention Framework sets out key obligations on regulated entities, introducing civil penalties for non-compliance. The relevant Treasury Minister can designate participants within sectors of the economy to be 'regulated entities', which will be subject to the Scams Prevention Framework obligations. The Government has committed to first designating banks, telecommunications, and certain digital platforms (initially including social media, paid search advertising and direct messaging services).

35 Reporters who opt-in to the referral process are contacted by IDCARE after submitting their Scamwatch report. IDCARE offers advice and directions on how the victim can recover from the scam, and how they can protect themselves from scams in future.

36 This is in addition to victim contacts made in cooperation with law enforcement outlined in the Disruption section of this report.

37 ACCC, Submission in response to Treasury's Scams Prevention Framework – Exposure Draft (4 October 2024), p. 1 and ACCC, Scams Prevention Framework: ACCC Submission to the Senate Economics Legislation Committee inquiry into the Scams Prevention Framework Bill 2024, (20 December 2024), p. 1.

The Scams Prevention Framework sets out principle based obligations that require regulated entities to take reasonable steps to prevent, detect, disrupt, report and respond to scams, and establishes governance and reporting processes to support these obligations.

The Scams Prevention Framework also establishes a single external dispute resolution scheme (to be operated by the Australian Financial Complaints Authority for at least the first three designated sectors), offering scam victims an avenue to have their complaints heard by an independent third party and to seek compensation.

The ACCC has provided views to Treasury through its consultation on the Scams Prevention Framework[38] and will have a key role as the Scams Prevention Framework general regulator, monitoring and enforcing compliance.

The ACCC is continuing preparatory work to effectively implement the Scams Prevention Framework.

More information about the Scams Prevention Framework is available on Treasury's website.[39]

In 2024, victim support and consumer advocacy organisations played an important role in helping scam victims recover, both financially and emotionally, from the impact of scams. The National Anti-Scam Centre invited the Consumer Action Law Centre[40] (CALC) to describe key scam victim support initiatives in 2024. Their content is set out below.

Victim Support and Consumer Advocacy: Consumer Action Law Centre[41]

Consumer Action Law Centre led campaign advocacy about scams on behalf of the sector in 2024, with two major submissions and called for legislation to protect consumers from scams and ensure scam victims are compensated by industry.

By supporting clients to tell their own stories, the campaign has reframed the public narrative moving discussion away from victim-blaming and instead looking at the broader ecosystem required to disrupt scams, starting with the role of industry to do more to prevent them.

Consumer Action Law Centre also supported a group of over 80 HSBC customers, many of whom had had their entire life savings stolen in a sophisticated scam across mid/late 2023 to early 2024. Consumer Action Law Centre raised deep concerns about HSBC's prolonged failure to prevent or respond to the scam with various regulators including the ASIC, the ACCC and the Australian Prudential Regulation Authority.

In December 2024, ASIC took enforcement action, suing HSBC Bank for its 'widespread failures to act honestly, efficiently and fairly' and protect hundreds of its customers from scams.

38 ACCC engagement included making two public submissions in response to Treasury's then-named Scams Code Framework discussion paper, and the subsequent Exposure Draft of the Scams Prevention Framework. Refer ACCC, Submission in response to Treasury's Scams Prevention Framework – Exposure Draft (4 October 2024), and ACCC, Scams Prevention Framework: ACCC Submission to the Senate Economics Legislation Committee inquiry into the Scams Prevention Framework Bill 2024, (20 December 2024).

39 Department of the Treasury, Scams Prevention Framework – Protecting Australians from scams, https://treasury.gov.au/publication/p2025-623966.

40 The Consumer Action Law Centre is a campaign-focused consumer advocacy organisation, see https://consumeraction.org.au/ (accessed 16 February 2025).

41 The Consumer Action Law Centre provided content for this information box.

Looking forward

As the National Anti-Scam Centre moves into its second year of operation, it will maintain a focus on providing better protection for consumers and business. A key focus in 2025 will be to consolidate existing data sources into a combined data set, to enable greater analysis informing scams prevention and disruption, consumer awareness and victim support.

Critical to this will be preparations for the Scams Prevention Framework, including further investment in technological capabilities to support secure sharing and storage of data and the onboarding of industry data partners in readiness of new data-sharing obligations. As part of the investment in this technology uplift, in 2025 the National Anti-Scam Centre will continue to explore artificial intelligence and machine learning opportunities to proactively scan for, identify and help disrupt scams. The National Anti-Scam Centre will continue to work to make it easier for Australians to report scams through Scamwatch.

As additional stakeholders collaborate with the National Anti-Scam Centre to share data, anti-scam efforts across the ecosystem will be strengthened. Through the near real-time sharing of actionable data and by receiving intelligence from across industry and government, the National Anti-Scam Centre will provide enhanced prevention and disruption of scams and deliver better protection for consumers and business. Our focus for 2025 includes prioritising working with industries to be regulated under the Scams Prevention Framework, namely banking, digital platforms and telecommunications providers.

Throughout 2025 we will continue to develop consumer awareness activities aimed at assisting consumers to identify and avoid scams. The national media campaign in the first half of 2025 and Scams Awareness Week later in the year will drive community awareness of scams and communicate protective behaviours to guard against scammers. The National Anti-Scam Centre community outreach will strengthen existing relationships and collaboration with key stakeholders such as Services Australia, ASIC's Moneysmart, eSafety Commissioner, National Disability Insurance Scheme, industry and law enforcement to maximise our reach to build scam resilience for at-risk members of our community.

In the light of the successful collaboration with the JPC3 in 2024, the National Anti-Scam Centre is committed to its continued staff secondment and support for cooperation with law enforcement. The National Anti-Scam Centre will also participate in the Singapore Police-led Frontier+ initiative bringing together anti-scam units across the Asia Pacific region to tackle transnational scams. In 2025, the National Anti-Scam Centre will continue to learn from, and contribute to, global anti-scam efforts, through participation in global forums and ongoing engagement with key international stakeholders.

Appendix 1 – Scamwatch data and observations

All data presented in Appendix 1 relates to reports submitted to Scamwatch only.

Report and loss statistics

Scamwatch is a detailed data source that includes information about scam types, victims affected, communication and payment methods used by scammers, and information about the backgrounds of reporters and victims. Importantly, around 90.0% of reports to Scamwatch are from people who have not suffered a financial loss. This data enables further exploration of trends in scam categories, methods, and impacted communities.

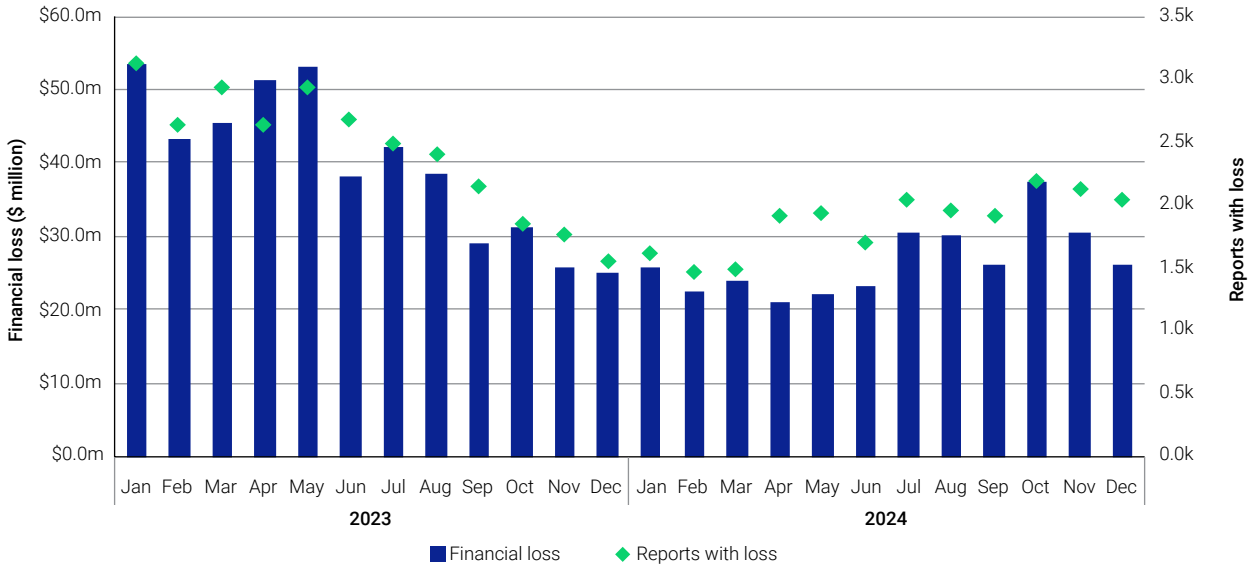
Scamwatch data is a subset of total combined losses reported to Scamwatch, ReportCyber, AFCX, IDCARE and ASIC, so caution should be exercised in making definitive statements about total losses and trends based upon Scamwatch data alone. Of the various data sources in this Report, in 2024 Scamwatch data comprised 47.4% of all reports and 12.9% of all loss.

Scamwatch received 249,448 reports in 2024, a 17.3% decrease compared with 2023. Over 22,400 reports (approximately 9.0%) included a financial loss in 2024, compared to 9.7% in 2023. Financial losses reported to Scamwatch decreased by 33.1% compared with 2023, dropping from $476.8 million in 2023 to $318.8 million in 2024. However, the Scamwatch median loss did not change from $500.

In mid-2024 the National Anti-Scam Centre introduced a pilot program testing two short form reporting options for scam ads and URLs, making it easier for consumers to report to Scamwatch. Since implementing the two report forms, a total of 2,241 reports have been received through Scamwatch, 1,026 using the ad form and 1,215 using the website form. Verified scam website URLs from these forms are referred by the National Anti-Scam Centre for assessment for takedown, further disrupting the ability of scammers to contact consumers.

Losses reported to Scamwatch

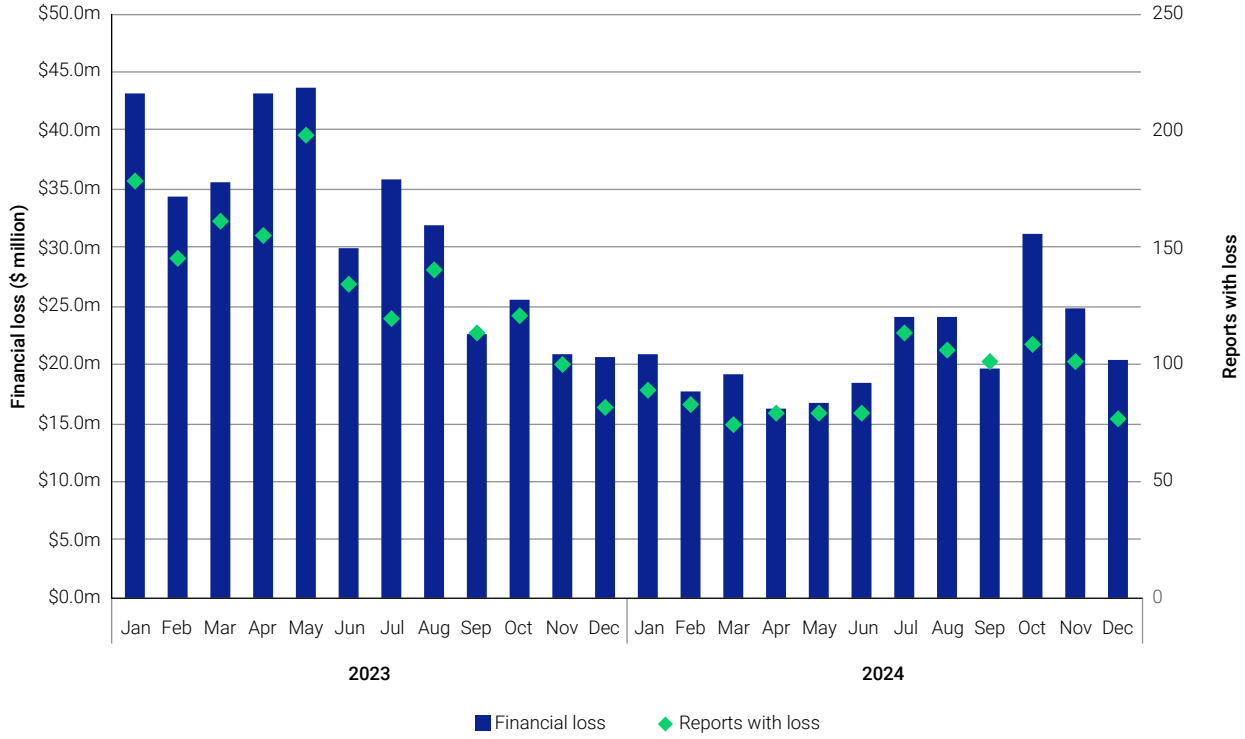
Figure 1: Losses and reports with loss by month 2023–2024



The National Anti-Scam Centre has observed that there may be several factors contributing to the decrease in reporting between 2023 and 2024 including:

- An increase in the sophistication of scams, making it harder for consumers to recognise significant scams and report them. This is why the National Anti-Scam Centre continues to collect and share data and intelligence across the scams ecosystem, which informs public scam alerts and other awareness-raising activities.
- An increase in the promotion of a variety of reporting channels including direct to specific businesses in the ecosystem. Organisations such as the National Anti-Scam Centre routinely include IDCARE's phone number and information on our consumer and victim information.
- A decrease in consumers experiencing scams possibly due to scam prevention initiatives such as improved call and SMS blocking, phishing filters and fraud monitoring.
- Public awareness and education assisting consumers to identify scams.
- The potential for report fatigue highlights the need for our continued focus on user experience for consumers reporting through Scamwatch.

Figure 2: Number of reports in 2024 by month, where losses per report were $50k or higher



Scamwatch data shows that from January to June 2024, 10,132 people reported losing money, while from July to December this increased to 12,276 people reporting losses. Median losses also increased in the second half of the year, as did reports of financial loss to investments scams and phishing scams. The slight uptick in the latter part of 2024 highlights the need to continue to uplift scams prevention, including through the Scams Prevention Framework which will impose consistent and enforceable obligations across the scams ecosystem.

Scam categories reported to Scamwatch

The most reported scams in 2024 were phishing scams. Scamwatch received 97,831 reports about phishing scams, a decrease of 9.9% compared to 2023. Despite being the most reported scam only 1.5% of people reporting phishing scams reported a financial loss.

More Australians reported a financial loss to shopping scams[42] compared to any other scam type in 2024 as observed in Scamwatch data. There were 10,022 Australians who reported a loss to shopping scams, reporting total overall losses of $9.8 million in 2024. This is a 24.2% decrease from the 13,213 who reported financial loss to shopping scams in 2023.

42 Shopping scams includes the Scamwatch categories: online shopping scams and classified scams.

Figure 3: Top scam categories by reports with loss

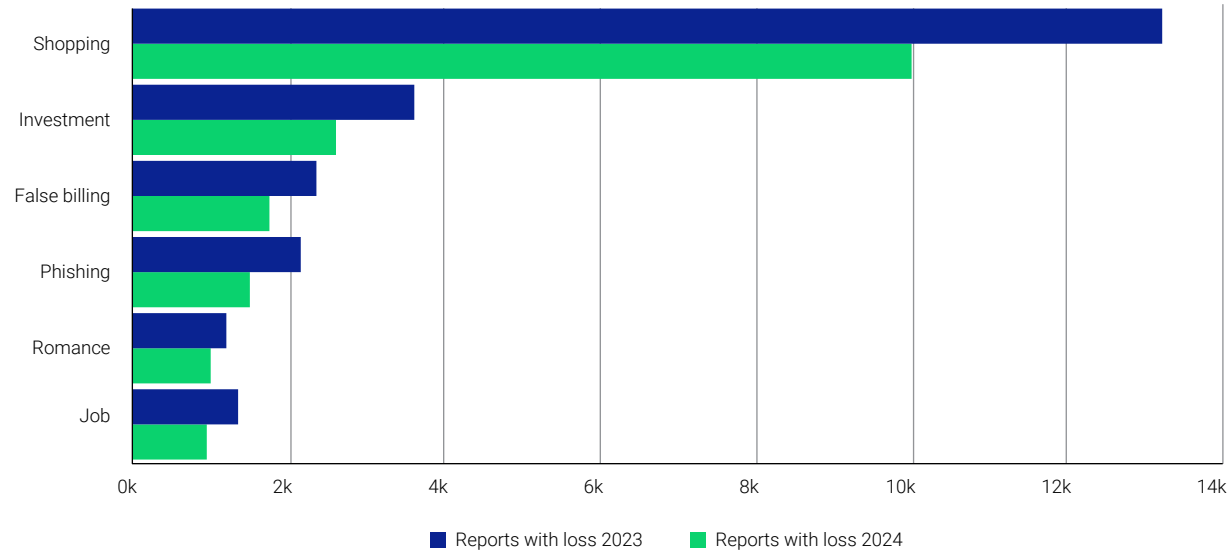
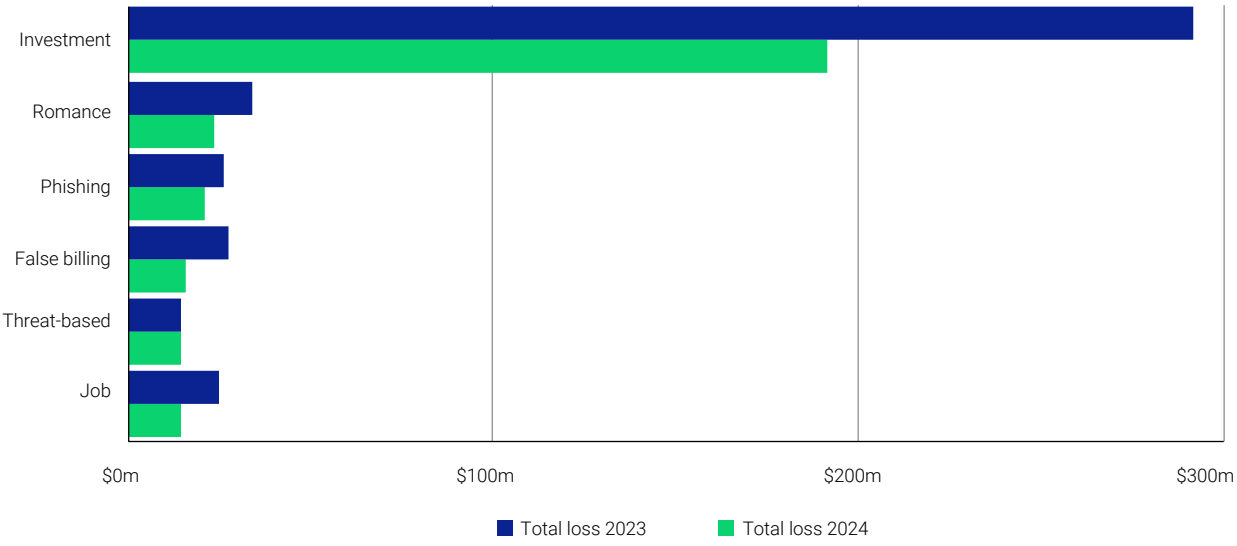


Figure 4: Top scam categories by overall loss



Investment scams led to the highest overall losses ($192.3 million), although the amount lost decreased by 34.1% compared with 2023. The top five scam categories by loss accounted for 83.5% of the total loss reported to Scamwatch in 2024. Most scam types saw a decrease in overall reported losses, but there were some exceptions.

There was a 26.6% increase in reported losses for unexpected money scams and while fewer people reported a loss, where they did lose money, they lost significantly more with median losses doubling in 2024. Scams contributing to the increase in losses associated with unexpected money scams are 'Grant scams'[43] on Facebook and a small number of very large loss inheritance scams.

43 Grant scams involve individuals being told they are eligible for a grant or similar financial incentive; usually by a trusted contact whose social media account has been taken over by the scammer. Attempting to access the 'grant' involves an infinite series of fees and up-front payments.

There was an increase of 8.3% in reports about threat-based scams[44] from 5,607 in 2023 to 6,071 in 2024. Losses remained stable at $13.9 million. There were fewer reports with loss, but where people lost money, the amount lost increased (the median loss doubled from $1,500 in 2023 to $3,220 in 2024).

Contact methods reported to Scamwatch

While the most frequently reported contact method in 2024 was email (90,819), only 3,459 people reported losing money. Comparatively, the most reported contact method leading to financial loss was social media and more people lost money in 2024 than 2023. There were 7,724 reports about social media scams with financial loss in 2024, just over the 7,706 reported 2023. Social media scams led to overall losses of $69.5 million (a decrease in overall losses from the $93.5 million in 2023), the median loss being $330.

Phone scams had the highest overall losses with $107.2 million reported lost across 2,179 reporters. Scamwatch data suggests that phone scams tend to lead to higher individual losses, with a median loss of $3,900.

The contact method that saw the largest decrease in financial loss was internet, with losses decreasing by almost 61.0% from $69.7 million to $27.2 million. The largest decrease in reports with loss was also internet, almost 40.0% (8,124 reports with loss to 4,889 reports with loss).

Figure 5: Top contact methods by number of reports with loss

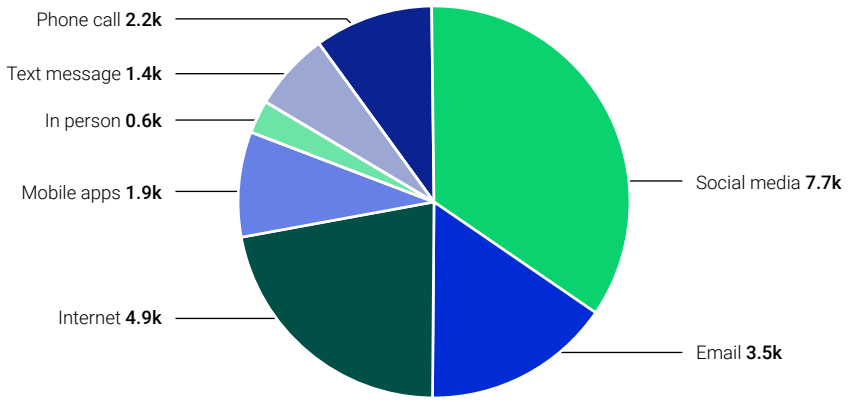
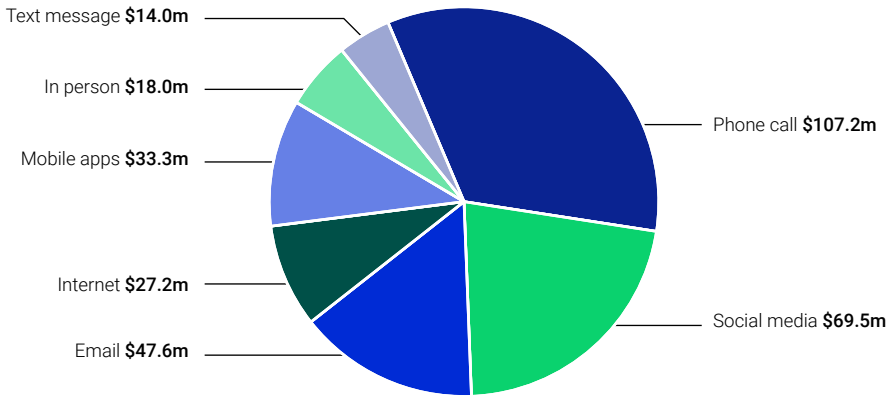


Figure 6: Top contact methods by overall loss



44 Threat-based scams include threats to life, arrest or other in Scamwatch categories.

The only contact method for which total number of reports to Scamwatch increased was via email, with a 5.7% increase from 85,935 to 90,819, continuing the trend from the increase observed in 2023.

The increase in email scams was partly driven by bulk extortion emails, and specific scam campaigns where scammers impersonated government entities such as myGov, the Australian Taxation Office (ATO) or Services Australia. In 2024, there were over 23,700 reports to Scamwatch of scams impersonating myGov, the ATO or Services Australia (and associated services such as Centrelink), with losses of $4.0 million.

Payment methods reported to Scamwatch

Consistent with payment methods in 2023, the most reported payment method in 2024 was bank transfer (7,943 reports) which accounted for 44.5% of overall losses with $141.7 million reported lost.[45]

Figure 7: Top payment methods by number of reports

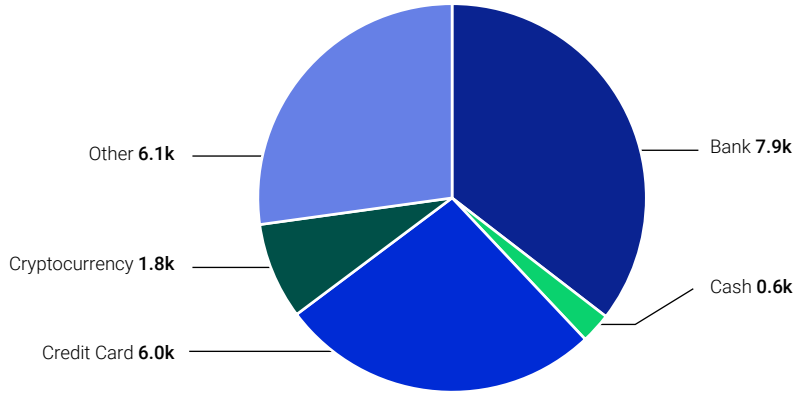
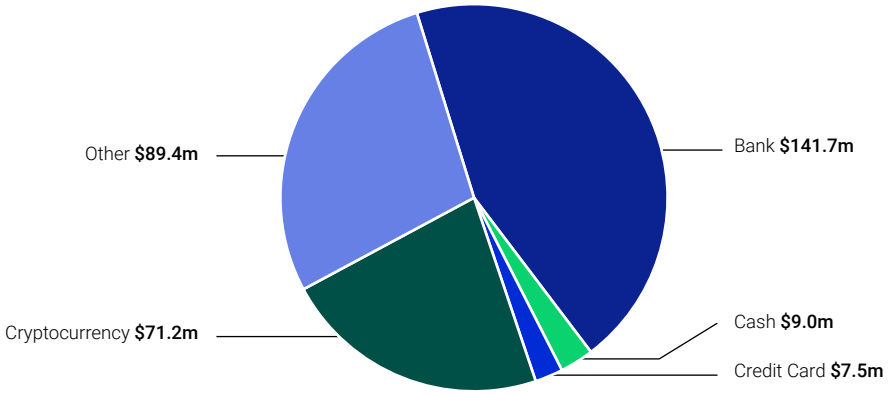


Figure 8: Top payment methods by overall loss



45 In 2024, the Scamwatch Report a Scam Form was updated to allow reporting of multiple bank transactions. Cryptocurrency payments i.e. pure cryptocurrency payments via wallets were captured in a new way to facilitate better sharing with cryptocurrency platforms. The data combines 'pure cryptocurrency' with Digital Currency Exchanges (DCE) which may include bank transfers to purchase cryptocurrency.

People and communities at increased risk of harm from scams

Anyone can experience a situation which may result in exposure to a scammer where their ability to prevent financial loss or harm is limited. Education level, status, wealth, employment, age, health and culture do not provide immunity from scams. Given the right set of circumstances, it can happen to anyone.

However, some people and communities face significant barriers and circumstances that can make them more vulnerable to a scam (for example, those experiencing inadequate housing, financial constraints, poverty, food insecurity, or poor health). They may also be disadvantaged by inequality and systems, which can lead to increased risk of harm from scams. Many communities and demographics may face significant barriers to accessing information which could assist them to avoid scams and may also find it difficult to report a scam. This can make it harder for them to manage the effects of the scam including by seeking assistance.

While analysing Scamwatch data regarding communities at increased risk of harm from scams is important, in some instances the data sample size is small relative to the complete Scamwatch data; consequently, caution should be exercised when drawing conclusions from a relatively small sample size.

Reports to Scamwatch by people from First Nations communities

People identifying as First Nations[46] reported fewer scams to Scamwatch in 2024 with 4,254 reports compared to 6,192 in 2023. Of these 661 reported a financial loss compared to the 693 in 2024. The median loss in 2024 was $500. Overall reported losses increased by 73.1% to $6.5 million (from $3.8 million in 2023). This increase was largely driven by a greater number of high loss reports across First Nations reporters. In 2023, there were 16 reports with losses of $50,000 or more, in 2024 this increased to 27.

Other reasons for the increase include an increase in the number of people reporting losses to betting and sports investment scams (6 in 2023 to 36 in 2024). The median loss increased 63.9% from $610 to $1,000 in 2024. Overall losses were $221,148 (up from $5,337 in 2023). Given the relatively small numbers of reports from people identifying as First Nations, it is difficult to draw trends from the data. Building on the Stop. Check. Protect. Campaign, the National Anti-Scam Centre will promote content designed for First Nations people to increase scam awareness.

Most First Nations people who reported financial loss experienced shopping scams (225).[47] The contact method leading to the highest overall loss in 2024 for First Nations people was phone calls, with 64 people reporting losses of $2.6 million. However, financial loss was most reported for social media scams with 263 people reporting losses.

Reports to Scamwatch by people from culturally and linguistically diverse (CALD) communities

People reporting to Scamwatch who identified as CALD[48] made 11,666 Scamwatch reports in 2024. Of these, 1,841 people reported losing money totalling $38.8 million, a decrease of 36.0% compared

46 The Scamwatch form provides an optional field for reporters to specify if they are Indigenous.

47 Shopping scams includes the Scamwatch categories: online shopping scams and classified scams.

48 The Scamwatch form provides an optional field for reporters to specify if they speak a Language other than English. It does not ask what language or ask for information about reporters' specific cultural background.

to $60.5 million lost in 2023. The median loss in 2024 was $1,000, significantly higher than the median of $500 for all Scamwatch reporters in 2024.

Table 4: Top 5 scams by loss reported by people from CALD communities in 2024

Scam category	Reports with loss	Total loss	Median loss	% change in total loss from 2023
Investment	276	$19.5m	$10.0k	-49.3% ▼
Threat-based	60	$7.5m	$50.0k	-0.37% ▼
Romance	104	$3.8m	$1.0k	66.2% ▲
Job	178	$2.0m	$4.4k	-49.2% ▼
False billing	142	$1.3m	$1.1k	7.2% ▲

While people from CALD communities reported losing more money to investment scams, $19.5 million in 2024, threat-based scams had the highest median loss of $50,000. People from CALD communities made up 5.8% of people reporting threat-based scams, but accounted for 54.1% of losses for this scam type.

Reports to Scamwatch from people with disability

People with disability made 19,989 reports to Scamwatch in 2024. Of these, 1,758 people reported losing money amounting to $20.8 million. This represents a decrease of 32.6% on the $30.8 million lost in 2023.

The most common contact methods where people with disability lost money were social media, with 556 reports totalling $4.4 million, and internet with 359 reports totalling $3.8 million. However, phone scams led to the highest overall losses with $5.6 million lost across 190 reports.

People with disability reported more losses to identity theft in 2024, with 78 people reporting overall losses of $2.0 million. This represents an over 371.1% increase in overall losses compared to 2023. Some people reported the compromise of their government services and scammers changing where payments were sent. Financial loss to false billing scams increased 63.8% to $804,785 in 2024.

People with disability were more likely to lose money to shopping scams[49] than any other scam type with 599 reports with loss and overall losses of $630,695.

Table 5: Top 5 scams by loss reported by people with a disability in 2024

Scam category	Reports with loss	Total loss	Median loss	% change in total loss from 2023
Investment	179	$7.4m	$5.2k	-55.6% ▼
Romance	191	$4.8m	$2.5k	16.1% ▲
Identity theft	78	$2.0m	$1.0k	371.1% ▲
Phishing	124	$1.2m	$1.4k	-63.7% ▼
Inheritance and unexpected money	29	$1.1m	$2.5k	24.5% ▲

49 Shopping scams includes the Scamwatch categories: online shopping scams and classified scams.

Scamwatch reports by Australians based on age

In 2024, all age groups reported fewer scams, fewer scams with loss and lower total loss compared to 2023. People aged 65 and over had the highest reported losses of $99.6 million, 31.3% of all losses reported to Scamwatch, despite making up only 17.2% of the population.[50] This represents a 17.6% decrease in reported losses from the $121.0 million reported lost by people aged 65 and over in 2023.

People aged 65 and over had the highest median loss of $1,000, down from $1,300 in 2023, and excluding anonymous reports, they were the most likely to report a scam in 2024 with 62,147 reports.

In terms of likelihood to experience a financial loss, people aged 35–44[51] reported the most Scamwatch reports with loss, 3,755 reports with overall losses of $40.1 million.

There were significant differences in the scams leading to financial loss for different age groups. For those aged 18–24[52] threat-based scams led to the highest aggregate losses. This may be due to the large volume of both real and fake sextortion scams,[53] as well as authority scams targeting young migrants and international students. The highest loss scam type for people in the 25–34 and 35–44 age groups was investment scams, followed by jobs scams.

In older age groups, investment and romance scams led to the highest losses. People aged 55–64 reported $40.9 million in losses to investment scams, 40.2% lower than 2023, and $6.6 million in losses to romance scams, 37.8% lower than 2023. Many Australians aged 65 and older have retired and may be seeking investment opportunities, which may explain people in this age group reporting total losses to investment scams of $66.6 million, 20.4% lower than 2023.

Table 6: Top 2 scam types by overall loss for age groups in 2024

Age group	Highest loss scam type	Losses	2nd highest loss scam type	Losses
Under 18 years	Shopping[54]	$126,074	Threat-based	$32,332
18–24 years	Threat-based	$3.5m	Investment	$1.4m
25–34 years	Investment	$8.3m	Job	$3.4m
35–44 years	Investment	$21.9m	Job	$4.4m
45–54 years	Investment	$28.8m	Romance	$2.9m
55–64 years	Investment	$40.9m	Romance	$6.6m
65 and over	Investment	$66.6m	Romance	$7.8m
Unspecified	Investment	$24.6m	False billing	$3.8m

50 According to census data people aged 65 and over make up 17.2% of the population.

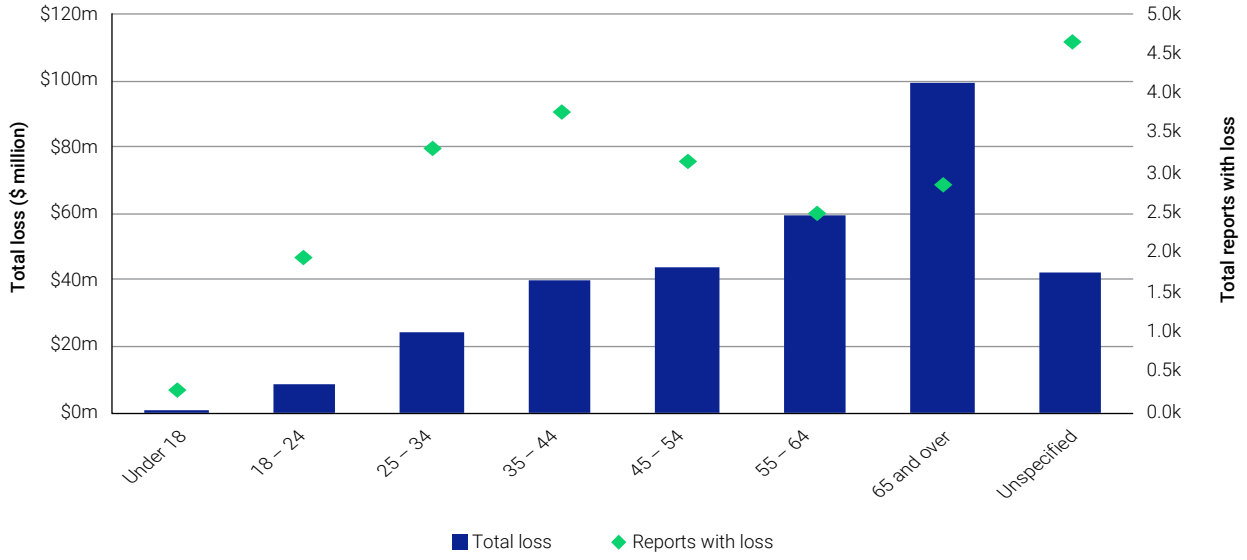
51 According to census data people aged 35–44 make up 13.7% of the population.

52 According to census data people aged 20–24 make up 6.2% of the population.

53 Fake sextortion in this context refers to scam activity where the perpetrator threatens to release explicit images or video of a victim if money is not paid, when in fact they do not have these images. Real sextortion is also known as image-based abuse where the perpetrator has images or videos that they threaten to release if money is not paid.

54 Shopping scams includes the Scamwatch categories: online shopping scams and classified scams.

Figure 9: Scam reports with losses by age group

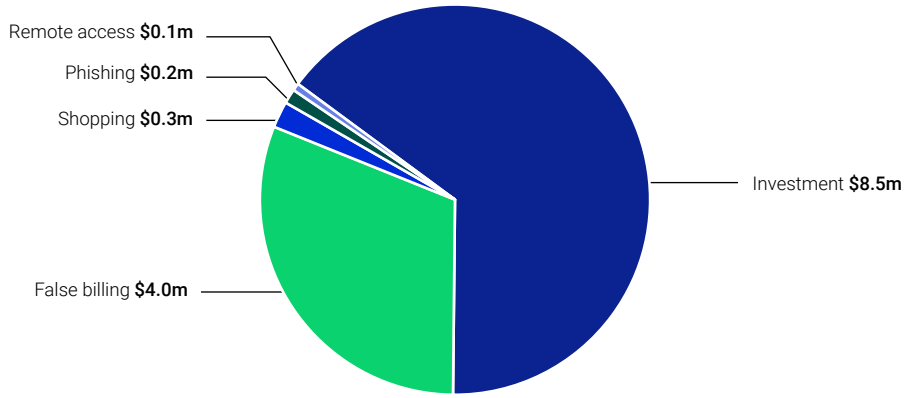


Scamwatch reports from small business

Small businesses are targeted by scammers through a variety of channels, including phishing attempts and fake invoices.[55] Small businesses lodged 1,909 reports to Scamwatch in 2024, with 258 recording financial loss amounting to $13.1 million, 24.0% lower than 2023.

Small businesses reported the highest total loss to investment scams, $8.5 million representing an increase of 78.7% from 2023. False billing was the most reported scam type both with and without financial loss. False billing reports from business generally relate to 'payment redirections' also known as 'business email compromise' scams. Small businesses reported more scams, more scam reports with loss and higher aggregate loss than medium and large businesses.

Figure 10: Top five scams by financial loss reported by small business



55 Small business includes reports from small (5 to 19 employees) and micro businesses (0–4 employees).

Appendix 2 – About the data used in this report

The data in this report is for the period 1 January to 31 December 2024. It includes 5 data sources: Scamwatch, ReportCyber, the AFCX, IDCARE, and ASIC.

In many cases there can be overlap in the scams reported to these organisations, for example, by the same scam being reported by the same person to several of the entities that record scam activity. To the extent possible, such overlaps between datasets have been identified and duplication removed, with a separate 'adjustments row' included to account for this in the totals reported throughout this report. Further information on the approach used to identify the extent of the overlap between the datasets is set out below.

In last year's dataset, the National Anti-Scam Centre received individual reports from ASIC, but in 2024 the National Anti-Scam Centre requested and received aggregated data from ASIC.

Scamwatch data

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

The National Anti-Scam Centre's Scamwatch service includes information about scam types, victims affected, communication and payment methods used by scammers, and information about the backgrounds of reporters and victims.

The validity of a loss amount and category was verified for all Scamwatch reports with losses over $1,000 until 30 September 2024, and losses over $10,000 from 1 October 2024. The move from $1,000 to $10,000 as the baseline for checking losses had minimal impact on overall loss figures and allowed analysts to focus on other priorities including the identification of emerging scam trends. The overlap between the Scamwatch report set and the ReportCyber set, IDCARE and AFCX datasets was accounted for. The process for this is described in the datasets below, except for the AFCX overlap, which was found by searching for reports involving an AFCX member bank in the Scamwatch report form (ANZ, Bendigo and Adelaide Bank, CommBank, Macquarie Bank, National Australia Bank or Westpac).

Data may change because of quality assurance processes and reporters withdrawing reports. In addition, changes were made to the Scamwatch report form which have minor impacts on the data represented on the Scamwatch public statistics page and data in this report. For example, a new field for recording cryptocurrency losses was added in March 2024, and although there was some delay in this loss data being uploaded to the public statistics page, this report and other National Anti-Scam Centre publications now include that data.

Scamwatch data is publicly available at https://www.scamwatch.gov.au/research-and-resources/scam-statistics.

Australian Signals Directorate – ReportCyber

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

Only reports in the ReportCyber dataset relating to scams (rather than other types of cybercrime) were included in this report. Throughout the year, high loss reports in ReportCyber of $1 million and over were reviewed for accuracy and validity, for example by checking in AUSTRAC's databases. As with Scamwatch data, analysis of the ReportCyber data in this report began from that plausible lower amount of $, rather than the initial pre-any alteration figure of $1.1 billion. The overlap between the ReportCyber and Scamwatch dataset was identified through finding reports with the same reporter's name and reported loss amount. We identified reporters making multiple reports about the same incident to ReportCyber by searching for reports by the same (non-anonymous) reporter name with the same (non-zero) amount lost. Where a duplicate report was identified, it was removed from the dataset used in this report.

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[56] 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.

IDCARE data included in this reported is limited to reports about Australians (i.e. excluding New Zealand or other international parties) of scam types. Overlap between the IDCARE dataset and other datasets was comprised of reports to IDCARE referred by any of the National Anti-Scam Centre, the ReportCyber, ASIC, AFCX members,[57] and Police services.[58]

56 For a list of organisations that use IDCARE services refer to https://www.idcare.org/about-idcare/our-subscribing-organisations accessed 10 February 2025.

57 Bendigo and Adelaide bank, ANZ Bank, the Bank of Queensland, Commonwealth Bank, Latitude Financial Services, Macquarie Bank, the National Australia Bank, Westpac Bank.

58 The Australian Federal Police, NSW Police, NT Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police, Western Australia Police.

Australian Securities and Investments Commission (ASIC)

ASIC (www.asic.gov.au) is Australia's corporate, markets, financial services and consumer credit regulator. Since November 2023, ASIC has directed consumers to report to scams to Scamwatch. ASIC and the National Anti-Scam Centre established new automated data sharing arrangements in 2024, which simplifies the process of reporting investment scams from Scamwatch to ASIC.

ASIC receives Reports of Misconduct as well as intelligence from overseas regulators which concern (mostly investment) scams. These reports comprise the data contributed by ASIC in this report.

Financial sector data

The AFCX is an independent, not-for-profit company. The AFCX provide a platform where participating organisations share and gain operational data and insights from each other. Since AFCX receives operational reports from each participant, there are several differences from Scamwatch reporting. While there is broad alignment, there may be small differences between scam categories used by AFCX and National Anti-Scam Centre. From time-to-time AFCX members identify omissions, and corrections or backloading can lead to changes in the data. Most AFCX cases report financial losses, however customers may report attempted scams to their financial institution. In some cases, the customer may recover part or all their loss, and the total reported losses are not adjusted for recoveries.

The AFCX data in this report is comprised of 2024 calendar year data from ANZ, Bendigo Bank, CommBank, Macquarie Bank, National Australia Bank, Westpac, Cuscal and COBA.[59] Three banks contributed data for part of the 2024 calendar year – Suncorp (since September), Rabobank (since October) and Bank of Queensland (since December).

Remaining ABA members and COBA members will begin reporting data over 2025. Incremental change to the data is expected as more members report. The National Anti-Scam Centre is undertaking further work with banks and the AFCX to better align data to support comprehensive reporting in the future.

The AFCX data in this report referred to includes situations where people may have also reported to Scamwatch, ReportCyber, and/or IDCARE. Capturing the extent of this overlap is described in the relevant organisation's section above.

Comparison with data outcomes in the Targeting Scams Report 2023

The 2023 Targeting Scams Report utilised the same methodologies to identify the extent of overlap between datasets. The same extent of overlap analysis was conducted on the Scamwatch, ReportCyber, ASIC, IDCARE and AFCX datasets in this Report.

The majority of the adjustments in this year's report involve overlapping reports from referrals to IDCARE also found in the referring agency's dataset. In 2023, there were fewer adjustments for this reason as the 'baseline' IDCARE data already excluded datasets from reports from other agencies.

59 The AFCX data in this report does not include data from all AFCX members. AFCX publicly list a selection of their members, including ANZ, Westpac, Commonwealth Bank, NAB, the Australian Taxation Office, the COBA, Macquarie Bank, Bendigo and Adelaide Bank, Latitude Financial Services, Optus, Australian Payments Plus and the Bank of Queensland.

In last year's dataset, the National Anti-Scam Centre received individual reports from ASIC, but in 2024 the National Anti-Scam Centre requested and received aggregated data from ASIC. This was not possible in previous years due to ASIC receiving reports of scams directly from the public, making overlap with other datasets likely. In 2024, ASIC did not take reports of scams directly from the public, instead re-directing reporters to Scamwatch.

The AFCX data contributed to this report has expanded since 2023's report with the addition of partial year data from Suncorp, Rabobank and the Bank of Queensland. The AFCX data set will continue to grow in coming years.

The National Anti-Scam Centre will continue to work with the datasets provided and to consider how best to use those to present data, including to enable comparison into the future.

Unreported losses

Not all Australians report scams. Despite the existence of multiple reporting platforms, the extent and impact of scams is under-reported, and some cohorts are markedly under-represented in official reporting figures as noted above.

The Australian Bureau of Statistics (ABS) Personal Fraud data shows that in the 2022–23 financial year (the most recent data available), 2.5% of Australians (514,300) experienced a scam.[60] Sixty nine percent of people who experienced a scam notified (or were notified by) an authority. This means that approximately 30.0% 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. Consequently, this under-reporting does not mean actual losses would be 30.0% higher if those people had reported.

60 Source: https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release accessed 7 February 2025.

Australian Government

National
Anti-Scam
Centre