Australian Government

National Anti-Scam Centre

National Anti-Scam Centre in action

Quarterly update

January to March 2024

Acknowledgment of country

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

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

ACCC 05/24_24-18

www.accc.gov.au

Contents

Introduction

This is the third Quarterly Update of the National Anti-Scam Centre since it was established on 1 July 2023. This update provides information about the activities of the National Anti-Scam Centre from 1 January to 31 March 2024 and the impact of government and private sector initiatives to combat scams.

The National Anti-Scam Centre fosters collaboration through its Advisory Board, working groups and ongoing engagement with industry, consumer organisations and government. These forums are used to share insights to assist the private sector to implement strategies against scams. The sharing of information assists businesses to mitigate risks associated with scams and implement disruption activities.

Prior to the introduction of the National Anti-Scam Centre there was an absence of cross sector engagement. In the nine months since the National Anti-Scam Centre was established, it has brought together industry participants from the finance, telecommunications and digital platforms sectors with government and identified opportunities for these participants to work together to expand existing initiatives across the ecosystem leading to results in terms of driving down scam losses.

This update includes data about scam reports and losses reported to the National Anti-Scam Centre's Scamwatch service (www.scamwatch.gov.au), the cybercrime reporting platform, ReportCyber (www.cyber.gov.au)[1] and financial transaction data from the Australian Financial Crimes Exchange (the AFCX, www.afcx.com.au).

During this quarter all 3 data sources observed a decrease in scam losses. This continues the trend observed during the latter half of 2023 and demonstrates the continued impact of collaboration across government, industry, and law enforcement. Australians reported $73.2 million in losses to Scamwatch, $173.2 million to ReportCyber and $99.2 million to the AFCX. The combined total this quarter was $345.6 million.[2] The National Anti-Scam Centre will integrate these (and other) key sources of scams data to provide more regular and comprehensive intelligence about scam activity in Australia. The first stage of data integration will be achieved in July 2024 when ReportCyber data is integrated with the National Anti-Scam Centre's Scamwatch data.[3] This is expected to be followed by the Australian Securities and Investments Commission (ASIC) and the Australian Communications and Media Authority (ACMA) in September and financial services data via the AFCX by October. Complete data integration is dependent on near real-time data sharing arrangements to the National Anti-Scam Centre being established.

The National Anti-Scam Centre commenced receiving near real-time data from ReportCyber in December 2023. The National Anti-Scam Centre will have full capability for near-real time data sharing (in and out) by July 2024 with negotiations to onboard entities continuing in the second half of 2024. This provides an opportunity for organisations to get ahead of the Government's future Code obligations and set up data sharing processes to inform their scam prevention and disruption activities. Negotiations are continuing with the telecommunications sector, digital platforms, financial services, cryptocurrency exchanges, victim support services, law enforcement and government agencies such as the Australian Taxation Office and Services Australia.

1 ReportCyber is the Australian Government's online cybercrime reporting tool, coordinated by the Australian Signals Directorate's Australian Cyber Security Centre.

2 This combined total has not been adjusted to remove possible duplication. Reporters may make reports to different organisations. As the National Anti-Scam Centre technology develops duplicates will be more easily identified. Integration of ReportCyber, AFCX and Scamwatch is expected by October 2024.

3 The National Anti-Scam Centre receives ReportCyber data, however the integration which removes duplication between ReportCyber and Scamwatch data is expected by July 2024.

Ahead of full data sharing capability, to facilitate prevention and disruption of harmful scams, the National Anti-Scam Centre has automated (not real-time) data sharing arrangements sending data to 7 partners[4] including the AFCX, which represents a significant portion of the financial sector. Manual data sharing arrangements are in place for the National Anti-Scam Centre to share data with the telecommunications sector. Data is not yet received from the telecommunications sector.

The National Anti-Scam Centre has commenced a scam website takedown service this quarter targeting, among other things, phishing scams and online shopping scams. This is in addition to ASIC's takedown of investment scam websites and provides broader protection for Australians against online scams.

The National Anti-Scam Centre also plays a critical role in raising awareness of scams through education and community outreach by meaningfully protecting and supporting victims to recover from scams. The National Anti-Scam Centre publishes resources and alerts and administers the Scamwatch reporting service.

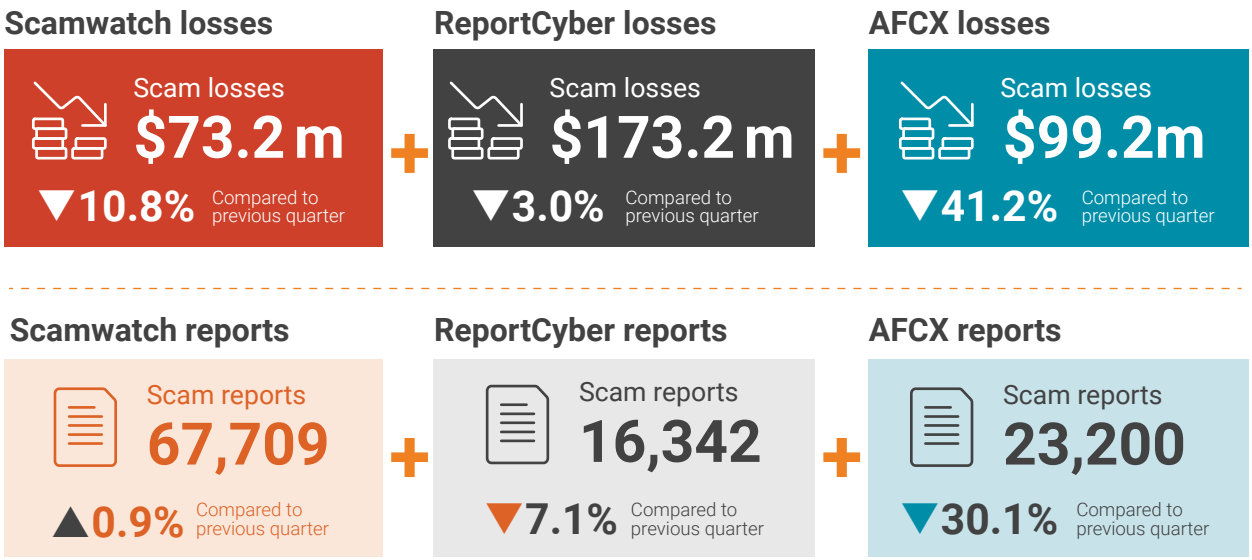
4 ASIC; ReportCyber; the AFCX; IDCARE; Meta; Gumtree and Western Union.

Spotlight on scams

The Quarter – January to March 2024

Scam losses continued their downward trend in this quarter, with decreased losses reflecting ongoing decreases in losses to investment scams. The downward trend in losses since the inception of the National Anti-Scam Centre highlights the importance of the public-private partnership model in safeguarding Australians from scams. The National Anti-Scam Centre Scamwatch data shows that 60% of the $8.9 million decrease in total losses from quarter 2 to quarter 3 was attributable to the reduction in investment scam losses.

The National Anti-Scam Centre collects scam reports and monitors losses through its Scamwatch reporting service. Through enhanced information sharing capabilities, the National Anti-Scam Centre now receives near-real time scam data from ReportCyber and quarterly scam data from the Australian Financial Crimes Exchange (AFCX). This data is not combined in this Quarterly Update due to the potential for duplication. The National Anti-Scam Centre is working towards consolidating scam categorisation across reporting entities.[5] This will provide increased reliability for stakeholders using scams data to inform priorities and develop targeted initiatives.



The **National Anti-Scam Centre's Scamwatch service** shows losses were $73.2 million, compared to the $82.1 million in the previous quarter (a 10.8% decrease). Reports increased nominally with 67,709 reports this quarter compared to the 67,116 reports in the previous quarter (a 0.9% increase). 6.8% of reports included a financial loss, down from the 9.7% across 2023 and the 12.1% in 2022. This may indicate that increased efforts to raise awareness about scams is having some impact with many people reporting scams that they have not lost money too. Importantly for investment scams, reports with loss decreased from 42.7% in 2023 to 34.2% this quarter.

5 Organisations collect or maintain data sources relevant to scams for different purposes. The type of data collected and the purpose for which it is collected is not consistent. Not all scams data is based on public reporting. For example, the AFCX data is transaction-based data. The National Anti-Scam Centre's Scamwatch service will be updated in the new financial year to ask reporters for information about other places they have reported to improve the identification of duplicate reporting.

For those who reported a financial loss, the average amount lost was $15,212 (a 4.4% decrease from the $15,913 in the previous quarter).[6] This slight increase in report numbers in conjunction with lower reported financial losses is a positive indicator that the Government's commitment to tackle scams, together with the National Anti-Scam Centre and its partners are making a difference through raising awareness of scams and educating Australians about how to spot and avoid scams.

Losses to **ReportCyber**[7] were $173.2 million, compared to the $179.7 million in the previous quarter (a 3% decrease). 16,342 Australians reported scams to ReportCyber compared to the 17,597 in the previous quarter (a 7.1% decrease). For those with a financial loss who reported to ReportCyber, the average amount lost was $18,421, down 1.8% on the previous quarter.

The **Australian Financial Crimes Exchange** reported 23,200 cases this quarter with financial losses of $99.2 million.[8] This represents a decrease in cases of 30.1% from the 33,200 in the previous quarter and a decrease of 41.2% from the $168.8 million in the previous quarter.[9]

More detailed information about scams reported to the National Anti-Scam Centre's Scamwatch service is set out in **Appendix 1** to this report. Information about the data source and data cleaning processes is set out in **Appendix 2**.

6 There were 4,815 reports that included a financial loss. The average of all Scamwatch reports was $1,082 and the median was $501.

7 Data source: reports from the public and law enforcement about scams only to cyber.gov.au between 1 January and 31 March 2024.

8 Data source: between 1 January and 31 March 2024 financial transaction data from members of the Australian Financial Crimes Exchange.

9 Data includes payments made using BECS, NPP and BPAY but excludes credit card.

National Anti-Scam Centre in Action

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

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

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

To strengthen this commitment, in the 2024–25 Federal Budget the Government provided:

- $6.3 million to the ACCC for a National Anti-Scam Centre public awareness campaign about scams to help the public identify, avoid and report scams
- $37.3 million over 4 years (and $8.6 million per year ongoing) for the ACCC, ASIC and the ACMA to administer and enforce mandatory industry codes for regulated businesses to address scams on their platforms and services, initially targeting telecommunications, banks and digital platforms services relating to social media, paid search engine advertising and direct messaging
- $23.3 million over 4 years for the Australian Taxation Office to continue to oversee and operate the secure eInvoicing network
- $1.6 million over 2 years for the Treasury to develop and legislate the overarching Scams Code Framework.

Collaboration

Collaboration between the National Anti-Scam Centre, ASIC, banks, and telecommunications providers has been key to the decreases in losses to scams observed over the last 2 quarters. For example, the National Anti-Scam Centre identifies and refers investment scam URLs to ASIC, contributing to the 5,000 website takedowns[10] achieved to date. Enhanced technological capabilities within the National Anti-Scam Centre will be critical to ongoing collaboration by enabling more timely and comprehensive analysis and sharing of actional scam intelligence and emerging scam trends. The Government's introduction of mandatory codes will ensure the private sector has clear and enforceable obligations to share intelligence about scam activity and take action to prevent and disrupt scams that target their customers and users.

10 ASIC URLs removed between 1 July 2023 and 31 March 2024. This compares to the 4,000 referenced in the Fusion Cell Report between mid-August to mid-February 2024.

Technology and intelligence sharing

The aim of the National Anti-Scam Centre is to make Australia the world's hardest target for scammers by improving cooperation between government, industry, and law enforcement to prevent scams and empower Australians to avoid scams. Prior to the establishment of the National Anti-Scam Centre, data sharing was manual and disparate. Technology[11] enables the National Anti-Scam Centre to ingest, analyse and share data at scale and supports collaborative strategies for scam disruption, victim support and scam awareness across government and in partnership with industry.

World leading public-private partnership safeguards Australians from scams

By the end of FY 25/26 the National Anti-Scam Centre will have technology, systems and partnerships in place to significantly reduce the prevalence and impact of scams on individuals, businesses, and the economy. Our experience demonstrates that building the technological capability is necessary but insufficient for success. Data sharing must be reciprocal, and the support of mandatory and enforceable obligations in a Scams Code Framework, will be key to realising the National Anti-Scam Centre's vision to:

- enhance the ability to detect scams early through effective monitoring, data collection, data sharing and analysis of scam trends and patterns
- use this informaiton to provide a coordinated response, and collaborate with industry and law enforcement to disrupt scams
- inform policies and regulations that protect consumers and businesses from scams and enhance overall cyber and financial security
- ensure victims have access to support, and maximise the chances of recovering funds lost
- build resilience in consumers and small business through targeted, empowering and effective communications.

This will lead to a safer digital and physical environment where the risk and damage caused by scams is minimised and public trust in digital and financial systems is strengthened.

11 In July 2023, the government invested $58 million to establish and run the National Anti-Scam Centre, including $39.5m (68%) to establish and enhance technology. Funding is across 3 years from 1 July 2023 to 31 June 2026.

The table below outlines the key stages over 3 years to deliver the technology uplift and increased capability of the National Anti-Scam Centre to foster collaboration to disrupt scams.

FY23/24	FY24/25	FY25/26
✓ Establishment & governance ✓ Public/private Advisory board ✓ People & workforce capability ✓ Partners & engagement ✓ Collaborative disruption projects ✓ Industry forums & working groups ✓ Technology foundations ✓ Scamwatch website uplift ✓ Investment scam fusion cell ✓ Auto referrals for victim support ✓ URL sharing to ASIC ✓ Data standards ✓ Data sharing ready (EOFY23/24)	National Anti-Scam Centre website Scam website takedown service Website and scam ads report service Data partner onboarding: police; banks; digital platforms; cryptocurrency exchanges; telcos; regulators Data integration and reporting Disruption strategy Awareness campaign Second fusion cell Actionable intelligence service AFCX Intel Loop partnership Scam email forwarding service	Whole of ecosystem near real time data sharing Proactive intelligence Fusion cells 3 and 4 Ongoing awareness Technology enhancements Coordinated response to emerging scams

Appendix 3 provides the National Anti-Scam Centre's vision for centralising intelligence and enabling data sharing across the ecosystem, which is a priority for the 2024–25 Financial Year, and a significant step towards achieving the goals above.

A key risk and continuing challenge is the ability to attract technical talent. Despite this, the National Anti-Scam Centre is on track to establish the technology foundations at the end of our first year of operation and expand data sharing to detect and disrupt scams at increased speed and scale over the next year.

During this quarter we achieved the following milestones for the technology uplift.

Scamwatch website uplift – web and reporting portal

The National Anti-Scam Centre runs Scamwatch, which provides a reporting service for the public to report scams and information about how to spot and avoid them. The National Anti-Scam Centre uses the report data in its engagement with businesses to develop strategies to combat scams and to promote community awareness about scams. The report data provides a baseline for assessing the impact of initiatives because Scamwatch has been collecting data for over 15 years and receives over 300,000 reports annually.

Since the National Anti-Scam Centre was established, it has been implementing iterative improvements to the reporting portal and data collection to enhance the reporting experience for

victims and gather further data to support disruption by additional industry participants such as digital currency exchanges.

This quarter, the National Anti-Scam Centre added the ability to capture improved bank information and cryptocurrency scam details. The National Anti-Scam Centre shares[12] this information with banks via the AFCX, and during the next quarter will share with the first cryptocurrency exchange to facilitate disruption actions such as blocking or freezing accounts and wallets.

Security continues to be at the heart of all technology delivery, with the National Anti-Scam Centre services regularly undergoing independent security assessments to protect Australians' information. This work is done through a partnership with CyberCX.[13]

A Privacy Impact Assessment was also undertaken this quarter to inform collection of information on the website portal and from partners and on-sharing of that information. The *Privacy (Australian Government Agencies – Governance) APP Code 2017* requires agencies to undertake a written Privacy Impact Assessment for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information. The National Anti-Scam Centre program not only involves new and changed ways of handling personal information but will involve significant volumes and considerable complexity of information that will be shared across a multifaceted ecosystem. The National Anti-Scam Centre Program has a higher privacy risk compared to scam-related work prior to the inception of the National Anti-Scam Centre. Therefore, a Privacy Impact Assessment was commissioned to ensure the program complies with the Privacy Act 1988 and the Australian Privacy Principles.

The assessment process was undertaken by independent external advisers and identified no significant privacy risks.

Technology foundations – data reporting

The National Anti-Scam Centre receives regular requests for data and information about scam trends, for example from Commonwealth government agencies, State and Territory government, media, consumer advocates, university researchers, law enforcement and businesses. The National Anti-Scam Centre has launched an improved public scam data tool – https://www.scamwatch.gov.au/research-and-resources/scam-statistics/scam-statistics-public-beta. This service allows the Australian public to explore scam data and trends, including by scam type and demographic. This resource is undergoing design improvements and will continue to be expanded to make publicly available additional scam information.

Having migrated over 2 million historical scam records to a modern platform in January, the National Anti-Scam Centre can now extract insights from past and new scam reports in ways that were previously not possible. For example, the National Anti-Scam Centre was able to identify the sectors commonly exploited in payment redirection scams. Planning and design was completed this quarter to use advanced searching capability for the quick identification of scams and trends.

As the data sharing capability grows, the timeliness and depth of this intelligence will inform an actionable intelligence service that will support collaborative disruption activities and reduce the time scams are operating in Australia. Currently, disruptive activities use National Anti-Scam Centre Scamwatch data.

12 Full reports are only shared where the reporter consents.

13 https://cybercx.com.au/about-cybercx/.

Technology foundations – Proactive scam intelligence

This quarter, the National Anti-Scam Centre designed and planned the technical architecture to automate scam categorisation of reports and to proactively gather information about prevalent scams on the internet.

The National Anti-Scam Centre receives a large volume of reports each day through the Scamwatch 'Report a Scam' webform. Consumers have varying understandings of scam types, meaning that different descriptors may be selected by different consumers for the same conduct. Previously, ensuring like scam reports are grouped with like, required time-intensive manual reviewing of reports, often requiring re-categorisation. The National Anti-Scam Centre is training an algorithm to review submitted scam report categories against a scam taxonomy, to automate reclassification facilitating faster sharing of reports and earlier identification of trending scam types.

Machine learning is also being developed to search social media platforms to identify potential scams. This technology will facilitate faster identification of scams, supporting the National Anti-Scam Centre to quickly refer suspected scam URLs to takedown services for disruptive action and alert the public to emerging scam types. The National Anti-Scam Centre is establishing relationships with staff at relevant digital platforms to progress in-platform disruption. While there has been some progress in establishing pathways to refer scams to major social media platforms for disruption, the National Anti-Scam Centre and key partners expect social media platforms to take greater responsibility for proactive monitoring and removal of scams and targeted in-platform warnings to users.

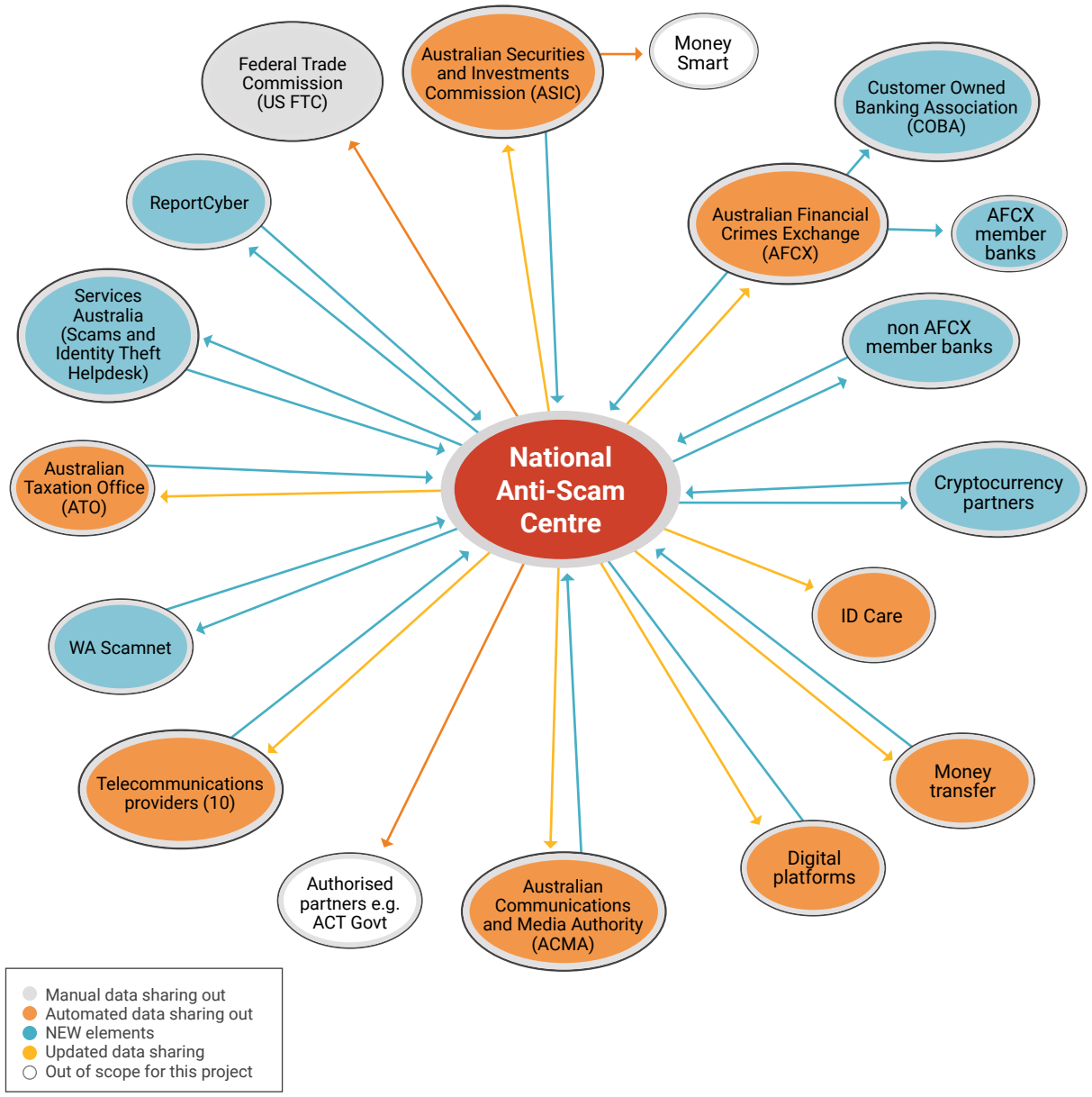
Data sharing ready – Data sharing and integration

Extensive consultation with close to 50 partners across public and private sectors and law enforcement has been undertaken, including socialising proposed data elements required for the National Anti-Scam Centre to identify and disrupt scams. So far, data is provided to 7 partners[14] and received from 1.[15] Figure 1 shows the priority data sharing partners the National Anti-Scam Centre is encouraging to connect and share data to provide increased resilience across the ecosystem.

14 Now sharing with ReportCyber, AFCX, ASIC, IDCARE, Meta, Gumtree, Western Union and ReportCyber.

15 ReportCyber provides near real time data.

Figure 1: Future state – National Anti-Scam Centre regular data sharing



The foundational work to support data sharing and reporting is on track to bring more government and private sector partners on board to provide and receive scam data and intelligence.[16] This important work underpins new capability to disrupt scams at scale. As well as providing a more holistic picture of scam activity through the aggregation of scam data, this data sharing supports the 'no wrong door' principle for consumers by sharing intelligence from scam reports across the ecosystem regardless of where consumers report.

The National Anti-Scam Centre meets weekly with the major banks to share information on scam trends and intelligence. This assists the longer-term activities by building a shared understanding of what information organisations need and how they use it to stop or prevent scams. The National Anti-Scam Centre also runs a working group which brings together over 100 representatives from

16 The National Anti-Scam Centre is in the early stages of implementing automated data sharing. Further information around timeframes will be outlined in the April-June National Anti-Scam Centre in Action Quarterly Update.

digital platforms; the financial sector; telecommunications and consumer organisations to discuss scam trends and intelligence. Over the quarter bilateral meetings were held with many organisations across the ecosystem to better understand their scam prevention processes and data holdings.

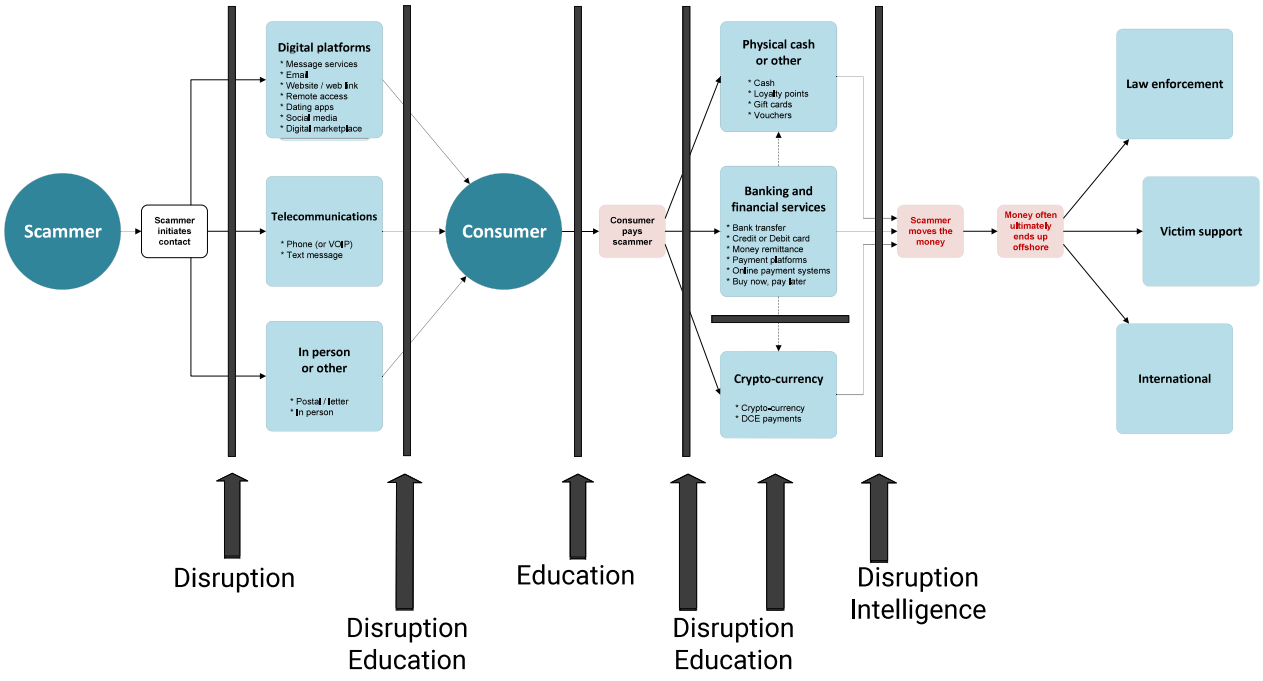
The next report will provide detailed information about the progress of data sharing arrangements with entities.

Disruption

One of the National Anti-Scam Centre's key objectives is to enable the disruption of scams. Disruption can be implemented to prevent contact, to stop contact where it has already occurred, or to prevent payment. It can focus on disrupting the scammer or the victim. For example, when a scam bank account is identified, a bank may disrupt payments going into that scam account preventing the scammer from getting access to any more funds. But action can also be taken to notify any victim paying into that account to ensure that they are made aware of the scam and won't pay funds to additional or alternative scam accounts.

While prosecution of scammers is important to deter them from committing these crimes, enforcement on its own will not prevent widespread financial crime perpetuated through scams. Scam investigations take considerable time and can be complex, given they will often involve international cooperation. An investigative approach can take many months or years, compared to disruption which can prevent harm quickly. Where disruption occurs at scale it can make it much harder for scammers to be successful thus deterring them from those methods. Disruption techniques can deter scammers by rendering their efforts futile. When disruption is combined with initiatives that build resilience in the community such as education and awareness, scam losses should reduce significantly. These initiatives are enabled by the National Anti-Scam Centre because they require cooperation, information sharing and testing to identify those that will have the greatest impact. Figure 2 below highlights the key opportunities for disruption across the ecosystem:

Figure 2: Opportunities for disruption and education across the ecosystem



Website takedown services

Prior to 2023 there was little capability in Australia to remove scam websites at scale. Scam websites would remain active for months, sometimes years which made them harder for the public to identify and contributed to the rise in scam losses. In July 2023, ASIC (a key partner of the National Anti-Scam Centre) commissioned an investment scam website takedown capability. To support ASIC's work, the National Anti-Scam Centre identifies and shares the URLs from investment scams reported to Scamwatch or otherwise identified by the National Anti-Scam Centre and its partners to ASIC for takedown. As a result of this collaborative work and ASIC's own proactive work, ASIC has since shut down over 5,000[17] investment scam websites.

While progress has been made to disrupt investment scam websites using ASIC's takedown service, many other types of scam websites continue to cause losses to Australians. Prior to the establishment of the National Anti-Scam Centre there was no dedicated service that could take down phishing scams, impersonation scams and online shopping scams. In March 2024, the National Anti-Scam Centre commenced an arrangement with a third-party website takedown service to refer up to 500 scam websites per day. In the final days of this quarter, the National Anti-Scam Centre trialled the service. It sent 10,000 URLs that were reported between 1 January and 24 March 2024 for assessment. This trial was used to refine the data quality and processes for identifying sites suitable for takedown. Given the broad time, many websites had already been removed, and some were not full URLs or were in fact legitimate entities. However, of those referred before the end of the quarter, 369 were taken down. This compares to 7 manual takedown requests initiated directly by the National Anti-Scam Centre during the quarter. The websites taken down included employment scams, online gaming scams and fake online stores. From July 2024, members of the public will be able to use a simplified report form to report scam websites. These websites will be sent through to the takedown service for assessment for takedown.

Investment Scam Fusion Cell

The time-limited Investment Scam Fusion Cell, co-led by the National Anti-Scam Centre and ASIC, brought together government and industry over the past 6 months to work in close partnership to reduce accelerating consumer losses to investment scams. This fusion cell was the first in a series which will be conducted over the 3-year period of the National Anti-Scam Centre.

The fusion cell's formal work concluded in February. The work of the fusion cell contributed to the reduction in losses to investment scams observed in Scamwatch data over the last 2 quarters from $52.4 million in October to December 2023 to $47.1 million over January to March 2024. The National Anti-Scam Centre is working to encourage broader uptake of some of the successful initiatives from the fusion cell, for example by working with other telecommunications providers to implement call diversions to provide warnings to people calling scam phone numbers. The National Anti-Scam Centre is also implementing new simple reporting processes to facilitate the referral of scam websites from businesses for takedown and scam advertisements for blocking or takedown by digital platforms. The report on outcomes of the fusion cell is available here: https://www.accc.gov.au/national-anti-scam-centre.

Law enforcement

Information sharing can support both disruption and enforcement activities. The National Anti-Scam Centre continues to collaborate with law enforcement in Australia and overseas. This is primarily achieved through the placement of a National Anti-Scam Centre secondee at the Joint Policing Cybercrime Coordination Centre (JPC3). During this quarter, the National Anti-Scam Centre partnered

17 The National Anti-Scam Centre's Targeting Scams Report (29 April 2024) noted 3,500 websites which was the number of websites reported taken down up to the end of 2023. This is now updated to February 2024 to be 4,000 websites.

with the AFP and overseas law enforcement on a project to notify victims who were unaware they are involved in a scam and disrupt the effectiveness of the scam.[18] This work is continuing.

The National Anti-Scam Centre participated in or led a range of forums focused on collaboration with law enforcement this quarter including key Operations meetings and the Economic Crime Forum. The case study below highlights the co-operation between the National Anti-Scam Centre and State and Federal Police through the JPC3.

Money mule disruption: case study

In February 2024, the National Anti-Scam Centre received a report from a victim who lost $1.6 million to an imposter bond scam. The victim believed their funds were being deposited into a term deposit account, however the funds were in fact being sent to an account controlled by scammers.

National Anti-Scam Centre staff contacted representatives from the bank of the account controlled by the scammer on the same day the report was received, to ensure the matter was escalated quickly.

Australian Transaction Reports and Analysis Centre (AUSTRAC) searches and JPC3 liaison identified the scammer's account had also received a $1.5 million transfer from a second victim, and a further deposit of $40,000 from a third victim with over $3.14 million of the victims' funds already transferred to the United Kingdom.

National Anti-Scam Centre staff seconded to the JPC3 conducted AUSTRAC research identifying another account held by the same money mule with a different bank. Over $340,000 had been sent to the United Kingdom from this account. Following notification from the National Anti-Scam Centre, banking staff located a second account linked by common payees in the United Kingdom and placed restrictions on both accounts.

The National Anti-Scam Centre secondee shared details of the money mules with Victoria Police's liaison officer in JPC3 for law enforcement action.

International engagement

Global Fraud Summit

In March 2024, the National Anti-Scam Centre participated in the Global Fraud Summit in London and presented on cross-sector collaboration. The summit was attended by ministers and representatives from Australia, Canada, New Zealand, the United States, United Kingdom, Singapore, France, Germany, Italy, Japan, New Zealand and the Republic of Korea alongside the International Criminal Police Organisation (INTERPOL), United Nations Office on Drugs and Crime, the Financial Action Task Force, and representatives of the European Union. Key messages included that responsibility to prevent fraud sits with everyone in the ecosystem; necessitating cooperation from industry, government and law enforcement to effectively address scams. An overview of the National Anti-Scam Centre's fusion cell model was shared to demonstrate the successful initiatives coordinated by the National Anti-Scam Centre to tackle complex investment scams in Australia.

18 Specific details about the methodology of these projects are not shared publicly to prevent scammers understanding them.

As part of the summit, ministers signed a communiqué setting out an agreed global framework to tackle fraud. The communiqué[19] has 4 key pillars:

- pillar 1: building international understanding of the domestic and international fraud threat
- pillar 2: empowering the public by aligning and enhancing global messaging on fraud and driving forward global co-ordination of returning lost funds
- pillar 3: pursuing fraudsters acting transnationally by coordinating and increasing international law enforcement activity
- pillar 4: recognising the role of industry in the fraud response and encouraging strong collaboration both with the public sector and cross-sector.

The National Anti-Scam Centre will continue engagement with the United Kingdom through the International Fraud Council to cement the international approach to scams prevention.

International Consumer Protection and Enforcement Network

In March 2024, the National Anti-Scam Centre presented at an International Consumer Protection and Enforcement Network webinar on Online Scams hosted by the Office of Competition and Consumer Protection – Poland. The presentation shared key developments since the establishment of the National Anti-Scam Centre with a focus on the benefits of intelligence and information sharing to disrupt scams. The presentation also outlined how the National Anti-Scam Centre is developing and leveraging partnerships to approach scams collaboratively.

ASEAN[20] – Australia New Zealand Free Trade Area (AANZFTA) Consumer Affairs Program (CAP) E-Commerce Scams Workshop

This quarter, the National Anti-Scam Centre collaborated through AANZFTA to plan an E-Commerce Scams Workshop to be held on 15-17 May 2024 in Manila, Philippines. The 3-day workshop will cover:

- Day 1: E-commerce landscape in the AANZFTA
- Day 2: Australia's National Anti-Scam Centre and the anti-scam ecosystem
- Day 3: Consumer education and stakeholder engagement.

It will feature National Anti-Scam Centre led presentations and practical workshops including one on disruption with representatives from the Commonwealth Bank of Australia and Optus.

19 https://www.gov.uk/government/publications/communique-from-the-global-fraud-summit/global-fraud-summit-communique-11-march-2024.

20 ASEAN member states are Brunei Darussalam, Cambodia, Indonesia, Lao People's Democratic Republic, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam.

Awareness and protection

Empowering consumers and small businesses to spot and protect themselves from scams is a key objective for the National Anti-Scam Centre. This includes designing and delivering meaningful community engagement and working on strategies to empower at-risk communities and small business through our education and awareness campaigns.

Detection and response to payment redirection scams

At the end of 2023, the National Anti-Scam Centre Emerging Trends and Response working group[21] identified an upward trend in reports of false billing scams, particularly payment redirection through business email compromise and email impersonation. False billing scams were the second most common scam reported to the National Anti-Scam Centre's Scamwatch service.[22]

The working group identified real estate (agents, solicitors, conveyancers), construction, motor vehicle sales, funerals, aged care, schools, health and disability care as the sectors most often impersonated or compromised and recommended targeted education to raise awareness of false billing scams. The National Anti-Scam Centre published a media release on payment redirection scams in response to the issues discussed by the working group. Overall, this attracted 71 media mentions with a potential audience of over 4 million people.[23] National Anti-Scam Centre staff also convened an online Industry Forum in March 2024 with over 100 representatives from various organisations, which included presentations from the ATO on e-invoicing and the National Anti-Scam Centre on false billing scams.

Raising business awareness of these scams and providing guidance on how they can better protect their customers assists in hardening Australia as a target for scammers.

21 The Emerging Trends and Response working group has over 100 members across banks, digital platforms, telecommunications providers, consumer advocacy groups and government.

22 From 1 October 2023 to 31 March 2024, Scamwatch received just over 8,500 reports of false billing scams. ReportCyber also collects information about business email compromise scams, recording 1,085 reports with losses of $24.1 million from 1 January to 31 March 2024. Note ReportCyber's 'business email compromise' (BEC) scam category encompasses various scam conduct occurring through breaches of email systems. BEC is considered a subset of Scamwatch's 'false billing' category and accounts for a small number of scams recorded within the 'false billing' category. Other reports categorised under Scamwatch's 'false billing' category include loan scams, fake invoices or goods and services paid for but not received.

23 Data from Streem analysis.

Payment redirection scam awareness case study

Scam problem

"My child's school sent me an invoice via email which was genuine using the school's email address. It requested a lump sum payment of school fees of $40,000. After paying the money, the school advised that it did not receive a payment. It turned out scammers had infiltrated the email system and changed the invoice to include new payee details which directed the payment to a scammer."

"We were working with a conveyancer to purchase a house. Someone got into the conveyancer's email system. For weeks we were communicating with someone pretending to be the conveyancer and we paid the $90,000 remaining for a house deposit."

"Our business email address has been impersonated by a scammer. They have adjusted the email slightly so that is almost a copy of ours. They have been emailing our customers to change the banking details on fake invoices."

Response

In March, the **National Anti-Scam Centre** held an Industry Forum on payment redirection scams with over 110 participants from sectors often impacted by false billing scams (health, real estate, motor vehicle sales, construction). The forum included:

- A presentation from the ATO on the ***Peppol* e-Invoicing system**[24], a global system for business to business and business to government invoicing which minimises the risk of interception and payment redirection.
- The National Anti-Scam Centre presented case studies highlighting the differences between business email compromise and those that impersonate businesses to better arm businesses to protect their business and their customers.
- A guide for businesses was circulated after the event to assist them in protecting their systems and customers.

The National Anti-Scam Centre published a media release[25] on payment redirection scams on 4 April which was supported by members of the Scams Awareness Network through networks and social media.

Next steps

Awareness alone will not significantly reduce the losses to false billing scams. The Australian Banking Association announced in November 2023 that the design of the industry-wide **Confirmation of Payee** system would begin immediately, with the build and rollout expected over 2024 and 2025. **Confirmation of Payee** offers significant protection against false billing scams by making it clear to a person making a payment who that payment is going to. When an email invoice appears to come from a business with a new BSB and account number, the system will be able to verify whether the payment is going to the intended payee.

The National Anti-Scam Centre will continue to monitor sectors impacted by these scams and encourage businesses to protect themselves by regularly changing email passwords and not reusing passwords, adopting e-invoicing, limiting the amount of information posted online regarding the business and encourage their customers to call businesses to verify any change of payment details.

24 https://www.ato.gov.au/businesses-and-organisations/einvoicing/peppol.

25 https://www.accc.gov.au/media-release/beware-of-fake-invoices-from-scammers-impersonating-businesses.

Community engagement and media

The National Anti-Scam Centre's outreach strategy prioritises the following key audiences: First Nations communities, older Australians, youth, people from culturally and linguistically diverse backgrounds, people with disability and small business.

Key highlights from this quarter's engagement include:

- presentations to Pacific Nations working visa holders in conjunction with the Department of Employment and Workplace Relations, Indian Senior Citizens Association of New South Wales, probus clubs and community health groups
- coordination with several organisations to provide National Anti-Scam Centre support for campaigns, joint media and social media alerts – including a Quantum AI alert with the Australian Securities and Investments Commission, phishing media release with Australia Post and payment redirection scams with the Australian Taxation Office
- 13 community events largely targeting older Australians
- ongoing work with private sector and government partners to plan the annual Scams Awareness Week campaign which will run from 26 August 2024.

The National Anti-Scam Centre also reaches Australians across various digital channels, including through media releases on the National Anti-Scam Centre website, scam alert emails to subscribers, social media platforms such as Scamwatch X and the Scamwatch website. The overall media reach was 191 million. Key media activities this quarter and their media reach included:

- The National Anti-Scam Centre issued a media release in the days leading up to Valentine's Day to warn people looking for love to beware of financial criminals luring them into investment scams. The media release was covered extensively by online media, TV and radio, with a potential audience reach of 17.4 million Australians.
- Publishing investment scam media releases about celebrity investment scams and deep fakes and online investment trading platform scams. The media on investment scams was driven by the learnings from the fusion cell. The target audience was older Australians with retirement savings. As such the media activity included coverage from publications such as Seniors Discount Club Online, Sunrise and The Morning Show on Channel 7, 2GB and ABC radio. Overall, this attracted 56 media mentions with a potential audience of over 7 million people.[26]
- Issuing a media release warning Taylor Swift fans of fake Eras Tour ticketing scams in response to a spike in reports of scammers compromising social media accounts to sell fake tickets to the hacked profile's friends list. The media release received wide media coverage across print, media, TV and radio, with a potential audience reach of 12.7 million people.
- Posting an alert on Scamwatch X about Spotify impersonation scams.
- Posting a series of real vs fake quizzes using legitimate looking screenshots to Instagram stories.

26 Data source – Streem analysis.

Digital reach

Media reach

191.8m

Scamwatch Twitter (X)

93,325
total impressions

412
retweets

570
likes

Scam content across all digital channels

199,167
total impressions

112
posts

1.5m
visits to Scamwatch website

3,519
visits to the National Anti-Scam Centre webpage on ACCC website

153,080
subscribers to scam alert emails

Victim referrals and responses

During the quarter, the National Anti-Scam Centre continued its referral of scam victims who 'opt-in' to have their report automatically referred to IDCARE for tailored scam recovery support; removing the need for victims to report to both organisations. Over the quarter, the National Anti-Scam Centre referred 1,710 reporters to IDCARE.

The National Anti-Scam Centre continues to build its capability to respond to and refer victims to ensure they receive the right support to recover from scams. For example, the National Anti-Scam Centre regularly interviews scam victims and uses the information to provide more tailored advice to victims.

The National Anti-Scam Centre is now trialling a process to provide victims reporting investment scams immediate and tailored advice which reduces delays in victims starting the recovery process.

The National Anti-Scam Centre has been engaging with victim support services and obtaining valuable consumer and industry feedback about the reporting process and the website. Accessibility enhancements to the website were launched this quarter, improving the 'Contact us' and 'Report a Scam' forms to make it easier for Australians to lodge scam reports or request a community presentation or copies of the Little Book of Scams.

The National Anti-Scam Centre's victim engagement continues to highlight the many Australians that over this quarter have experienced significant harm to their mental health after experiencing financial crime. Many of these victims' access crisis support from services such **Lifeline – 13 11 14 and Beyond Blue – 1300 22 4636** and need ongoing mental health support to recover.

During the next quarter the National Anti-Scam Centre will continue rolling out tailored responses for victims of different scam types and evaluate the effectiveness of these. It will continue direct engagement with scam victims that are particularly at risk of mental health crisis or require immediate advice to ensure that they are referred to services that can assist.

Looking Forward

The National Anti-Scam Centre will continue to uplift our technological capabilities to ensure a clear understanding of the state of scams in Australia and support prevention and disruption of scams by industry. The National Anti-Scam Centre is working towards ensuring near-real time data sharing capability by July 2024 and onboarding data sharing partners in the second half of 2024.

Work will continue with the Treasury and other regulators on the Government's Scams Code Framework and implementation of mandatory industry codes. The ACCC, ASIC and the ACMA will begin preparations for administering and enforcing the codes for regulated businesses to address scams on their platforms and services.

Work will commence on a $6.3 million public awareness campaign about scams to help the public identify, avoid, and report scams.

Planning is underway for the next fusion cell which is expected to begin in June 2024. Potential topics are being workshopped with stakeholders.

Appendix 1 – National Anti-Scam Centre Scamwatch service: Reports and losses

Data provided in this section is sourced from the National Anti-Scam Centre's Scamwatch service. More comprehensive Scamwatch data is available on the Scamwatch website at https://www.scamwatch.gov.au/research-and-resources/scam-statistics. Our new public beta lets you add filters to find the data you want. Figures presented represent reported losses only, which is likely to be significantly lower than actual losses as many scams are not reported.

Types of scams

Investment scams continue to cause the most financial losses this quarter. However, there has been a steady downward trend each quarter, reducing from $52.4 million in October to December 2023 to $47.1 million in January to March 2024.

Similarly, phishing scams remained the top reported scam type with 27,848 reports, slightly up from the 26,533 in the October to December 2023 quarter.

Top 3 scam losses by type

Investment scams

$47.1m

▼10.1%
compared to previous quarter

Dating & romance scams

$5.9m

▼14.5%
compared to previous quarter

Phishing scams

$3.9m

▼5.5%
compared to previous quarter

Top 3 scam reports by type

Phishing scams

27,848

▲5%
compared to previous quarter

False billing scams

8,544

▼1.2%
compared to previous quarter

Identity theft

4,517

▼13.1%
compared to previous quarter

Source: Scamwatch.

With rising cost of living pressures on households, scammers continue to use social media to deceive people looking to earn extra income through a second job or 'side hustle'.

Some at-risk groups were disproportionately impacted by job scams, including younger Australians aged 18–44 and people from culturally and linguistically diverse backgrounds. Scammers posed as well-known brands advertised through WhatsApp messages or social media, offering 'work from home', 'flexible hours' or a 'guaranteed income'. The National Anti-Scam Centre published a media release in January 2024 to help raise awareness of job scams.

Scam contact methods

During this quarter text messages, emails and phone calls continued to be the top contact methods for scammers. Whilst losses were down, reports increased for these 3 contact methods this quarter compared to the previous. This may indicate increasing attempts to scam Australians using these contact methods.

Top 3 losses by contact method

$23.9m Phone calls

▼2.4%
compared to previous quarter

$14.2m Social media

▼10.7%
compared to previous quarter

$12.8m Emails

▼17.3%
compared to previous quarter

Top 3 reported contact methods

25,462 Text messages

▲0.9%
compared to previous quarter

20,350 Emails

▲2.3%
compared to previous quarter

11,916 Phone calls

▲5.7%
compared to previous quarter

Source: Scamwatch.

As reported in the October to December 2023 quarter, there continues to be an uptick in the number of scammers using social media to target Australians with reports increasing by 11.8%. Social media scam losses reduced slightly from last quarter, decreasing by 10.7% from $15.9 million in October to December 2023 to $14.2 million in January to March.

Impact of scams on communities

First Nations communities

Data for First Nations people is unlikely to be an accurate reflection of the level of harm caused by scams due to significant barriers to reporting.[27] First Nations people lodged 1.6% of all reports and lost $1 million to scams; approximately 1.4 % of total losses in the January to March 2024 quarter.[28] Dating and romance scams overtook investment scams this quarter to become the highest scam losses category for First Nations people.

First Nations People – Top 3 scam losses

Dating & romance scams

$279,045

▲105%

compared to previous quarter

Remote access scams

$162,610

▲1308%

compared to previous quarter*

Investment scams

$127,514

▼23%

compared to previous quarter

Note: * Over $150,000 of this $162,610 total was attributed to one report.

Culturally and linguistically diverse communities

People identifying as culturally or linguistically diverse reported a total of $11.3 million in losses this quarter which represents 15.5% of all losses to Scamwatch for the quarter.[29] There continued to be reports about high loss threat-based scams with almost all of them involving threats to arrest Chinese Australians.

The National Anti-Scam Centre has issued warnings previously about in-language scams targeting specific communities and targeting people with English as a second language or on temporary visas. The National Anti-Scam Centre is continuing to produce the Little Book of Scams in 17 languages other than English to ensure anti-scam messages reach culturally and linguistically diverse communities.

Culturally and Linguistically Diverse communities – Top 3 scam losses

Investment scams

$7.8m

▲184%

compared to previous quarter

Dating & romance scams

$1.1m

▲357%

compared to previous quarter

Threats to life, arrest or other

$940,308

▼69%

compared to previous quarter

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

28 ABS data states that 3.8% of the Australian population are Aboriginal or Torres Strait Islander with 33% of these under 15 years of age.

29 22.8% of Australians speak a language other than English at home.

People living with disability

People living with disability lodged 7.6% of all reports to Scamwatch in the January to March quarter, amounting to $3.9 million (or 5.3% of all reported losses to Scamwatch).[30] False billing scam losses increased this quarter for people with disability. This trend was driven by some high loss reports including a payment redirection scam where a National Disability Insurance Scheme (NDIS) plan manager's email system was compromised, and funds transferred by a plan manager to a scammer; a rental accommodation scam and some reports about property services requested and paid for but not completed. The National Anti-Scam Centre has shared information about scam reports with the NDIS and is exploring the potential for data sharing.

People living with disability – Top 3 scam losses

Investment scams

$1.4m

▼60%
compared to previous quarter

Dating & romance scams

$1.2m

▼10%
compared to previous quarter

False billing scams

$306,631

▲53%
compared to previous quarter

Impact of scams on older Australians

People aged 65 and over made the most scam reports this quarter with reported losses of $21.2 million (28.9% of all losses reported to Scamwatch) despite only making up 16% of the population.[31] Losses to investment scams decreased 15% but there were increases in romance and phishing scam losses. The increase in romance scam losses was driven by 3 reports accounting for $1.5 million in losses all involving initial contact via WhatsApp and Facebook. The increase in phishing scam losses was driven by several high loss bank impersonation scams and police impersonation scams.

Older Australians Top 3 scam losses

Investment scams

$14.3m

▼15%
compared to previous quarter

Dating & romance scams

$2.8m

▲161%
compared to previous quarter

Phishing scams

$1.1m

▲35%
compared to previous quarter

30 18% of people in Australia live with disability.

31 16% of the Australian population are aged 65 and over, https://www.aihw.gov.au/reports/older-people/older-australians/contents/demographic-profile.

Impact of scams on small business

Small businesses[32] are often targeted by scammers through various channels, including phishing attempts or fake invoices. Reports from small businesses to Scamwatch made up 0.7% of all reports and 2.4% of losses at $1.8 million.

Small Business Top 3 scam losses

Investment scams

$1.3m

Significant increase
compared to previous quarter*

False billing scams

$380,065

▼48%
compared to previous quarter

Classified scams

$51,101

▲16%
compared to previous quarter

Note: * This was a 60-fold increase from the previous quarter. Report numbers are too low to draw out any significant loss trends for investment scams.

32 Small business includes reports from small and micro businesses. Small and micro businesses have between 0–19 staff.

Appendix 2 – About the data used in this Quarterly Update

The data in this Quarterly Update is for the period 1 January to 31 March 2024 unless otherwise specified.

This report includes references to data from the National Anti-Scam Centre's Scamwatch service, law enforcement's cybercrime report service, ReportCyber, and the Australian Financial Crimes Exchange (AFCX). Each data set collects different data, with Scamwatch the only source that includes reports where losses have not been incurred (as well as reports involving losses). ReportCyber is a service to report crime, therefore reports are from victims and will include a loss. The AFCX is transaction data submitted by the banks and not directly reported from the public, it also only has cases with loss.

The combined data included in this report will contain duplicates. Victims may have reported to their bank (and therefore counted in AFCX data) and to Scamwatch and/or ReportCyber.

Over the coming months, the National Anti-Scam Centre technology build will integrate information from many more of the reporting services and data sources to provide a consolidated data set. As a result, we anticipate future Reports will consolidate, aggregate and de-conflict more data across additional datasets to produce a more accurate picture of scam activity in Australia.

Unreported losses

Not all Australians report scams. Despite the existence of several reporting platforms, we know the extent and impact of scams is under-reported and some cohorts are markedly underrepresented in official reporting figures.

The National Anti-Scam Centre is conducting more work to encourage reporting from all communities, and to reduce the stigma of scams so that more people are comfortable to report them. The Australian Bureau of Statistics (ABS) Personal Fraud data shows that in the 2022–23 financial year, 2.5% of Australians (514,300) experienced a scam. A person is considered to have experienced a scam if they have responded to a scam and sought further information, provided money or personal information, or accessed links associated with the scam. 69% of people who experienced a scam notified (or were notified by) an authority. This means that approximately 30% of people who experienced a scam did not report it. It is likely many of those who did not report incurred a small or no direct financial loss and consequently this under reporting does not mean actual losses would be 30% higher if those people reported.

Scamwatch data

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

The National Anti-Scam Centre's Scamwatch service is a rich data source that includes information about scam types, victims affected, communications and payment methods used by scammers, and some information about the backgrounds of reporters and victims. It is the only data source drawn on in this Quarterly Update that collects information about scams that do not always involve a

financial loss, making it a valuable long-term metric to observe trends in scam report numbers over time. Some victims may only report to ReportCyber where they have suffered a financial loss.

The validity of a loss amount and category is verified for all Scamwatch reports with losses over $1,000. Reports with any loss reported from overseas are verified for an Australian nexus.

Australian Signals Directorate – ReportCyber cybercrime report service

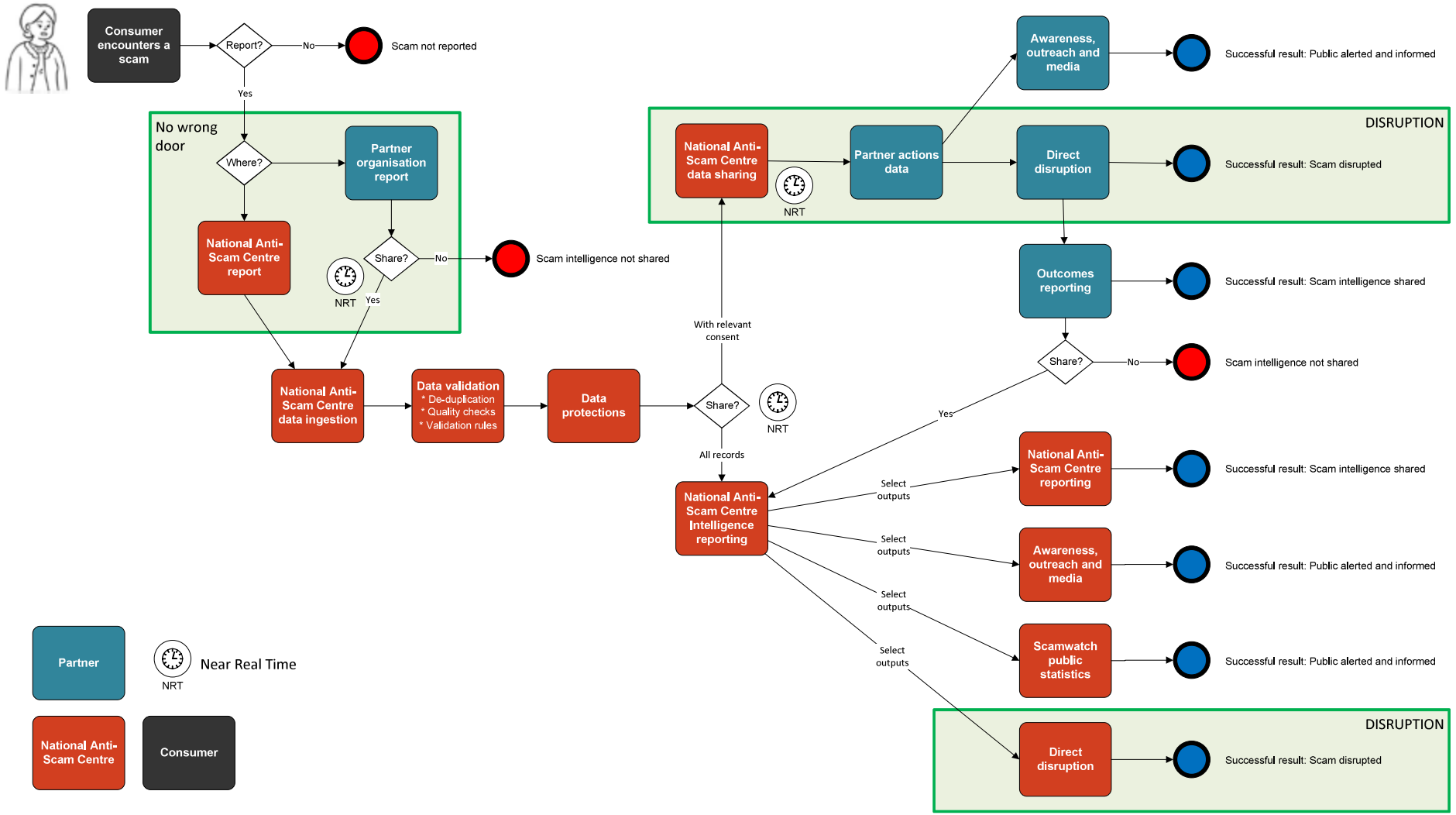
ReportCyber (www.cyber.gov.au) is a cybercrime reporting platform hosted by the Australian Cyber Security Centre of the Australian Signals Directorate. It was developed as a national policing initiative with State and Territory police, the Australian Federal Police and the Australian Criminal Intelligence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

National Anti-Scam Centre staff verify reports of very high losses (greater than or equal to $1 million) and corrects any errors in the data.

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

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

Appendix 3 – National Anti-Scam Centre vision for the data sharing ecosystem



Appendix 4 – Benefits Register

	Benefit name		Performance measure	Measure type	Baseline FY22/23	Target FY23/24	Target FY24/25	Target FY25/26	First 3 Quarters FY23/24 Actual (1 July 2023 to 30 March 2024)
B1	National Anti-Scam Centre slows the acceleration of financial loss due to scams	1 i	Slower growth/reduction in financial losses to scams	Effectiveness	34% growth on previous year	12% growth on previous year	8% growth on previous year	5% growth on previous year	36% reduction on previous year to date (July to March)
		1 ii	Fusion cell activities reduce financial losses to investment scams	Effectiveness	358,549,140	320,000,000	310,000,000	300,000,000	168,000,000
B2	Greater collaboration between government and industry improves scam disruption and prevention	2i	Collaboration improves scam intelligence, disruption and awareness	Effectiveness	Not applicable	Case Study - Emerging Trends and Response Working Group	Case Study - Data Integration & Technology Working Group	Case Study - Prevention & Communication Working Group	In progress
		2ii	Fusion cells improve scam disruption	Effectiveness	Not applicable	Case Study - Investment Scams Fusion Cell	Case Study - Fusion Cell 2 Case Study - Fusion Cell 3	Case Study - Fusion Cell 4	See Appendix 2
		2iii	Increased collaboration with priority government and industry partners	Effectiveness	Not applicable	Establish baseline using new Stakeholder Management Tool: * # government engagements * # industry engagements	to be determined	to be determined	242 government engagements 232 industry engagements
		2iv	Increased outreach and engagement with 'at risk' groups	Effectiveness	22 presentations	26	26	26	22
B3	Near real time data and timely trend reports improve understanding of the scam landscape	3 i	Decrease in the number of scam reports that need to be re-categorised	Efficiency	Not applicable	Establish baseline	TBA	TBA	In progress
		3 ii	Increase in automated data sharing arrangements to provision near real-time data to NASC partners	Effectiveness	6	10	20	40	7
		3iii	Increase in automated data sharing arrangements to consume near real-time data from NASC partners	Output	0	5	10	40	1
B4	Joined up systems improve support services for scam victims	4 i	Improved support for consumers who lose money or identity to scammers	Output	Not applicable	Case Study - Victim Engagement	Case Study - Victim Engagement	Case Study - Victim Engagement	In progress
B5	Increased scam awareness improves consumers ability to recognise, protect, and report on scams	5 i	Increase in alignment of anti-scam messaging across Prevention & Communication working group members	Effectiveness	Not applicable	Establish baseline via Working Group survey	80%	100%	In progress
		5ii	Increase in average views per media-release	Output	6 million	9 million	11 million	11 million	9,034,166
		5iii	Reduction in webform abandonment	Effectiveness	54% abandonement	50% decrease on baseline	50% decrease on FY23/24	50% decrease on FY24/25	-9%


Australian Government


National
Anti-Scam
Centre