Australian Government

National Anti-Scam Centre

National Anti-Scam Centre in action

Quarterly update

April to June 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

Important notice

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

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

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

ACCC 11/24_24-47

www.accc.gov.au

Contents

Introduction 1

Spotlight on scams (April to June 2024) 3

Public reporting services: Scamwatch & ReportCyber 3

Scamwatch insights and trends 3

The National Anti-Scam Centre in action 13

Prevention & Disruption 13

Consumer awareness 20

Community engagement 20

Victim support 22

Victim referrals and responses 22

Looking forward 23

Appendix 1 About the data used in this quarterly update 24

Scamwatch data 24

Australian Signals Directorate – ReportCyber cybercrime report service 24

Combined data: ReportCyber and Scamwatch 24

Financial sector data: the AFCX 25

Unreported losses 25

Appendix 2 Scamwatch Q4 Data 27

Introduction

This is the fourth quarterly update of the National Anti-Scam Centre which marks the foundation year for coordination of anti-scam activity across government, industry, law enforcement and consumer organisations in Australia. During this time the National Anti-Scam Centre has worked with over 500 organisations, including organisations involved in working groups, fusion cells, the Advisory Board and those supporting campaigns.[1]

This report includes data about scam trends from reports received in the April to June 2024 quarter (Q4). It also outlines the increased effort by the National Anti-Scam Centre to bring together data sources and intelligence from across the ecosystem to inform efforts to disrupt scams and support the public to spot and avoid scams.

Since the Federal government established the National Anti-Scam Centre, analysis of public reports to Scamwatch shows that as people continue to report scams, losses have decreased. Scamwatch received **288,604 reports** between 1 July 2023 and 30 June 2024, which was consistent with the **290,362 reports** received in 2022–23. At the same time, losses reported by the public to Scamwatch decreased by 41.0% from **$559.9 million** in 2022–23 to **$330.0 million** in 2023–24. The number of people reporting a financial loss to Scamwatch decreased by 32.0% from 32,919 in 2022–23 to 22,351 in 2023–24.[2]

The previous update by the National Anti-Scam Centre in Q3 included combined losses reported to Scamwatch, law enforcement (ReportCyber) and the Australian Financial Crimes Exchange (AFCX). In this Q4 report, the analysis confines data to public reporting services only (Scamwatch and ReportCyber). It separates the AFCX data[3] to avoid potential duplication in financial losses.[4] The detailed insights in this Q4 report are drawn from Scamwatch reports only.

Consumers report scams to a variety of different places including their bank, Scamwatch, other government organisations, and law enforcement agencies (ReportCyber). Currently scam data is sourced from a variety of organisations which understandably, and historically collect data for different purposes and use different systems. While these data sources are helpful in informing anti-scam efforts and providing insight on scam activity, there is value in continued improvements in data sourcing and analysis. As such, the National Anti-Scam Centre will continue to work over the next year to align data sources, identify duplication, bring in more data across the ecosystem and prepare to support the implementation of the Scams Prevention Framework.[5]

Through its Scamwatch service, the National Anti-Scam Centre collates and publishes scam statistics via an interactive data dashboard which is updated monthly.[6] Stakeholders can refer to the dashboard to understand broad trends in the Scamwatch data.

More businesses and government organisations sharing data with the National Anti-Scam Centre is critical to increasing the available intelligence about scam activity. Over the next six months, the

[1] Information about the key stakeholders that the National Anti-Scam Centre works with is available on the website: https://www.nasc.gov.au/what-we-do/how-were-run and https://www.nasc.gov.au/what-we-do/collaboration.

[2] Note that these figures reflect reports the National Anti-Scam Centre's Scamwatch service and do not include ReportCyber or data from any other organisation.

[3] The AFCX data for Q4 is provided in Appendix 1 to this report.

[4] The National Anti-Scam Centre has access to case level reports in the ReportCyber platform which enables it to identify duplicates. The AFCX and the banking sector do not share case level reports with the National Anti-Scam Centre therefore duplicates cannot be removed from the data. The AFCX data does not align with publicly reported data because it is based on the date of transaction rather than the date of report. Further, report numbers do not equate to individuals but to transactions.

[5] https://treasury.gov.au/consultation/c2024-573813.

[6] Scamwatch interactive dashboard: https://www.scamwatch.gov.au/research-and-resources/scam-statistics.

Scamwatch report form will undergo changes to simplify processes for consumers reporting scams and to collect better data to support disruption. The National Anti-Scam Centre is working to ensure that the best available data is relied upon to help inform the public on scam trends as well as support ecosystem wide efforts to stop the victimisation of Australians by criminals who perpetrate scams.

Looking further ahead, the Federal government is developing a new Scams Prevention Framework which is intended to place obligations on regulated entities to report suspected scams to the Australian Competition and Consumer Commission (ACCC), leveraging government investment in the National Anti-Scam Centre data and intelligence sharing infrastructure. These reporting obligations are intended to apply alongside other obligations to be placed upon designated sectors to have governance arrangements, and to prevent, detect, disrupt, and respond to scams.

This report highlights some of the key achievements in the quarter, including the implementation of automated, near real-time scams data sharing with the Australian Securities and Investments Commission (ASIC) and developing a cryptocurrency application programming interface (API) to enable data sharing with cryptocurrency platforms and digital currency exchanges.

These achievements and future initiatives help ensure the National Anti-Scam Centre has a lead role in anti-scams collaboration and is positioned as a key force in the government's fight to reduce the number of Australians harmed by scams.

Of course, more needs to be done. In the year ahead, in addition to continuing disruption efforts, a key focus will be on data sharing, improvements to data collection and enhanced coordination. The National Anti-Scam Centre will work with stakeholders to support businesses to comply with the Scams Prevention Framework once it takes effect and to develop consistent approaches to reporting on scam activity across the ecosystem.

Spotlight on scams (April to June 2024)

Public reporting services: Scamwatch & ReportCyber

The National Anti-Scam Centre collects scam reports from the public through its Scamwatch reporting service. The Scamwatch service enables the public to provide information about scams that is used to inform awareness raising activities and shared with a range of stakeholders to disrupt scams. 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).[7] This provides a more holistic picture of scam activity reported to public authorities. Information about scams data sources and the National Anti-Scam Centre's approach to data used in this report is provided at **Appendix 1**.

During Q4, Australians made **90,332 reports** to Scamwatch and ReportCyber about scams. These reports included **$233.8 million** in combined scam losses.[8] Of these, 13,825 (15.3% of all reports) had a financial loss, compared to the 13,636 (16.3% of all reports) in Q3.

Overall, there was a 7.3% increase in scam reports and a 2.4% decrease in reported losses to these public reporting services in Q4 compared to Q3. Data in Q4 indicates that the significant decreases observed in the previous quarters and across the last twelve months have slowed.

Scamwatch insights and trends

This section of the report provides information about scams as reported through the National Anti-Scam Centre's Scamwatch service.

Scamwatch is used by the National Anti-Scam Centre to monitor trends. It acts as the most comprehensive collection of information about scams and the people reporting and experiencing them in Australia. Scamwatch intelligence is shared with private and public sector organisations, reported on regularly to the National Anti-Scam Centre Advisory Board and discussed in collaborative forums to test and compare scam trends across the ecosystem. The media regularly requests information about Scamwatch reports and it is used to inform the National Anti-Scam Centre's awareness raising activities.

This report shines a light on trends in Q4, including an increase in phishing scams. Investment scams have continued to be the scam leading to the highest overall losses. The report highlights that more money overall was stolen by scammers when contact was made by phone call compared to other contact methods, that more people lost money to social media scams than any other contact method and that financial loss mostly occurred by bank transfer compared to other payment methods.

In Q4, Scamwatch received **75,372** reports about scams. Of these, 5,550 people (7.4%) reported a financial loss leading to total financial losses reported of **$66.0 million**.

The average amount lost as reported to Scamwatch was $11,889 which represents a 24.2% decrease from $15,691 in Q3. The median loss was $400.

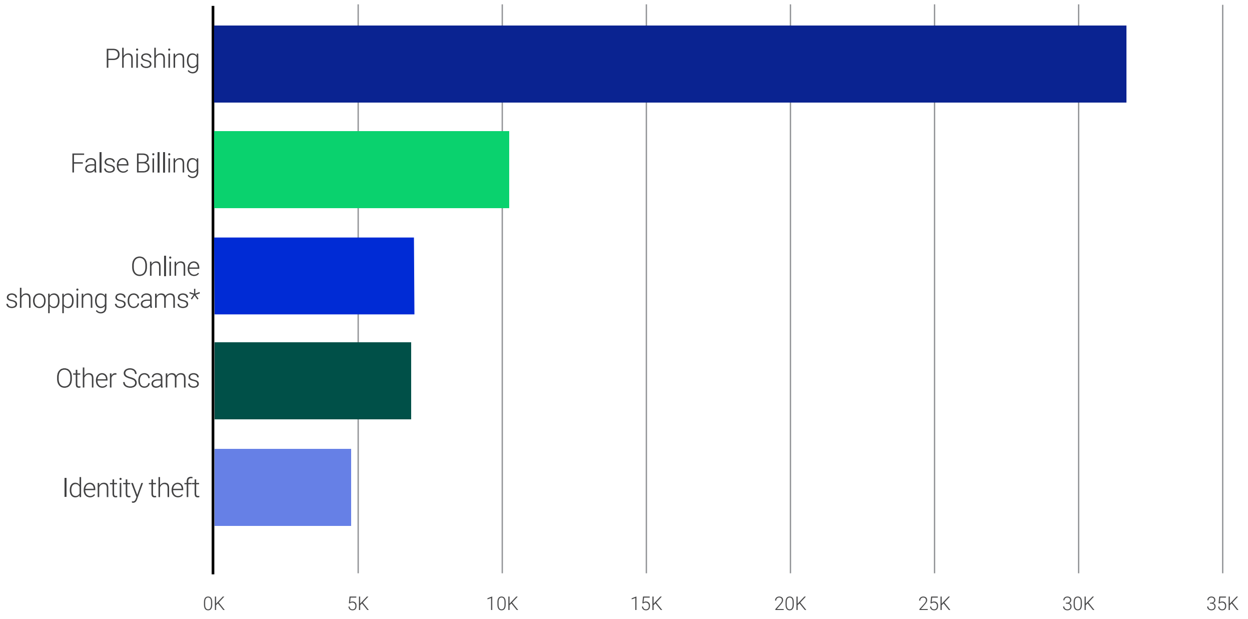
[7] Report | Cyber.gov.au.

[8] Note that the data referenced here is ReportCyber and Scamwatch combined. Data in the introduction comparing 2022–23 FY with 2023–24 FY is data from Scamwatch only.

Scamwatch data tables for Q4 are available at **Appendix 2** and further information is available to view, export and analyse via the Scamwatch website statistics page.[9]

Phishing remained the scam most reported to Scamwatch in Q4 with 31,653 reports, an increase of 13.7% from Q3.

Figure 1: Top 5 scam categories in reports to Scamwatch in Q4



* Includes classified scams

Well-known brands and government organisations continue to be commonly impersonated in phishing scams. For example, the National Anti-Scam Centre identified a trend in scams impersonating Coles Supermarkets with fake offers for redemption of Coles Rewards points. The National Anti-Scam Centre analysed several data sources, engaged with Coles and shared relevant intelligence. Coles updated the scam warning on its website and included a description and example screenshot of the scam to warn customers.

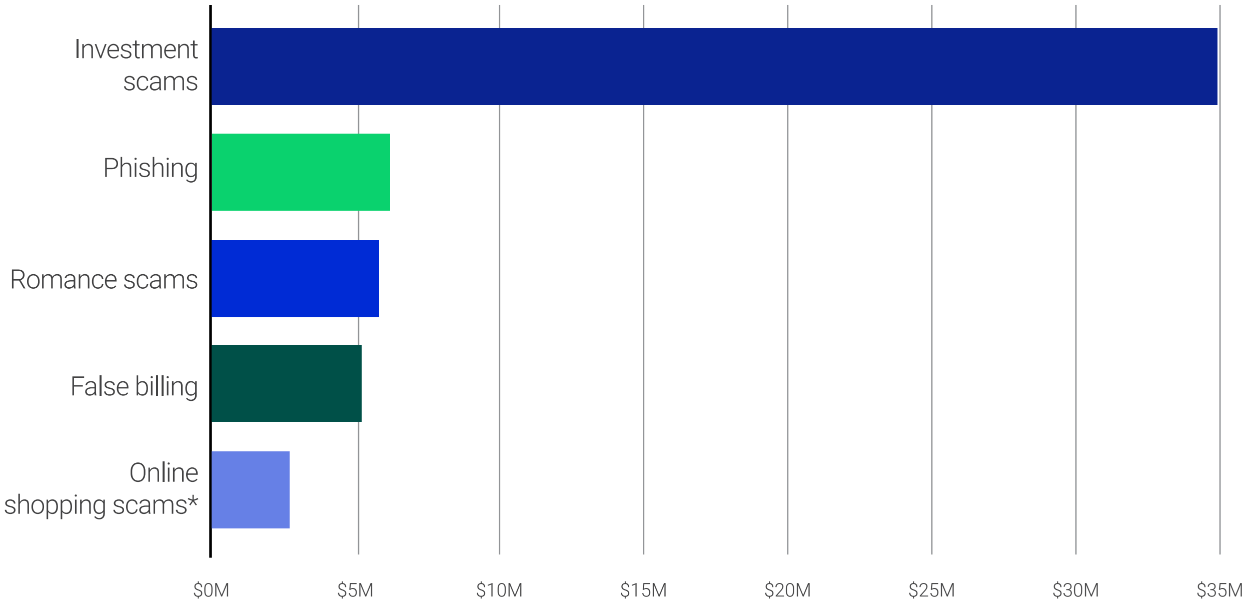
Thanks to reports from Australians to Scamwatch, we were able to issue or share at least 13 warnings or advice related to phishing scams across the public and private sector in Q4.[10]

Investment scams continued to lead to the highest overall losses with $34.9 million reported lost in Q4, a decrease of 24.8% from Q3. This decrease was likely the result of ongoing efforts across government and industry following the Investment Scam Fusion Cell in February 2024. Organisations such as ASIC continued to take down the websites of investment scams referred to it by the National Anti-Scam Centre and other partners, and banks and telcos continued with activities that were initiated during the fusion cell (such as sharing phone numbers for call diversion).

[9] Scam statistics | Scamwatch.

[10] Examples include: Au.domain name phishing scam; NASC impersonation; ATO tax refund phishing scam; AFP phishing action; phone spoofing; and ASIC impersonation scam.

Figure 2: Top 5 scam categories in losses reported to Scamwatch in Q4

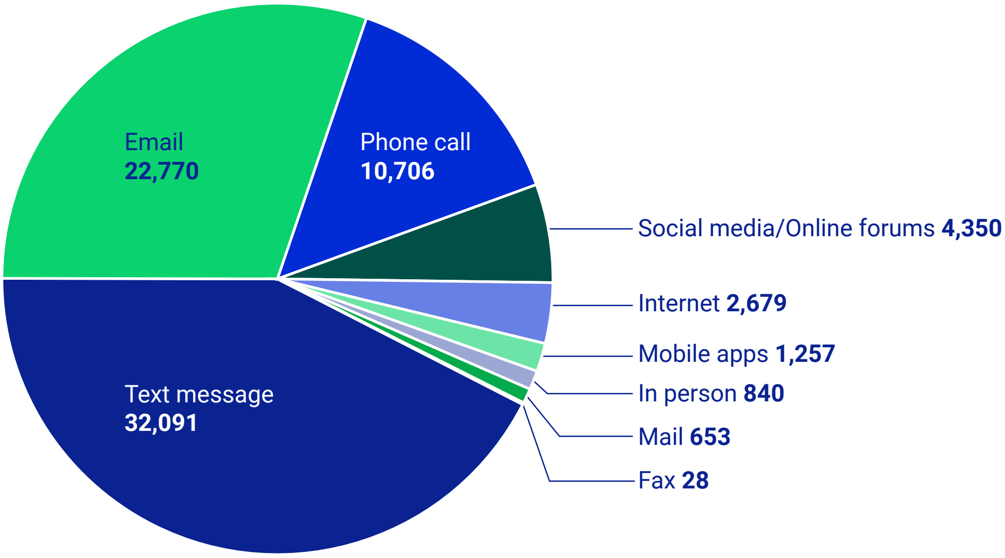


* Includes classified scams

Contact methods

This quarter, data reported to Scamwatch indicates that text message, email and phone calls continued to be the most common contact methods[11] used to attempt to scam Australians.

Figure 3: Contact method – number of reports to Scamwatch Q4



[11] Contact methods that Scamwatch collects are: SMS, Email, Phone call, Social media/online forums, Internet, Mobile apps, In person, Mail and Fax. Fax was removed from the Scamwatch form on Friday 6 September.

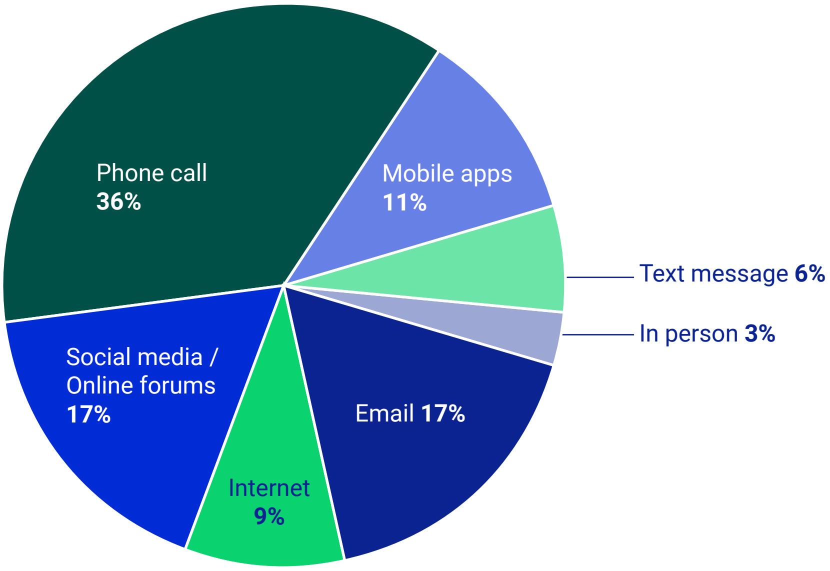
While overall total losses were highest for scams via phone call, more people lost money to social media scams than any other contact method.

Table 1: Number of reports with loss and total losses by contact method

Contact method	No. of reports with loss	Total losses
Social media	1,962	$11.2m
Internet	1,110	$5.8m
Email	908	$11.4m
Phone call	588	$23.9m
Mobile apps	419	$7.4m
SMS	384	$4.2m
In-person	136	$2.0m
Mail	43	$59,765

The contact methods leading to the highest overall losses were phone call ($23.9 million), email ($11.4 million) and social media ($11.2 million).

Figure 4: Contact method – percentage of overall losses in Q4



This quarter 45.1% of social media scams reported to Scamwatch included a financial loss, up from 36.9% in Q3. Similarly, reports of internet scams with a financial loss increased from 34.4% in Q3 to 41.4% in Q4. This compares to the just 7.4% of Scamwatch reports overall which included a financial loss, and may indicate that social media scams and scam websites are harder for people to identify as a scam, leading to a higher proportion of people who report losing money compared to other contact types.

In Q4, the National Anti-Scam Centre observed a trend in reports about scam sellers on Facebook Marketplace.[12] The National Anti-Scam Centre referred over 2,000 Facebook URLs suspected of being a scam to Meta for action. In response, Meta removed or blocked some of these URLs.

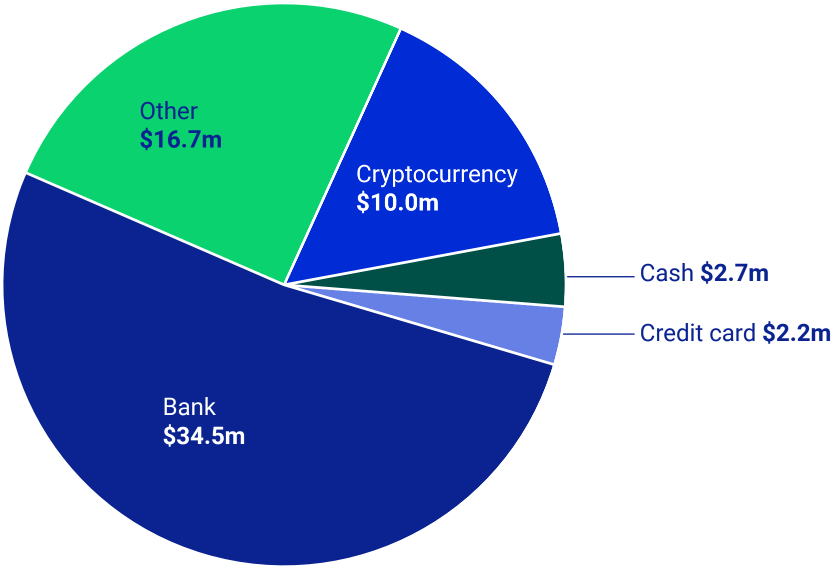
[12] Source: Scamwatch reports.

To improve its capability to quickly disrupt scam websites and social media advertisements, the National Anti-Scam Centre has launched simpler ways for the public to report scam advertisements and scam URLs.[13]

Payment methods

People who report to Scamwatch can also report the scammer payment method.[14]

Figure 5: Losses by payment method reported to Scamwatch in Q4



This quarter the most common payment methods reported to Scamwatch were bank transfer and credit card, as outlined in table 2 below.

Table 2: Payment method by reports and total losses in Q4

Payment method	No of reports	Total losses reported
Bank transfer	2,159	$34.5 m
Credit card	1,632	$2.2 m
Other[15]	1,480	$16.7 m
Cryptocurrency[16]	141	$10.0 m
Cash	138	$2.7 m

[13] https://www.scamwatch.gov.au/report-a-scam those who haven't lost money can choose to report an advertisement or website using the short form.

[14] When a reporter selects that they lost money on the Scamwatch form they can nominate: cash, bank, credit card, iTunes gift card, other gift card, Australia Post load and go prepaid debit card, digital currency exchange, Google Wallet, MoneyGram, PayPal, UKASH, Western Union, World Remit, or other.

[15] Other payment includes: iTunes gift card, other gift cards, Google Wallet, PayPal, UKASH, money remitters, and other such as superannuation or unspecified.

[16] Scamwatch reporters can select money and then nominate a digital currency exchange but can also select 'cryptocurrency' as a payment method. The Scamwatch form was changed during Q4 to capture more information about cryptocurrency losses. This was in testing and so these losses may be adjusted slightly in the future.

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.

Reports to Scamwatch by people from First Nations communities

People identifying as First Nations[17] made 1,241 reports in Q4. Of these, 165 people reported losing money, with a total of $1.4 million reported lost. This represents a 47% increase in overall losses compared to $944,876 in Q3. The median losses for First Nations people was $478, higher than the median for all reporters of $400.

Table 3: Top 3 scams by loss reported to Scamwatch by First Nations people

Scam type	Reports with loss	Total losses
Investment scams	14	$435,257
Romance scams	11	$299,100
Threat based scams	4	$202,320

Most First Nations people who reported financial loss experienced online shopping or false billing scams (75 people reported losing money to these scams). The contact method leading to the most financial loss in Q4 for First Nations people was email, with 24 people reporting losses of $389,210.

In June 2024, the National-Anti Scam Centre launched a short-run radio campaign, developed in partnership with First Nations radio stations. The campaign utilised the reach and credibility of First Nations owned and operated community radio stations and delivered 6,699 radio spots. 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 including Knuckey Lagoon, Palmerston Indigenous Village, Daly River and surrounding areas in the Northern Territory. The campaign aimed to raise awareness about scams targeting First Nations people in remote communities and empowered them to protect themselves and report incidents to Scamwatch.

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

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

People reporting to Scamwatch who identified as CALD[18] made 3,529 reports in Q4. Of these, 431 people reported losing money totalling $8.8 million. This represents a decrease of 21.0% compared to the $11.2 million reported lost in Q3. The median loss was $760, which was significantly higher than the median of $400 for all Scamwatch reporters.

Table 4: Top 3 scams by loss reported to Scamwatch by CALD communities

Scam type	Reports with loss	Total losses
Investment scams	52	$3.6 m
Romance scams	35	$2.3 m
Threat-based scams	14	$1.3 m

Many reporters from CALD communities lost money to online shopping scams (169 reporters) or false billing and job scams (65 reporters).

While it was positive to see decreases in reported losses to investment scams and romance scams in Q4, people from CALD communities reported a total of $1.3 million in financial losses to threat-based scams which was an increase of 42.7% compared to the $940,308 reported lost in Q3.

It is common for threat-based scams to impersonate law enforcement and threaten people from CALD communities. On 21 June 2024 the National Anti-Scam Centre published a warning[19] about criminals calling people and pretending to be from the National Anti-Scam Centre. The warning noted that the scammer would tell the person their phone number was being used in a scam in China and offer to help clear the record. The criminals would say they were working with the Chinese police and threaten the victims.

People from CALD communities reported losing more money to scams initiated by phone call ($3.7 million across 52 reports) and mobile apps ($2.7 million across 55 reports) than to other methods of contact.

The National Anti-Scam Centre previously issued warnings about in-language scams targeting specific communities, people who speak English as a second language, and those in Australia on temporary visas. The National Anti-Scam Centre has now published the *Little Book of Scams* in a wider range of languages other than English, to help anti-scam messages reach CALD communities.[20] A video of the Book is also available online.[21]

The National Anti-Scam Centre has also commenced a Job Scam Fusion Cell to disrupt jobs scams. This decision was informed by the opportunity to reduce the significant harm to younger people and people from CALD communities, who often lose money to these scams.

[18] 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.

[19] Scam alert: NASC impersonation scammers | Scamwatch.

[20] The Little Book of Scams | Scamwatch available in English, Chinese simplified, Arabic, Vietnamese, Greek, Italian, Spanish, Hindi, German, Macedonian, Croatian, Traditional Chinese, Tagalog/Filipino, Korean, Indonesian, Farsi, Turkish, Dari.

[21] Videos in the above languages available here: How to spot and avoid scams - YouTube.

Reports to Scamwatch from people with disability

People with disability lodged 6,225 reports to Scamwatch in Q4. Of these, 442 people reported losing money amounting to $4.4 million (or 7.0% of all reported losses to Scamwatch). This represents an increase of 19.0% on the $3.7 million reported lost in Q3. The median amount lost was $489. The increase in overall losses reported was largely driven by increases in losses to investment and false billing scams.

The top three scams leading to the highest overall losses reported by people with disability were:

Table 5: Top 3 scams by loss reported to Scamwatch by people with disability

Scam type	Reports with loss	Total losses
Investment scams	41	$2.2 m
Romance scams	44	$648,399
False billing scams	26	$504,999

The scam more likely to lead to losses for people with disability in Q4 was online shopping scams with 166 people reporting losses totalling $235,203. Remote access scams were also reported by 18 people with disability with losses totalling $200,433.

People with disability were more likely to lose money to social media scams (155 reported losing money) however total losses due to social media scams were relatively lower than other contact methods with an overall total loss of $880,671. This was followed by internet scams, with 86 people reporting losing money totalling $1.0 million, and then email scams, with 68 people reporting losing money with total losses of $1.4 million.

The National Anti-Scam Centre has published an Easy Read[22] version of the *Little Book of Scams* which provides clear advice for everyone about how to avoid scams. It may also assist people with cognitive impairment or brain injury to recognise and avoid scams. It is available via the Scamwatch website.[23]

Scamwatch reports by Australians based on age

People aged 65 and over had the highest reported losses of $19.2 million (29.0% of all losses reported to Scamwatch) despite only making up 17.2% of the population[24] and they accounted for 25.4% of all Scamwatch reports made in Q4. This represents a decrease of 8.0% from the $20.8 million reported in Q3. Of those reporters that specified their age, people aged 65 and over were more likely to report scams (19,156) than other age groups.

Reporters aged 65 and over reported the highest aggregate losses. However, in terms of likelihood to experience a financial loss, people aged between 35 and 44[25] made up 17.4% of the 5,550 people who reported losing money to Scamwatch, the highest proportion of those who experienced a loss based on age. In Q4 966 people in the 35–44 age group reported losing a total of $7.2 million, compared to the 728 people aged 65 and over who reported total losses of $19.2 million.

[22] Inclusion Australia defines Easy Read as a way of writing to present information so that it is easier for people with low literacy to read. https://www.inclusionaustralia.org.au/wp-content/uploads/2023/04/A-Guide-to-Commissioning-Easy-Read-Resources.pdf.

[23] Easy Read version: The Little Book of Scams | Scamwatch.

[24] 17.2% of the Australian population are aged 65 and over according to 2021 Census data https://www.abs.gov.au/statistics/people/population/population-census/latest-release.

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

Table 6: Scamwatch reports and losses by age group (over 18) in Q4

Age	Reports	Reports with loss	% of the 5,550 aggregate reports with loss[26]	Aggregate loss
18–24	1,587	479	8.6%	$1.9 m
25–34	3,787	791	14.2%	$5.2 m
35–44	5,537	966	17.4%	$7.2 m
45–54	7,196	739	13.3%	$6.7 m
55–64	9,381	642	11.5%	$14.2 m
65 & over	19,156	728	13.1%	$19.2 m

There were some significant differences in the scams leading to financial loss for different age groups. For those aged 18–24[27] threat-based scams led to the highest aggregate losses – this may be due to the large volume of sextortion scams,[28] as well as authority scams targeting young migrants and international students. Job scams led to the second highest aggregate losses for the 18–24 age group. People in the 25–34[29] age group had the highest aggregate losses to investment and false billing scams. In the 35–44 age group 79 people reported losses to investment scams totalling $3.4 million.

In the older age groups, investment and romance scams led to the highest losses. Ninety one people aged 55–64[30] lost a total of $7.1 million to investment scams, followed by 30 people reporting total losses to romance scams of $3.5 million. Many Australians aged 65 and older have retired and may be seeking investment opportunities, which may explain the 107 people in this age group reporting total losses to investment scams of $11.7 million.[31] However, unlike any other age group, 113 people aged 65 and over reported losses to phishing scams totalling $4.1 million, representing a 258.0% increase in phishing scam losses for this age group (compared to the $1.1 million lost in Q3). The National Anti-Scam Centre prioritises alerts and warnings to the public about phishing scams including in community presentations to older Australians.

Table 7: Categories leading to highest losses for age groups

Age group	Highest aggregate losses	2nd highest aggregate losses
Under 18	Threat-based scams	Online shopping
18–24	Threat-based scams	Job scams
25–34	Investment scams	False billing
35–44	Investment scams	Romance
45–54	Investment scams	False billing
55–64	Investment scams	Romance
65 and over	Investment scams	Phishing

[26] This is the % of the 5,550 total reports with loss made to Scamwatch in Q4.

[27] Census data groups ages from 20–24 which is 6.2% of the population.

[28] 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. This compares to blackmail or image-based abuse where the perpetrator has images or videos that they threaten to release if money is not paid. People report both to Scamwatch.

[29] According to census data people aged 25–34 make up 14.2% of the population.

[30] According to census data people aged 55–64 make up 11.8% of the population.

[31] This is a decrease of 16% from the $13.9 million lost in Q3 to investment scams to this age group.

Supporting people and communities to stay safe from scams

A principal objective of the National Anti-Scam Centre's outreach strategy is to empower people who may face barriers or increased risk of harm to identify and avoid scams.[32] Key outcomes from this quarter's engagement include:

- Increasing consumers' ability to spot and avoid scams through delivering over 32,000 printed copies of the *Little Book of Scams* to organisations from across Australia. Common distribution points included aged care facilities, police stations, community centres and groups, Members of Parliaments' electorate offices, and local government centres.
- Equipping over 2000 older Australians and those from CALD backgrounds to identify, avoid, and recover from scams, through delivery of 25 scams awareness presentations.
- Developing scams resilience among at-risk groups, including by 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. This work reduces the number of PALM workers targeted by scammers, particularly in-person scams in which personal information and bank details are stolen.

Community, consumer, and industry reach

25
Scams awareness presentations given to 2000+ consumers

32,000
printed copies of the Little Book of Scams distributed

presentations at industry events

Q3	6
Q4	11

Scamwatch reports from small business

Small businesses are targeted by scammers through a variety of channels, including phishing attempts and fake invoices.[33] Reports from small businesses to Scamwatch made up 0.6% of all reports and 3.1% of losses at $2.1 million in Q4. There was a large increase in false billing losses (264.0% increase from Q3) driven by three high loss reports. These three reports amounted to $1.2 million in losses. All three of these high loss false billing scam cases reported business email compromise.

There were 56 reports from small businesses which included a financial loss. The median loss was $1,175 which was significantly higher than the $400 for all reporters. Twenty six reports from small businesses reported false billing scams totalling $1.3 million followed by 6 businesses reporting investment scam losses totalling $639,750. Eighteen small businesses reported online shopping scams totalling $39,808. Most losses for small business resulted from contact via email (24 reports totalling $1.4 million).

The National Anti-Scam Centre engages regularly with small businesses through established networks including via the ACCC's Small Business Information Network; the Small Business and Franchising Consultative Committee; and the Agriculture Consultative Committee. This includes providing information about how small businesses can protect themselves and their customers from scams.

[32] This strategy focuses on First Nations communities, older Australians, youth and children, people from culturally and linguistically diverse backgrounds, those living with a disability, and small businesses.

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

The National Anti-Scam Centre in action

This section of the report focuses on key activities and outcomes of the National Anti-Scam Centre in Q4, 2024.

Prevention and Disruption

Disrupting scams is a core function of the National Anti-Scam Centre. Disruption aims to prevent contact between scammer and victim, break contact where it has already occurred, or prevent the transfer of money or personal information. Both scammer and victim can be the target of disruption efforts. Because scams are constantly evolving, governments, law enforcement and industry must be agile in developing new disruption methods. In Q4 the National Anti-Scam Centre continued to:

- Protect consumers from exposure to scam content by sourcing and sharing actionable intelligence, such as websites, emails and advertisements from Scamwatch and other sources.
- Conduct direct victim-end disruption in collaboration with law enforcement agencies, notifying victims that they are involved in a scam, and providing recovery support.
- Work with businesses to respond to emerging scam trends.

Data and intelligence sharing with stakeholders

High quality, comprehensive, and consistent data is an essential tool in the fight against scams. With its coordinating function across the scams ecosystem and as manager of the Scamwatch reporting service, the National Anti-Scam Centre is uniquely placed to analyse, interpret, and identify trends in scams data. Sharing this intelligence with trusted industry partners equips businesses to shut down scams affecting them and their customers, or those taking place through their products and services.[34]

The National Anti-Scam Centre achieved a significant program milestone, establishing a data sharing agreement with ASIC. This agreement supports automated data sharing of scam intelligence on a timely basis. Initial data sharing focussed on investment scam data and reports, due to the high losses associated with this type of scam. These developments enhance Australia's whole of government response to scams by facilitating faster responses to, and analysis of, scams data from different parts of the ecosystem.

In Q4, the National Anti-Scam Centre participated in the AFCX's anti-scam intelligence loop (intel loop). The intel loop allows key stakeholders, including telecommunication companies, banks, and government agencies to share verified information with other participants in near real-time, enabling website takedowns, SMS blocking, and phone number diversions. It facilitates a pathway for sharing actionable intelligence, such as scam websites, with the National Anti-Scam Centre for takedown or other action.

[34] As a result of reviewing scam trends this quarter, the National Anti-Scam Centre began developing a guide to assist companies to protect their phone numbers from spoofing. This will be made available to key stakeholders by the end of 2024.

Data sharing engagement focused on key government stakeholders this quarter. It is anticipated that two-way sharing of scams data with ReportCyber will be operational by the end of the year, providing law enforcement with access to the significant scams intelligence contained in within the Scamwatch reporting service (at present Scamwatch receives data near real-time from ReportCyber – the enhancements relate to expanded sharing of Scamwatch data with ReportCyber).

Case study: from intelligence to action

Remote access scams impersonate trusted brands and convince people to download software which gives a criminal control of their device. The victim is instructed to log into internet banking enabling the criminals to access bank accounts and personal information.

Losses to remote access scams reported to Scamwatch had increased by 52.0% in Q3 compared to Q2.

Intelligence gathered revealed that the 65 and above age group are the most impacted, accounting for 47.9% of all losses. First Nations Australians are nearly 5 times more likely to suffer a financial loss from a remote access scam than the general population.

Analysis also revealed scammers impersonating employees of phone and software companies, with Microsoft, Telstra, and Apple commonly impersonated.

In response, during Q4, the National Anti-Scam Centre:

- Informed remote desktop application software companies of reports of scam activity using their products and encouraged them to adopt know-your-customer requirements, improve intelligence collection techniques, display prominent warnings throughout a user's journey, and take steps to assist victims to end a remote access session.
- Raised awareness by publishing a media release, which was picked up by multiple news services.
- Provided best practice protection advice to sectors commonly impersonated by remote access scammers.

The impact of these actions will take time to fully assess, but data in Q4 shows that the median losses to remote access scams decreased slightly from $5,000 in Q3 to $4,454 in Q4, and continues to fall. At the time of publishing, median losses after Q4 were $3,000. In Q4 there were 1,858 Scamwatch reports of remote access scams representing an increase of 2.5% from the 1813 in Q3. Financial loses in Q4 increased by 20.4% with $2.6 million reported lost but showed a slowing in the rate of acceleration from the 52.0% increase between Q2 and Q3. Financial losses in Q4 show a 66.7% reduction in losses compared to the same quarter in 2023 when $7.9 million was reported lost.

Fusion Cells to combat scams

The National Anti-Scam Centre co-led the **Investment Scam Fusion Cell** with ASIC for six months to February 2024. The final report on this fusion cell's work was published in May 2024,[35] highlighting the fusion cell's key achievements including:

- Creating referral processes for takedown of scam advertisements, advertorials, and videos resulting in more than 1,000 instances being removed by digital platforms.[36]
- Takedown of 220 investment scam websites.
- Diversion to a recorded warning of 113 attempted calls to confirmed scam phone numbers associated with low volume, but high impact, imposter bond/term deposit scams, preventing potentially millions of dollars in scam losses.
- Since the fusion cell ended, a further 548 calls were diverted by Optus, bringing the total calls diverted to 661 as of 30 June 2024. The Optus call diversions are ongoing. Telstra currently blocks calls to phone numbers verified by the National Anti-Scam Centre as being used in imposter bond/term deposit scams and will shortly join Optus in providing recorded warnings to their customers, further expanding the impact of this fusion cell initiative.

Investment Scam Fusion Cell key outcomes

1,000+
advertisements & videos removed by direct referral to digital platforms

220
investment scam websites taken down

113
attempted calls to scam phone numbers diverted to recorded warnings

In Q4, the National Anti-Scam Centre planned a **Job Scam Fusion Cell** which will run from August 2024 until March 2025. Participants include 29 organisations from recruitment and job platforms, law enforcement, banks, digital currency and cryptocurrency providers, digital platforms, telcos, academics, victim support services and impersonated entities.

- Job scams leverage fake opportunities for online work in the gig economy and target those seeking additional income. They typically involve the impersonation of a well-known business, claiming to be recruiting on its behalf. Victims are often invited into group chats where fake employees share images of their "earnings" to prolong the victim's involvement and to create a sense of belonging to a group of people successfully earning money.
- Through careful social engineering, the victim is given a range of reasons why they need to make payments to the scam operator. They may be required to deposit cryptocurrency or transfer funds to a nominated bank account to "recharge," "purchase," or "top-up" their account before they can complete their job requirements or access their "earnings."
- These scams tend to impact people with low income, those from CALD communities, the long-term unemployed, non-resident visa holders, and others that may have more limited employment options. Unlike most other scam types, consumers aged between 25 and 44 are reporting particularly high losses to job scams. Job scams are also used to recruit and groom money mules.

[35] https://www.nasc.gov.au/reports-and-publications/fusion-cells.

[36] Due to differences across platforms, calculating aggregate metrics of advertisements removed, advertisement impressions, and advertisement clicks on a comparable basis is difficult. The measures in the Investment Scam Fusion Cell Final Report should be interpreted as indicative estimates of the likely impact.

The fusion cell will focus on disrupting scams through:

- early identification of job scam campaigns and their enabling factors (digital platforms, fake websites, messaging apps, etc.)
- blocking or limiting scammers' ability to use enabling technology, products, and services
- developing strategies to stop consumers sending funds to scammers
- implementing awareness and protection strategies to arm targeted communities and demographics.

Improving the Scamwatch reporting service

As a result of learnings from the Investment Scam Fusion Cell, the National Anti-Scam Centre:

- Commenced a new short web form for reporting a scam advertisement.
- Developed an additional short web form enabling consumers to report scam websites to easily refer harmful URLs to the National Anti-Scam Centre.
- Captured cryptocurrency identifiers in scam reports to enable cryptocurrency firms to disrupt scams.

It is expected that simplified reporting through the introduction of short forms will generate more actionable intelligence and facilitate more timely removal of online scams. Faster removal reduces the number of consumers exposed to offending content, significantly reducing the harm of these scams.

Updates to the Scamwatch report form to enable reporters to include cryptocurrency identifiers, such as wallet addresses, in their scam reports were made in April. As of 30 June 2024, the National Anti-Scam Centre received more than 800 reports containing cryptocurrency identifiers. Sample data has been shared with key industry stakeholders and the National Anti-Scam Centre's new cryptocurrency API is expected to see its first automated data transfer with a cryptocurrency exchange in the coming months.

The National Anti-Scam Centre worked with key industry and government stakeholders to design the public interactive Scam Statistics page.[37] Feedback from stakeholders indicated the need for users to access the data more directly for their own analysis. For example, users working for state or territory government agencies have a particular interest in statistics relating to their jurisdiction. Users also interact with the scam statistics page for research for education courses, to inform scams awareness workplace training, for media and industry research, and to inform consumer affairs education.

Website takedown service

In March 2024, the National Anti-Scam Centre commissioned a website takedown service to target non-investment scam websites. This provides additional takedowns to ASIC's investment scams website takedown service. Establishing a takedown process for a broader range of scams provides further protection for Australians against online scams. Since the service commenced:

- Over 3,800 URLs were verified as malicious and sent to the web hosts for takedown.
- Over 86.0% were successfully removed.[38]

Phishing scam sites and fake online stores accounted for the greatest proportion of sites removed, though sites used in employment and online gaming scams were also commonly removed.

[37] Scam statistics page: https://www.scamwatch.gov.au/research-and-resources/scam-statistics.

[38] This includes those that were already in the process of being taken down.

There are a range of initiatives by government agencies to remove online scam content. Different approaches counter the unique characteristics of different scam typologies:

- ASIC engaged a web takedown provider in July 2023. This service successfully removed 1,440 scam websites in the quarter, for a total of more than 7,300 across 2023–24.
- Since 2019, the Australian Communications and Media Authority (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 May 2024, action was taken in approximately 1,200 cases.[39]

Collaboration with law enforcement

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.

The JPC3 coordinates resources from state, territory, and international law enforcement, Australian government agencies, and the private sector, consolidating these capabilities to support Australia's response to high-volume, high-harm cybercrime, including scams.

This quarter, the National Anti-Scam Centre continued its collaboration with law enforcement agencies by engaging with victims following enforcement actions. In a recent case, the National Anti-Scam Centre contacted over 1,500 victims of a sophisticated investment and cryptocurrency scam which stole more than $50.0 million. The National Anti-Scam Centre also developed a process along with the AFP and ASIC to notify 18,000 Australians identified through an international law enforcement action related to a cryptocurrency investment scam. These notifications advised the identified Australians they may have been involved in a scam, to cease investing further funds, seek support from their bank, and referred them to identity protection and crisis support services.

In May, the National Anti-Scam Centre participated in a workshop with law enforcement, digital currency exchanges, and blockchain analysis experts on Operation Spincaster. This operation targets romance baiting scams and 'approval phishing' in the cryptocurrency sector. Approval phishing involves deceiving victims into authorising fraudulent blockchain transactions, a tactic that has caused significant losses internationally. The workshop addressed improving responses such as victim engagement, reporting practices, and enhancing public-private partnerships.

[39] Intelligence is sourced from public reporters, Services Australia investigation teams, and a range of external partners.

Case study: collaborating with law enforcement

In October 2023, the Joint Police Coordination Centre (JPC3), in collaboration with the UK's Metropolitan Police and supported by EUROPOL, launched Operation Nebulae, targeting the Phishing-as-a-Service (PhaaS) platform LabHost and its criminal users.

LabHost, marketing itself as a 'one-stop-shop' for phishing, enabled cybercriminals to replicate the websites of over 170 banks, government entities, and other businesses. Starting at US$179 per month, cybercriminals received complete 'phishing kits' enabling them to host websites, generate email and text content, and manage campaigns to exploit their targets.

Over 94,000 Australians had sensitive information, such as one-time PINs, usernames, passwords, security questions, and passphrases stolen through the LabHost platform, which was then used to steal funds from victims' bank accounts.

On 17 April 2024, the JPC3, along with the Australian Federal Police and state police, executed 22 search warrants across five states targeting users of LabHost's services. On the day the warrants were executed, 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 five arrests as well as the takedown of LabHost's domain and 207 web servers hosting phishing websites.

At the time of publishing the National Anti-Scam Centre was working with law enforcement to notify thousands of victims identified in this operation.

International engagement

The fight against scams is a global one which requires strong international cooperation to be successful. This quarter, the National Anti-Scam Centre continued to strengthen its international partnerships by engaging with key international stakeholders.[40] The National Anti-Scam Centre joined leaders of Australian banks in Singapore in June, with the Assistant Treasurer. This was a valuable step in strengthening our alliance with Singapore and furthers our commitment to collaborating with our global network to fight scams. There was significant interest in Australia's fusion cell model and in learnings from the Australian experience.

In May 2024, staff from the National Anti-Scam Centre travelled to the Philippines to deliver a 3-day scams workshop as part of the ACCC's Consumer Affairs Program. This workshop supported Association of Southeast Asian Nations (ASEAN) member states to uplift consumer protection efforts in their jurisdictions.[41] As a result, participants reported increased confidence and ability to implement important anti-scam work, including data collection and analysis, typological classification of scams, and stakeholder engagement. Improving capability in Southeast Asia is important given the level of human trafficking where victims are forced to work in scamming centres.[42]

[40] UK agencies include UK Finance, the National Economic Crime Commission, Stop Scams UK, and the Credit Industry Fraud Avoidance System (Cifas). During the quarter, the National Anti-Scam Centre provided briefings to officials from Thailand, Vietnam, The Philippines and New Zealand on how the centre was established, operations, scam trends, initiatives and innovations. Similar briefings were provided to Malaysia, The Maldives, and Ireland. Briefings were provided to the Deputy Secretary General of Thailand's National Cyber Security Agency, the Vietnamese Competition Commission, the New Zealand Financial Markets Authority and Consumer Protection New Zealand.

[41] ASEAN member states in attendance included Cambodia, Indonesia, Laos, Malaysia, Myanmar, The Philippines, Thailand, and Vietnam.

[42] https://ijm.org.au/blog/scam-centres-run-by-human-trafficking/ and https://www.reuters.com/world/asia-pacific/hundreds-thousands-trafficked-into-se-asia-scam-centres-un-2023-08-29/.

In October, the National Anti-Scam Centre will partner with ASIC to deliver training to representatives from the State Securities Commission of Vietnam (SSC) on our work to combat scams in Australia. The training is part of a capacity building program under the Mekong-Australia Partnership between ASIC and the SSC – supported by the Australian Department of Foreign Affairs and Trade – to build technical expertise and share knowledge. NASC will also attended the Global Anti-Scam Summit ASIA region in Singapore.

International collaboration is contributing insights into the impact of scams, particularly in relation to developing countries and the growth in scamming centres in Southeast Asia. The United Nations Development Programme (UNDP) and coalition partners released an Anti-Scam Handbook (v.1)[43] which looks at the dynamics of scams in developing countries including the Asia Pacific. Many of the scamming centres are using technology to find victims all around the globe, including in Australia, which requires a coordinated global response.

The establishment of the National Anti-Scam Centre puts Australia at the forefront of the fight against scams. Through our international engagement, we have shared insights and learnings from our first year of operations, positioning Australia as a world leader in the anti-scam space. By contributing to these global initiatives, the National Anti-Scam Centre joins other nations in making it harder for the criminals behind the scams and ultimately in protecting more Australians. The building of these relationships across Q4 has enabled the National Anti-Scam Centre to maintain visibility across the whole scam life cycle.

[43] Anti-Scam Handbook | United Nations Development Programme.

Consumer awareness

Community engagement

The National Anti-Scam Centre's commitment to increased consumer awareness and scam-safe behaviour led to the development and dissemination of high quality, consistent, and accessible information about emerging scam trends. This quarter, key community engagement and media activities for the National Anti-Scam Centre included:

Digital reach

1.5m+ visits to Scamwatch website

370,000 distinct users (approx)

16k+ visits to the National Anti-Scam Centre page on ACCC website

11,000+ users

Scamwatch X

84,471 total impressions

368 reposts

896 engagements

Scam content across all digital channels

259,768 total impressions

96 posts

Subscribers to scam alert emails

155,000

▲2,665 new subscribers

Over the last quarter, the Scamwatch and National Anti-Scam Centre social media channels published scam alerts and amplified key stakeholders' scams messaging so consumers have access to accurate and consistent information about emerging and trending scams.

To better reach business and government stakeholders, the National Anti-Scam Centre LinkedIn profile was launched on 3 June 2024 and had 750 followers by the end of June. Over the month of June there were 9 posts which achieved over 27,000 impressions and 2,873 engagements, reflecting significant engagement by this segment of the community with scams messaging, and helping to position the National Anti-Scam Centre as the trusted source for scams information in Australia.

Stakeholder engagement on LinkedIn

LinkedIn profile launched on 3 June

750 followers by the end of June

9 posts

27k+ impressions

2,873 engagements

Payment redirection scams awareness – consumer reach

Social media post on payment redirection scams

250k impressions (approx)

500 shares

A post[44] related to payment redirection scams was shared by state and federal regulators as well as banks, consumer protection agencies, law enforcement, and community organisations across social media, achieving almost 250,000 impressions and over 500 shares.

[44] https://www.facebook.com/acccgovau/posts/pfbid0icExeUvZhL2NkWH1WQzYsw5QtoB3rsQKCCEYNkiMfbYegMhSSoe8KhjB5XYu4gYFl.

Victim support

Victim referrals and responses

In Q4, the National Anti-Scam Centre referred 1,831 Scamwatch reporters to IDCARE for tailored and timely scam recovery support.[45]

The National Anti-Scam Centre continues to develop tailored automatic email responses to Scamwatch reporters based on the type of scam reported and the losses suffered. During this quarter, tailored automatic responses were introduced for victims of remote access scams, victims of false billing scams, and businesses reporting false billing scams. This contact offers tailored directions and referrals ensuring victims can protect their information and devices, seek crisis support as necessary, and avoid further victimisation.

The National Anti-Scam Centre also provides information on the Scamwatch website to help people identify and avoid scams and understand what to do if they have been scammed.[46]

Many Australians over this quarter have experienced significant harm to their mental health after experiencing financial crime. Many victims of scams are referred by the Scamwatch service and National Anti-Scam Centre staff to crisis support services such as **Lifeline – 13 11 14** and **Beyond Blue – 1300 22 4636** and need ongoing mental health support to recover.

Support for scam victims in Q4

1831
scam reporters referred to IDCARE

222
tailored victim support emails sent

[45] 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.

[46] What to do if you've been scammed | Scamwatch.

Looking forward

As the National Anti-Scam Centre moves into its second year of operation, it continues to invest in uplifting its technological capabilities.

The National Anti-Scam Centre will continue to support the government as it develops consultation on the Scams Prevention Framework and start to bring on board businesses to share data in readiness for the new obligations in 2025.

As additional stakeholders collaborate with the National Anti-Scam Centre in sharing data, anti-scam efforts across the ecosystem will be strengthened, better protecting consumers. Through the near real-time sharing of reliable and actionable data and by receiving intelligence from across industry and government, the National Anti-Scam Centre remains well placed to achieve the aim of making Australia a harder target for scammers.

As outlined in the introduction, data across the eco-system is changing and the National Anti-Scam Centre is working with stakeholders to consolidate scam categorisation across reporting entities and identify any duplication across different data collections. This will enable the National Anti-Scam Centre to provide greater aggregation and like-for-like comparison of scam data in the future, giving stakeholders even more reliable scams data to inform priorities and develop targeted disruption initiatives. For example, this work will enable more detailed analysis of Scamwatch and ReportCyber data beyond the high-level aggregate combined figures. But as the collection of data changes and more data and intelligence becomes available, comparison with previous years will be less reliable. The collection and availability of more intelligence will be critical to support regulated entities to comply with the Scams Prevention Framework and will enhance the National Anti-Scam Centre and partners' capabilities to prevent, detect and disrupt scam activity.

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 About the data used in this quarterly update

The data in this quarterly update is for the period 1 April to 30 June 2024 unless otherwise specified.

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 is verified for all Scamwatch reports with losses over $1,000, for example by checking in AUSTRAC.

Data may change quarter to quarter because of quality assurance processes and reporters withdrawing reports. In addition, changes were made to the Scamwatch report form which may impact the data represented on the Scamwatch statistics page and data in this report. For example, a new field for recording cryptocurrency losses was trialled and there was some delay in this loss data being uploaded to the public statistics page.

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

Australian Signals Directorate – ReportCyber cybercrime report service

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.

Combined data: ReportCyber and Scamwatch

This Q4 report references data from the National Anti-Scam Centre's Scamwatch service and law enforcement's cybercrime report service, ReportCyber. Scamwatch and ReportCyber contain reports made directly from members of the public. High loss reports in ReportCyber of $1 million and over are reviewed for accuracy and validity, for example by checking in AUSTRAC. ReportCyber reports where a person has the same name and same amount lost as a report in Scamwatch are not included in the combined data in this quarterly report. This equates to about 3.0% of reports. These data sets use the date of report consistent with the approach of general crime reporting.

Table 8: Data in reports from the public – Scamwatch and ReportCyber

Organisation	No. of reports		Total losses		No. of reports with loss		% of reports with loss	
	Q3	Q4	Q3	Q4	Q3	Q4	Q3	Q4
Scamwatch	67,734	75,372	$71.9m	$66.0m	4,582	5,550	6.8%	7.4%
ReportCyber	15,993	14,960	$167.6m	$167.8m	9,054	8,275	56.6%	55.3%
Combined	**83,727**	**90,332**	**$239.5m**	**$233.8m**	**13,636**	**13,825**	**16.3%**	**15.3%**

Financial sector data: the AFCX

The Australian Financial Crimes Exchange (AFCX)[47] is an independent, not-for-profit company. The AFCX provide a secure and trusted platform where participating organisations share and gain operational data and insights from each other. This enhances the identification, investigation, and prevention of financial crime, and protects the organisations and their customers. Since AFCX receives operational reports from each participant, there are several differences from ScamWatch reporting. For example, one person who loses money to a scam may account for 3 cases if they have accounts with different banks who each report to the AFCX. While there is broad alignment, there may be small differences between scam categories used by AFCX and NASC. 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 has provided aggregate data to the National Anti-Scam Centre showing that its financial services members reported transactions totalling $181.4 million in financial loss to scams in Q4. This represents a small increase (5.2%) in financial loss from Q3 to Q4.[48] This increase may be reflected in the publicly reported data to Scamwatch and ReportCyber in the second half of 2024.

The AFCX data referred to above will include duplicates where people may have also reported to Scamwatch and/or ReportCyber. For this reason, AFCX data is not included in combined losses until further work is completed to align the data sets and remove duplication.

From time-to-time AFCX members identify omissions. Corrections or backloading can lead to changes in the data. AFCX cases report financial losses. In some cases, the customer may recover part or all their loss. The total reported losses are not adjusted for recoveries.

No new AFCX members have commenced reporting data to the AFCX since January 2024. Cuscal and COBA (on behalf of some members) commenced reporting in December 2023. Remaining ABA members and COBA members will begin reporting data over 2024 and 2025. Incremental change to the data is expected as more members report.

Unreported losses

Not all Australians report scams. Despite the existence of several 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.

[47] www.afcx.com.au.

[48] The AFCX data was accurate as at 2 August 2024. The AFCX also reported some information was missing in the Q3 data and therefore the true figure for Q3 was $172.5 million (not the $99.2 million previously reported in the Q3 Update) National Anti-Scam Centre quarterly update March 2024 | ACCC.

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 feel comfortable reporting.

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.[49] 69.0% 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.

The Australian Institute of Criminology reports[50] that 7.8% of 13,887 participants in its research experienced a fraud or scam in Australia in the past year, with the most common being online buying and selling scams. The study noted that about 22.1% of victims sought help from police or the Australian Cyber Security Centre, and that the actual number of fraud and scam victims was at least 4.5 times the number recorded by ReportCyber.

[49] Source: https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release. Accessed 7 July 2024. 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.

[50] https://www.aic.gov.au/sites/default/files/2023-07/sr43_cybercrime_in_australia_2023_v2.pdf. Fraud and scams defined as intentionally deceiving someone to obtain money or something else of value such as personal information.

Appendix 2 Scamwatch Q4 Data

All data in the below tables is for Q4 (1 April to 30 June 2024) and comparative period Q3 (1 January to 31 March)

Table 9: Scamwatch losses reported by scam type

Scam Type	Reports with loss	Q4	Q3	% change loss
Investment scams	523	$34.9m	$46.4m	-24.8%
Phishing	396	$6.2m	$3.8m	63.2%
Romance scams	251	$5.8m	$5.7m	1.9%
False billing	466	$5.2m	$2.6m	100.4%
Online shopping scams (inc. Classified scams)	2,634	$2.7m	$2.0m	37.3%
Remote access scams	157	$2.6m	$2.2m	20.4%
Jobs and employment scams (inc. Pyramid schemes)	186	$2.5m	$3.3m	-23.4%
Threats to life, arrest or other	65	$2.4m	$2.2m	7.7%
Identity theft	190	$1.5m	$1.8m	-17.3%
Inheritance & unexpected money	29	$696,914	$641,332	8.7%
Rebate scams	23	$356,498	$545,491	-34.6%
Other scams (inc. Ransomware and Mobile premium services)	313	$290,476	$87,042	232.2%
Psychic and clairvoyant	11	$267,677	$360,724	-25.8%
Travel, prizes and lottery scams	37	$167,861	$88,328	90.0%
Betting and sports investment	45	$166,339	$42,603	290.4%
Fake charity scams	21	$85,774	$21,517	298.6%
Overpayment scams	57	$34,764	$12,564	176.7%
Hacking	77	$34,197	$26,550	28.8%
Health and medical products	69	$25,008	$54,551	-54.2%
Total	**5,550**	**$66.0m**	**$71.9**	**-8.2%**

Table 10: Scam reports by scam type

Scam Type	Q4	Q3	% change
Phishing	31,653	27,850	13.7%
False billing	10,236	8,552	19.7%
Online shopping scams (inc. Classified scams)	6,935	6,897	0.6%
Other scams	6,816	6,482	5.2%
Identity theft	4,733	4,515	4.8%
Hacking	3,002	2,353	27.6%
Remote access scams	1,858	1,813	2.5%
Investment scams	1,776	1,680	5.7%
Rebate scams	1,233	1,102	11.9%
Threats to life, arrest or other	1,156	1,316	-12.2%
Travel, prizes and lottery scams	957	617	55.1%
Dating and romance scams	890	852	4.5%
Health and medical products	800	598	33.8%
Jobs and employment scams	718	666	7.8%
Inheritance & unexpected money	668	720	-7.3%
Ransomware and malware	510	327	56.0%
Overpayment scams	506	587	-13.8%
Mobile premium services	397	438	-9.4%
Betting and sports investment scams	238	124	91.9%
Fake charity scams	191	167	14.4%
Pyramid schemes	67	38	76.3%
Psychic and clairvoyant	32	40	-20.0%
Total	**75,372**	**67,734**	**11.3%**

Table 11: Contact methods reports and losses

Contact method	Reports	Reports with loss	Q4 Total loss	Q3 Total loss	% change
Phone call	10,706	588	$23.9m	$23.7m	0.8%
Email	22,770	908	$11.4m	$12.8m	-11.5%
Social media/Online forums	4,350	1,962	$11.2m	$13.6m	-17.5%
Mobile apps	1,257	419	$7.4m	$6.7m	11.7%
Internet	2,679	1,110	$5.8m	$7.1m	-17.5%
Text message	32,091	384	$4.2m	$2.1m	102.5%
In person	840	136	$2.0m	$5.7m	-64.9%
Mail	653	43	$59,765	$44,358	34.7%

Table 12: First Nations – Q4 top 10 (loss) reports and losses by category

Category Level 3	Amount lost	Number of reports	Reports with loss
Investment scams	$435,257	48	14
Dating and romance scams	$299,100	17	11
Threats to life, arrest or other	$202,320	14	4
Remote access scams	$123,031	30	4
Jobs and employment scams	$75,788	18	6
Online shopping (incl. classified)	$72,618	133	60
False billing	$62,795	206	15
Phishing	$43,935	390	6
Betting /sports investment scams	$36,565	16	7
Identity theft	$28,167	76	8

Table 13: CALD – Q4 top 10 (loss) reports and losses by category

Category Level 3	Amount lost	Number of reports	Reports with loss
Investment scams	$3.6m	160	52
Dating and romance scams	$2.3m	93	35
Threats to life, arrest or other	$1.3m	81	14
False billing	$508,509	426	35
Jobs and employment scams	$417,592	101	30
Online shopping (incl. classified)	$213,199	389	169
Remote access scams	$143,433	82	6
Identity theft	$122,890	317	11
Phishing	$102,275	1,159	29
Betting and sports investment scams	$19,514	18	6

Table 14: People with disability – Q4 top 10 (loss) reports and losses

Category Level 3	Amount lost	Number of reports	Reports with loss
Investment scams	$2.2m	155	41
Dating and romance scams	$648,339	223	44
False billing	$504,999	890	26
Online shopping (incl Classified)	$235,203	535	166
Threats to life, arrest or other	$205,620	83	6
Remote access scams	$200,433	148	18
Unexpected money	$137,831	79	10
Phishing	$113,867	2,262	39
Identity theft	$110,531	404	16
Fake charity scams	$33,711	28	3

Australian Government

National Anti-Scam Centre