

National Anti-Scam Centre in action

Quarterly update

October to December 2023

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 © Commonwealth of Australia 2024

This work is copyright. In addition to any use permitted under the *Copyright Act 1968*, all material contained within this work is provided under a Creative Commons Attribution 4.0 Australia licence, with the exception of:

- the Commonwealth Coat of Arms
- the ACCC and AER logos
- any illustration, diagram, photograph or graphic over which the Australian Competition and Consumer Commission does not hold copyright, but which may be part of or contained within this publication.

The details of the relevant licence conditions are available on the Creative Commons website, as is the full legal code for the CC BY 4.0 AU licence. Requests and inquiries concerning reproduction and rights should be addressed to the Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 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 Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 03/24_24-05

www.accc.gov.au

Foreword

In July 2023 the government invested \$58 million in a world-leading initiative to establish and run the National Anti–Scam Centre. Our fight against scams continues through hard work and collaboration with our partners across government, law enforcement, industry and consumer groups. Together we are making progress towards our goal of making Australia the world's hardest target for scammers.

We are improving the technology and awareness needed to protect Australians from new and emerging scams and their devastating financial and psychological impact.

We have observed a notable decline in scam losses reported to our Scamwatch service over the October to December 2023 quarter.

While we are very pleased to see the decline in reported losses, we know that many Australians continue to suffer devastating financial losses, with many scams going unreported. We also know that scammers are agile and increasingly make use of technology, so we remain committed to ensuring there are no weak links in the scam ecosystem. This commitment includes advocating for mandatory and enforceable industry codes for banks, telecommunications providers, digital platforms, and cryptocurrency exchanges.

This report sheds light on the significant scams impacting Australians and underscores the key disruption and prevention initiatives undertaken in the October to December 2023 quarter.

The activities shared in this report are a testament to the expertise and contributions of the organisations who engage in the development and implementation of effective activities to target scams.

It also recognises the significant efforts of consumer advocates, financial counsellors, and victim services that support many Australians to recover from the emotional and financial impact of scams.

I extend my sincere gratitude to those actively engaging with us, and to our partners who are leading initiatives aimed at safeguarding Australians from scams.

We look forward to the ongoing work with our partners and recognise that there is much more to be done, however we are making a difference.

Catriona Lowe Deputy Chair, ACCC

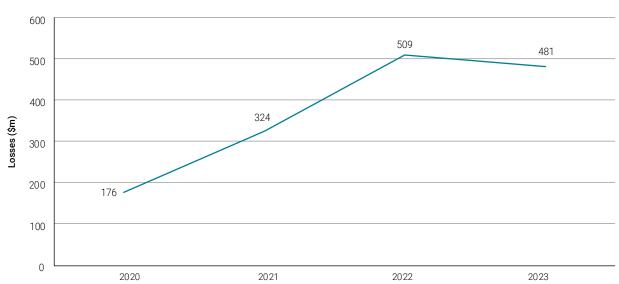
Contents

Foreword	iii
Executive Summary	1
Scams in Focus	3
National Anti-Scam Centre in Action	11
Collaboration	12
Disruption	15
Awareness	16
Support Services	20
Technology	23
Government Partner Initiatives	25
Law Enforcement Partner Initiatives	28
Looking Forward	29
Appendix 1 – Scam Data	31
Appendix 2 – Program Benefits Register	36

Executive Summary

The end of 2023 marked 6 months since the National Anti-Scam Centre was established. During the October to December 2023 quarter, we continued to see progress towards our vision of making Australia the world's hardest target for scammers.

We are achieving this through collaborative initiatives with partners in government, law enforcement, industry and consumer groups, while also engaging with Australians. Based on Scamwatch data we are cautiously optimistic that the trend of accelerating increases in losses to scams is beginning to turn.



The upward trend in losses to scams is beginning to turn

Australians reported \$82.1 million in losses to Scamwatch in the quarter. This is a reduction of 43% from the same quarter in 2022, and 26% from the July to September 2023 quarter.

Comparing data with the same quarter in 2022, we have seen significant falls, including:

- 38% decrease in investment scam losses to \$52.4 million
- 74% decrease in losses by cryptocurrency to \$12.4 million
- 31% decrease in losses by bank transfer to \$40.2 million
- 22% decrease in losses where social networking is the contact method to \$15.9 million.

Investment scams caused the greatest financial losses for Australians and phishing scams were the most reported scam type in the quarter.

Case studies are used throughout the report to illustrate how our work with partners across government, law enforcement and industry is protecting Australians from ever-more technically sophisticated and callous scams. We are, however, mindful of not disclosing strategic details that scammers could use to counter our prevention and disruption efforts.

Helping consumers spot and avoid scams

Promoting awareness of scams and ensuring victims can access support services is an ongoing priority.

In November 2023, we delivered the annual Scams Awareness Week with the theme 'Who's really there?'. The campaign was successfully delivered in collaboration with members of the <u>Scams</u> <u>Awareness Network</u> through media releases, paid media advertising, and organic social media content reaching millions of Australians.

We also engaged with the Consumer Education Network and presented at events run by Westpac and the Australian Taxation Office (ATO).

We continued working with organisations who engage with at-risk groups. This included interviewing people who had reported to Scamwatch to better understand their experiences and to inform our development of timely and clear guidance on scam identification and protection.

Coordinating scams prevention, disruption, and awareness activities

During the quarter, the Treasury published its consultation paper on the proposed Scams Code Framework. The ACCC lodged a submission, endorsing the introduction of mandatory industry codes and ensuring effective protections for consumers.

The investment scam fusion cell, co-led by the National Anti-Scam Centre and the Australian Securities & Investments Commission (ASIC) piloted a new disruption technology to break contact between scammers and potential victims.

In October 2023, our Executive General Manager attended the Global Anti-Scam Summit, where under-reporting of scams was highlighted as a significant issue worldwide.

We also hosted an online industry forum to provide an update on our key activities and invite questions from industry representatives.

Collecting and sharing data and intelligence across the scam ecosystem

Drawing on data and intelligence gathered from across the scam ecosystem we share details about social media scams through media releases and alerts on the Scamwatch website as well as with our working groups and networks.

Scams in Focus

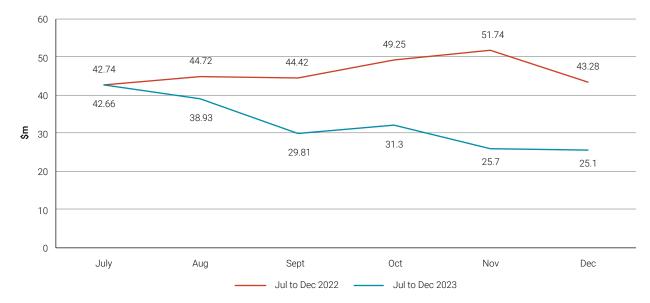
Infographic data is sourced from Scamwatch. It does not include data collected by ReportCyber or Australian Financial Crime Exchange, Australian Taxation Office, Australian Securities & Investments Commission, Australian Communications and Media Authority, which informs our annual Targeting Scams Report.

Since the establishment of the National Anti-Scam Centre, reports to Scamwatch indicate Australia has experienced a steady decrease in scam losses, which is largely due to a sharp decline in investment scams. Investment scams were chosen as the focus of our first fusion cell because losses to this type of scam are so high.

Total losses in December 2023 were \$25.1 million, down 41.7% compared to December 2022. The chart below illustrates the 6 straight months of declining losses compared to the 6 corresponding months in 2022. Investment scams were chosen as the focus of our first fusion cell because average losses to this type of scam are so high.

Comparing data with the same quarter in 2022, we have seen significant falls, including:

- 38% decrease in investment scam losses to \$52.4 million
- 74% decrease in losses by cryptocurrency to \$12.4 million
- 31% decrease in losses by bank transfer to \$40.2 million
- 22% decrease in losses where social networking is the contact method to \$15.9 million.



Scam losses July to December 2022 and 2023 (\$ million)

The Quarter – October to December 2023

Scam losses

Australians reported losses of \$82.1 million in the quarter, reflecting a 26% decrease in losses compared to the July to September 2023 quarter, and a 43% decrease in losses compared to the same quarter in 2022.

The average reported scam loss was down \$1,224, which represents a 14% decrease compared to the July to September 2023 quarter.



Scam reports

Australians lodged 67,116 scam reports to Scamwatch in the October to December 2023 quarter, a 14% decrease compared to the July to September 2023 quarter, and an 8% decrease compared to the October to December 2022 quarter.



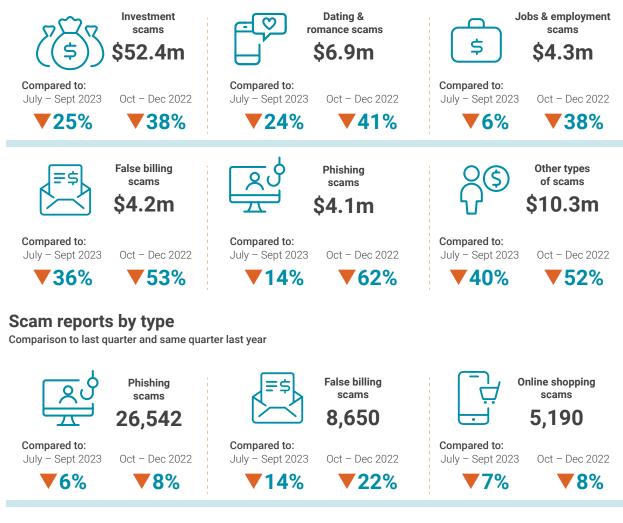
Types of scams

Investment scams continue to cause the greatest financial harm, although there is cautious optimism that prevention and disruption initiatives being rolled out across the national anti-scam ecosystem are having an impact.

Phishing scams were the most reported scam type in the quarter, making up 40% of total reports. However, losses to phishing scams were down by 62% compared to the October to December 2022 quarter.

Scam losses by type

Comparison to last quarter and same quarter last year





Compared to: July – Sept 2023

22%



Identity theft

scams



Compared to: July – Sept 2023



Hacking

23 Oct – Dec 2022





Other types

scams

19,868

In the quarter the National Anti-Scam Centre detected an increase in the number of reports of fake websites that look like genuine online retail stores. To help address this, we worked with retailers to disrupt scam activities and published advice for businesses impacted by scammers impersonating them. This involved sending direct requests to web hosts to take down scam websites and sharing advice with brands being impersonated on how they could make an intellectual property claim to web hosts. We also used media releases to raise awareness of online shopping scams and provide tips on how consumers can protect themselves. For example, in November 2023, ahead of the Black Friday and Cyber Monday sale weekend, we published a media release warning consumers to watch out for scam websites impersonating high-profile Australian retailers. The number of reports about online shopping scams decreased from 5,583 in the July to September 2023 quarter to 5,190 in the October to December 2023 quarter, indicating our education initiatives are having a positive impact.

Social media scams in focus

Scammers use social media data to strategically target people with scam advertisements that are based on profile preferences, personal details, and browsing history. However the reduction in the last quarter follows significant increases since 2020.

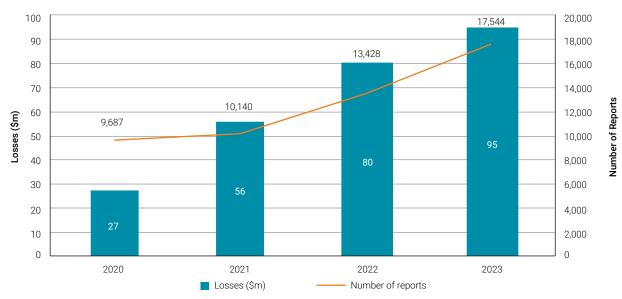
In the October to December 2023 quarter, 3,792 people reported \$15.9 million in losses to scams initiated on social media platforms or online forums. While down 36% on the previous quarter, and 22% on the same quarter in 2022, it still represents 20% of all reported losses to scams for the quarter.

Of social media scams, people over 65 experience the highest losses of any age group with 30% of all losses for social media being attributable to people over 65. This is a 57% increase compared to the previous quarter for this age group.

In 2023, losses to social media scams reached \$95 million which is a 249% increase in reported losses since 2020. In 2023 the majority of losses to social media scams occurred from contact via Whatsapp (47% of losses), Facebook (20%), Online dating sites (9%) and Instagram (9%).

For the calendar year, over 16,000 people who reported losing money to a scam said it started on a social media platform or an online forum with an ad, a post, or a message. Many people reported placing an order, usually after seeing an ad, but never received their goods. Some reports described advertisements that impersonated real, online retailers.

Scammers take advantage of their anonymity, and the relative low cost in reaching a wider audience through fake advertisements and other forms of contact, on social media.



Annual reported losses and number of reports from scams originating via social media or online forums from 2020 to 2023.

Impact of scams on particular communities

Impact of scams on First Nations people

Research conducted with organisations and advocates working with First Nations communities in the October to December 2023 quarter found scams affecting First Nations people are broad. In addition to the devastating financial impact, our interviews uncovered insights into the high sense of shame First Nations people experience if they are scammed.

First Nations people lodged 3% of reports to Scamwatch and lost \$541,615 to scams, resulting in approximately 1% of total losses in the October to December 2023 quarter.

Investment scams caused almost a third (\$166,262) of total scam losses. While this is still too high, it represents a 60% decrease compared to the July to September 2023 quarter. Financial losses related to dating and romance scams increased by 73% to \$136,371 compared to the July to September 2023 quarter.

First Nations People

Comparison to last quarter and same quarter last year



Impact of scams on culturally and linguistically diverse communities

Scammers stole \$8 million from people belonging to culturally and linguistically diverse (CALD) communities, which is 10% of the total losses in the October to December 2023 quarter. Alarmingly, members of the CALD community accounted for 88% of losses from 'threats to life, arrest, or other' category of scam, amounting to \$2.7 million. These scams involve tactics such as criminals posing as police targeting, intimidating, and stealing from international students studying in Australia.

Culturally and Linguistically Diverse (CALD)

Comparison to last quarter and same quarter last year



Impact of scams on people living with disability

Scammers target people living with disability. However, our research found people living with disability don't see themselves as more vulnerable to scams than other Australians.

People living with disability lost \$6.4 million to scams and lodged 8% of reports to Scamwatch in the October to December 2023 quarter. While down by 36% compared to the July to September 2023 quarter, at \$3.6 million, investment scams remained the top scam type, accounting for 56% of total losses, followed by dating and romance scams. False billing scams are particularly prominent among those living with disability.

People living with disability

Comparison to last quarter and same quarter last year



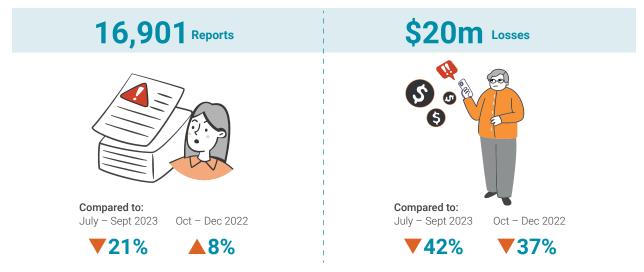
Impact of scams on older Australians

People aged 65 and over lost \$20.4 million to scams over the quarter, down 42% compared to the July to September 2023 quarter.

People in this age bracket were most impacted by investment scams as well as dating and romance scams.

Scam reports and losses for Australians aged 65+

Comparison to last quarter and same quarter last year



Scam contact methods

Text messages (38% of all scam contacts, 5% of scam losses for the quarter), emails (30% contacts, 19% losses) and phone calls (17% contacts, 28% losses) were the top 3 methods scammers. These methods accounted for 84% of all contacts and 51% of all scam losses in the quarter.

Top scam contact methods

Comparison to last quarter and same quarter last year



The highest financial losses were to scams where the contact method was phone, social media or email.

Top scam contact methods by losses Comparison to last quarter and same quarter last year \$15.5m Email \$15.9m Social media S24.5m Phone calls Compared to: Compared to: Compared to: July – Sept 2023 Oct - Dec 2022 July – Sept 2023 Oct - Dec 2022 July – Sept 2023 Oct - Dec 2022 **35% 22% 23% 10% 36% ▲11%**

Funeral live streaming scams: case study

In December 2023, the National Anti-Scam Centre identified an increase in the occurrence of a live streaming funeral service scam targeting friends and family mourning loved ones.

Australians were asked to subscribe to a funeral streaming site with a credit card to help the family pay for a live stream of the funeral. However, the content was not delivered, and/or the scammer failed to cancel the subscription when asked.

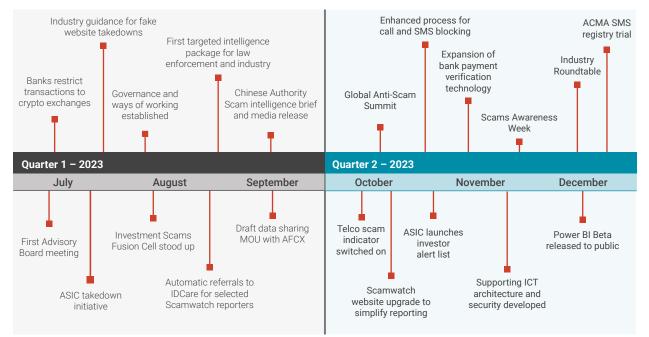
Scammers sent a Facebook friend request from an account featuring the official funeral notice originally shared by a legitimate account. At this time, we received reports of scammers targeting the funeral of a federal member of parliament. Reporters shared a link to the livestream on Facebook and the National Anti-Scam Centre contacted Meta requesting takedown of the livestream link. Meta acknowledged they were aware of the scam and were taking action against it.

National Anti-Scam Centre Executive General Manager Heidi Snell participated in a media interview alerting Australians to the scam and taking the opportunity to reinforce our messaging on how to spot and avoid scams.

National Anti-Scam Centre in Action

In this quarter we continued to work with and draw on expertise across government, law enforcement, industry, and consumer groups to make Australia a harder target for scammers. Together we collected and shared scam data and intelligence, implemented scam prevention and disruption initiatives, and provided better awareness alerts and education resources to help consumers identify and avoid scams. Key achievements are highlighted in the timeline below.





Collaboration

The National Anti-Scam Centre brings together expertise across Australia's anti-scam ecosystem, with working groups including members from government, law enforcement, industry, and consumer groups.

This collaboration provides opportunities to:

- optimise processes that provide early identification of emerging scams
- leverage new data flows and collection methods
- align communication messages and campaigns.

Spotlight on the Emerging Trends and Response Working Group

The Emerging Trends and Response Working Group implements strategies and processes to monitor scam trends and identify groups that are at risk of emerging scams.

Members represent a diverse mix of industries, along with government agencies and law enforcement. Members' extensive connections to industry sectors and culturally and linguistically diverse communities are leveraged to facilitate disruption and awareness activities in response to intelligence and data insights.

In this quarter, the Emerging Trends and Response Working Group identified false billing scams as an emerging trend with reported losses to these scams increasing in 2023.

The working group agreed to explore actions to combat false billing scams. The group identified two common variations. The most common type involved the impersonation of an email address – for example, a scammer pretending to be from an energy company and changing the email address by 1 or 2 letters to redirect a payment. A smaller number of reports are 'business email compromise' where a business has had its system compromised and the scammer has been able to send emails directly to the customer and redirect a payment.

Further analysis of business email compromise scams revealed that sectors most targeted by false billing scammers were:

- building, construction, and trade
- clubs, sporting groups, and community organisations
- health care
- business services, including accounting
- real estate.

A sample of Scamwatch data revealed that out of 156 reports, most (87) used a fake email address to impersonate a business and only 25 indicated a compromise of the business email system.

In these situations, the scammers generally send hundreds or thousands of emails, impersonating a legitimate business, hoping that recipients will pay the invoice because they happen to have made an order from the business being impersonated, or because they simply assume the invoice must be genuine.

Three initiatives will be undertaken in the next quarter:

- strategic engagement with key sectors
- law enforcement business email compromise initiatives
- consumer messaging for false billing scams.

Collaborating with Industry

The National Anti-Scam Centre hosted an online industry forum in December 2023, attended by more than 100 industry participants from organisations with limited previous engagement with us. These organisations included small digital platforms and application developers, money transfer operators, private investigators, national supermarkets, and international professional services firms.

The forum provided an opportunity to share information about our activities and achievements, while also responding to questions from participants.

The industry forum resulted in heightened awareness about our operations and generated partnership interest in the work against scams, including many requests to join the Scams Awareness Network.

Going forward, we will hold regular forums to maintain engagement with a wide cross-section of industry representatives.

International Collaboration

The Global Anti-Scam Summit

The Global Anti-Scam Summit, held in October 2023, was a valuable opportunity for government agencies and industry participants from around the world to share knowledge and strategies in the fight against scams.

Australia, along with other participating nations, contributed to the Global State of Scams Survey, the results showing a devastating picture of the worldwide effect of scams, highlighting the urgent need for action.

According to the survey, more than one quarter of the world's citizens lost money to scams or identity theft in 2022, culminating in financial losses estimated at US\$1.026 trillion.

The survey also highlighted that under-reporting of scams is a global issue with less than 40% of people impacted by a scam reporting their experience to the police or other government authority. Close to a quarter of people surveyed felt reporting a scam would not make a difference, but those who do report have a 1.5% higher chance of getting their money back than those who do not report.

Globally, only 3% of nations experienced fewer scam instances than the previous year. Australia was among the countries that experienced the highest growth in the number of scams.

The summit advocated for:

- a more global focus to fighting scams, including better international data sharing and best practice guidance
- an early alert system for emerging scams
- supportive consumer messaging that does not shame victims.

International Fraud Council

The National Anti-Scam Centre joined other members of the International Fraud Council from Japan, Singapore, the United Kingdom, Canada, the USA and New Zealand to develop an agenda and key messaging for the March 2024 Global Fraud Summit. The agenda focused on anti-scam best practices as well as legislation and policy recommendations for United Nations member states.

Disruption

This quarter the Investment Scam Fusion Cell continued to meet fortnightly and pursue disruption strategies to drive down investment scam losses. Areas of focus included:

- piloting call disruption technology to break contact between a scammer and a potential victim of an investment scam
- collating best practice guidance for disrupting investment scams
- identifying and taking down investment scam advertisements and websites.

One area of focus was imposter bond scams where scammers impersonate financial companies or banks and offer government / Treasury bonds or fixed term deposits. The case study below describes how we are working to disrupt this type of scam.

Imposter bond scams: case study

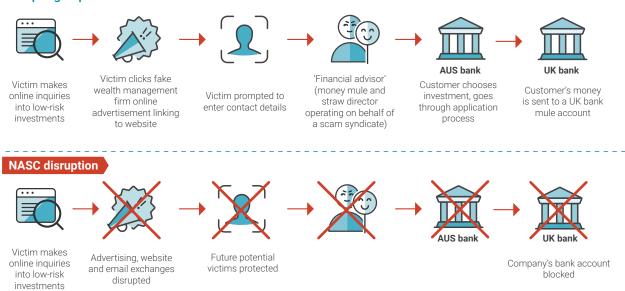
A local wealth management firm notified the National Anti-Scam Centre that it was being impersonated as part of an imposter bond scam.

Consumers inquiring about low-risk investments, such as term deposits and investment bonds were drawn into the scam. After clicking on an online advertisement, they were prompted to enter their contact details. This initiated contact with a (fake) 'financial advisor' who provided professional looking prospectuses and other documents. They were then asked to complete an application process which involved providing personal identification documents and subsequently transferred money to bank accounts controlled by criminals.

With ASIC and other partners, we disrupted this scam by removing the advertisement, taking down the scam website, providing an Investor Alert to the public, and diverting attempted calls by victims to a recorded warning message.

Bank accounts used to launder stolen money were blocked by the relevant banks. Intelligence was shared with police, who passed on relevant information to overseas enforcement partners.

Disrupting imposter bond scams



Awareness

Scams Awareness Week



The annual Scams Awareness Week communication campaign ran from 27 November to 1 December 2023.

The theme of impersonation scams with the tag line 'Who's really there?' was selected to reflect the high level (approximately 70%) of reports to Scamwatch that involve impersonating a legitimate organisation or person.

The Assistant Treasurer and Minister for Financial Services, Hon Stephen Jones MP, launched the campaign with a media release. His address to Parliamentary Question Time attracted good media coverage, television coverage on Nine and Seven News, as well as radio clips aired throughout the day.

Campaign achievements:

- Published 2 media releases, one about fake retail website scams in the lead up to Black Friday, and one to raise awareness about impersonation scams in general. These media releases secured a combined 647 media mentions with potential reach of over 13 million Australians.
- Ran a targeted paid media campaign on Meta and Snapchat. Snapchat proved to be highly successful driving 26% of traffic to the campaign landing page. Meta reached 1.4 million people on Facebook and Instagram, and Snapchat received 1.3 million impressions.
- Posted organic social media content with 21 posts across Facebook, Instagram, Twitter (X) and LinkedIn over the campaign period. The campaign achieved over 126,000 impressions and 5,835 engagements through Scamwatch and ACCC organic channels.
- Engaged with the Scams Awareness Network and the Consumer Education Network to align and amplify messaging. The Consumer Education Network comprises officials from the ACCC, Treasury, ASIC and state and territory and New Zealand agencies responsible for consumer affairs to collaborate and undertake coordinated information and education campaigns.
- Presented at several events run by Westpac and the Australian Taxation Office (ATO).
- Shared a stakeholder toolkit with over 400 partners across government, law enforcement, industry, and consumer groups. These organisations used their own channels to promote animated videos, social media tiles, and key messages.
- Collaboration with the eSafety Commissioner resulted in a podcast and impersonation scams guide delivered to a newsletter subscriber base of 22,000.

Media

The media continues to be interested in new and emerging scams and how they impact Australians.

Across the quarter there were 91 media queries across a range of key themes and scam types, including:

- cryptocurrency investments
- fake retail websites
- PayID
- rentals
- celebrity endorsement
- jobs scams.

Over the quarter, we saw increased reach and engagement with our digital channels.

Digital reach



175,454 subscribers to scam alert emails

Community engagement and outreach

Our aim is to raise awareness of scam detection and prevention, arm consumers with the tools to protect themselves, and to understand the scam-related issues that 'at-risk' groups are facing.

We prioritise supporting organisations who engage with 'at-risk' groups and those who are over-represented in scam victim numbers. These communities may encounter barriers to accessing, interpreting, or applying our standard communications messages.

Over the quarter, we engaged with:

- Carers ACT to understand how seniors and those living with disability can access scam-related support.
- State, Territory, and Commonwealth representatives on the National Indigenous Consumer Strategy group to discuss approaches to scams impacting First Nations Australians and a proposed alert service for remote communities in Western Australia.
- Rural Financial Counselling Services and Grazing Futures Business Resilience Project to reach and support members of the many isolated rural communities dispersed across Australia.

Vietnamese Community scam: case study

Early in the quarter, our intelligence identified an evolution of the authority scam targeting Mandarin speakers to also target Vietnamese speakers. This followed our earlier intelligence work and related media release in late September 2023 warning Chinese students living in Australia to be vigilant of an increase in scammers using alarming tactics to threaten, intimidate and steal from them.

Scammers contacted Vietnamese Australians and accused them of sending a package of credit cards and fake passports to Vietnam, which were supposedly being held in Vietnamese customs.

Through phone contact, people were transferred to a scammer pretending to be from Vietnamese police or customs who accused them of being involved in serious crime. Some cases involved claims of money laundering via a Vietnamese bank account and victims were asked to provide personal details to clear their name. Other cases were aimed at obtaining personal details while pretending to help the victim clear their name.

In December 2023, a new variation on the scam emerged, where criminals impersonated the Australian Federal Police.

This type of scam is highly sophisticated and convincing because it involves multiple perpetrators who play on victims' fears and threaten them and their family with years of jail time.

Leveraging learnings from the Chinese authority scam, we proactively reached out to Vietnamese community groups, university student associations and the Vietnamese embassy to disseminate in-language information to warn potential victims of the scam and provide guidance on scam identification and protection.

These actions directly contributed to the significant fall in financial losses (down 61%) to threats to life, arrest or other scams between quarter 1 and quarter 2 2023.

Using data and intelligence

Over the quarter, we reviewed Scamwatch reports and used intelligence from partner organisations to raise awareness of new, emerging, and trending scams.

We also identified industry sectors being targeted by scammers and provided awareness and protection information to industry bodies and businesses. This included engaging with recruitment firms and jobs boards to promote awareness about scams targeting job seekers.

Support Services

Realising you've been scammed can be devastating. The impact of scams extends beyond just financial losses. Reports to Scamwatch highlight the significant emotional and social harm caused by scams, including mental health crisis.

The shame and self-blame associated with scams can create isolation and trauma that can be difficult to overcome. Many Australians report losing their entire life savings, their superannuation, or their home as well as friends and family. Sadly, we are also aware of Australians who have died from suicide because of a scam.

If you have been scammed and need someone to talk to, you can contact:

- Lifeline on 13 11 14
- Beyond Blue on 1300 22 4636.

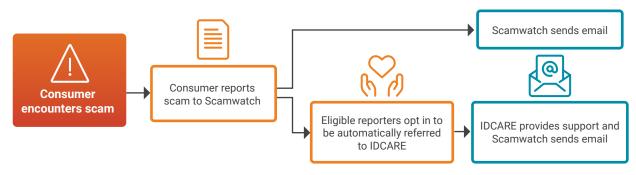
Best practice victim support

We are committed to enhancing and expanding our victim support capabilities.

In 2023, we worked with IDCARE, a not-for-profit support service, to implement a process to support people who experienced significant financial loss or were at high risk of identity compromise. These people are now automatically referred to IDCARE with their consent.

Everyone who makes a report to Scamwatch receives an email with information about how to protect themselves, including an IDCARE reference code that can be used to contact IDCARE.

Improvements to victim support during Scamwatch reporting



During the quarter, we interviewed a sample of people who reported to Scamwatch to better understand their experiences and whether our support services meet their needs.

Our interviews focused on:

- the questions they needed answered
- the types of information and support they received
- how helpful they found that information and support.

Throughout our interviews, scam reporters noted the importance of timely help, guidance on what to do next, and access to information from experts. Reporters told us they were assisted by 'checklist' style information, tailored to their specific experience, to guide them through recovering from identity compromise, and referrals to other services. For those presented with the option, uptake of the automatic referral process was high with 88% of reporters consenting in the 6-month period since implementation.

In the October to December 2023 quarter, we made 1,942 automatic referrals to IDCARE. We will continue to speak with victims to learn from their experiences and remain committed to providing better support for those who have experienced a scam.

Scam victim experience: case study

Jane does most of her banking online. One day she receives an SMS from her bank which says, "your transfer of AUD2,800.00 was paused – if you did not make this transaction, please call 1300XXXXXX to confirm payment – ref XXX".

The message appeared in the same text history as other legitimate messages from her bank.

Jane immediately calls the number and speaks with Martin who states he is from her bank's fraud team. Martin goes through Jane's bank's standard security questions – which Jane has answered many times before – and without Jane assisting he says he can see that she paid her energy bill last week, her phone bill 10 days ago, and he verifies Jane's full name and contact number.

Martin assures Jane that he can help her secure her account with two-factor authentication. Jane receives another SMS in the same text history with a one-time password which she relays over the phone to Martin. Martin continues to assure Jane he is securing her account, keeping her on the phone as he asks her to log out to check whether the new security measures are working. When the security procedure is almost complete, Martin asks Jane to change her password. Jane becomes suspicious and logs back in to see several large withdrawals.

Panicking, Jane hangs up and searches for her bank's phone number online—it's different to the 1300 number she called previously. She speaks with Amanda. Jane explains that she has just been scammed. Going through the bank's standard security questions with Amanda feels like it is taking such a long time, and what Jane needs is urgent help to get her money back. Once her identity is verified, Amanda informs Jane that it is "too late" and the money is gone. Amanda freezes Jane's account and tells Jane to go to her local branch to reactivate her account with 100-points of ID. Jane goes to her local branch immediately but is told her account can't be reactivated until an investigation is complete. In the meantime, bank branch staff suggest she lodge a police report.

Now distraught, Jane goes to her local police station, but the officers advise her that cases of bank fraud are best reported online through the ReportCyber website. Jane tries to lodge a report, but the form requires her to include details on the account the funds went to, and Jane can't access this information while her account is frozen.

Jane's story comes from a real Scamwatch report. Coordinated efforts across government and industry will help to address the methods scammers used to target Jane and the hurdles Jane faced in getting help:

- A new SMS sender ID registry is designed to disrupt a specific type of SMS impersonation scam, where scammers send SMS with alphanumeric sender IDs to imitate well-known brands such as banks.
- New obligations on banks to implement an anti-scam strategy under the proposed economy-wide mandatory industry codes.
- A 'no wrong door' approach to victim reporting, providing clear pathways of support and complaints handling for those who have been affected by scams.

Technology

A technology solution with real-time data sharing and intelligence capability to prevent, disrupt, investigate, and block scams, continues to be supported by our partners.

Through specialised forums, we collaborate with our partners to achieve:

- significant increases in scam data and intelligence
- continuous improvements to information sharing across the anti-scam ecosystem
- improvements in the quality and integrity of data.



National Anti-Scam Centre data sharing ecosystem

Over the quarter, other data sharing highlights included:

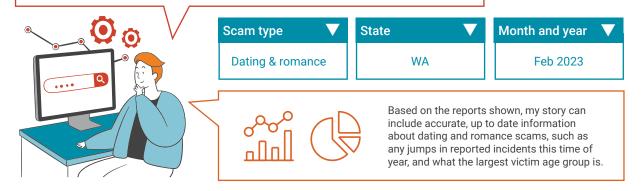
- Successful consumption of scam and general intelligence data from ReportCyber, now ready to be considered for scam trend analysis alongside Scamwatch reports.
- Extending our scam data sharing arrangements with the Australian Financial Crime Exchange (AFCX) and providing a wider range of suspect data to all member institutions, regardless of sector.
- Cooperation with the Australian Securities & Investments Commission (ASIC) to share investment scam reports and automated sharing readiness.
- Engaging with the Australian Taxation Office (ATO), Services Australia, Australian Communications and Media Authority (ACMA) and the Australian Federal Police (AFP) on how to exchange data in a timely and automated method.
- Continued focus on phone and text scam data, including SenderID, with telecommunications providers.
- Preparing for cryptocurrency scam data to be collected commencing in early 2024, to begin the necessary work to begin making scam data available to the Digital Currency Exchange sector.

Power BI Beta release

We have developed and made a scam statistics dashboard publicly available on the National Anti-Scam Centre website in a public Power BI Beta release. Feedback will be used improve our understanding of the type of scam data consumers would like to access, and how it is best displayed to meet their needs.

Journalist uses Power BI Beta

I'm a journalist in WA and I'm writing a story on the prevalence of romance scams in the lead up to Valentines Day. Here is what I search in the National Anti-Scam Centre Power BI Beta tool.



Government Partner Initiatives

The Treasury

The Government has committed to introducing new mandatory industry codes. These codes will outline the responsibilities of the private sector in relation to scam activity with a focus on banks, digital communications platforms, and telecommunications providers.

In November 2023, the Assistant Treasurer and Minister for Financial Services, the Hon Stephen Jones MP, and the Minister for Communications, the Hon Michelle Rowland MP, consulted on a proposed <u>Scams Code Framework</u> (the Framework) with the release of a consultation paper outlining the proposed features of the Framework and an anonymous survey for members of the public.

The survey sought information on consumers experience with scams, the impact on individuals, and improvements that could be made to reduce this impact.

The Government is considering stakeholder submissions and survey responses to inform the implementation of the Framework.

Australian Communications and Media Authority

The ACMA is continuing its work to disrupt scams before they reach Australians, including supporting new disruption initiatives and enforcing anti-scam rules.

SMS sender ID registry

As part of the Government's 'Fighting Scams' initiative, the ACMA is implementing an SMS sender ID registry. The registry will protect the alphanumeric message headers (shortened business names or related tags, such as 'ATO' or 'NAB') of brands and government agencies from impersonation.

In December 2023, the ACMA commenced a pilot phase of the registry, which will consolidate and centralise existing sender ID protections with some well-known brands and agencies. The pilot will be expanded in early 2024, focusing on brands that have been the target of impersonation scams.

Scam call and SMS blocking

In January 2024, telecommunications providers reported to the ACMA on scam call and SMS blocking activities for the period October–December 2023. Telecommunications providers reported blocking over 246.7 million scam calls and over 106.7 million scam SMS under ACMA registered rules.

Enforcing rules

The ACMA is continuing its work under the 2023–24 compliance priority to combat SMS scams. The ACMA has been auditing the compliance of SMS aggregators (telecommunications providers that send bulk SMS) to identify potential issues that could expose Australian networks to scams.

The ACMA recently acted against Telnyx Australia Pty Ltd, after its investigation found it <u>breached</u> <u>multiple anti-scam and public safety rules</u>. The ACMA also directed <u>Twilio Inc and Vonage Business</u> <u>Inc to comply with the anti-scam rules</u>.

Once a provider is directed to comply, it makes future enforcement easier to apply where breaches are found, including civil penalties.

Attorney General's Department

Expanding support services for victims of identity theft

The Attorney-General's Department received \$21.2 million following the Mid-Year Economic and Fiscal Outlook to deliver and improve support services for victims of identity theft and misuse.

This funding will:

- build on existing services provided by government and not-for-profit organisations
- help more individuals access tailored support and guidance to recover from identity compromise
- educate Australians on how to better protect themselves from identity theft and misuse through increased awareness.

Australian Securities & Investments Commission

Website takedowns

The quick removal of harmful websites is one of the most effective ways to stop financial criminals from harming Australians.

In November 2023, the Assistant Treasurer highlighted the capabilities of ASIC's scam website takedown service by providing an update on the thousands of websites taken down.

ASIC is working with Netcraft Ltd, a company specialising in cybercrime detection and disruption, to remove or limit access to malicious phishing and investment scam websites.

ASIC targets websites that are:

- fake or imposter entities offering financial services or investment scams
- fake trading platforms
- crypto-asset investment scams
- fake news articles and celebrity endorsement websites involving investment scams
- fake cryptocurrency and investment comparison websites
- fake bank scams.

These websites seek to steal consumers' information and money. ASIC expects the takedown service to impact the reach of these financial criminals, particularly those located offshore.

Between 1 July and 31 December 2023, Netcraft has initiated the takedown of more than 3,840 investment scam and phishing websites. This includes over 3,490 sites that have been taken down, and almost 350 sites that were in the process of being taken down.

ASIC's scam website takedown capability is part of the government's Fighting Scams initiative to disrupt scams and protect Australians from financial harm. This initiative supports our program of anti-scam work.

Approximately 30% of scam reports received by Scamwatch involve a website.

ASIC's investor alert list

Investor alert list: If it's on the list, don't take the risk

ASIC launched a public investor alert list in November 2023, which includes domestic and international entities ASIC is concerned are offering financial services to Australians without appropriate licenses, exemptions, authorisation, or permission.

The investor alert list helps to inform consumers about investments that could be fraudulent, a scam, or unlicensed.

It also includes 'impostor' entities who impersonate or falsely claim to be associated with a legitimate business (impersonation scam).

The investor alert list is shared in real-time with the AFCX, whose membership includes the major banks. Entries are also added to the International Organisation of Securities Commission's Investor Alert Portal.

Between 8 November 2023 and 31 December 2023, ASIC added 239 entries on the investor alert list.

Cryptocurrency Trading: Case Study

On 12 December 2023, ASIC received a report involving an Australian consumer who had spotted a website claiming to offer forex and cryptocurrency trading.

Following its assessment, ASIC referred the website to Netcraft for takedown, which subsequently occurred within 48 hours.

ASIC also considered it was necessary to warn other Australians who were considering investing through the website (or had invested through the website) and issued a warning through the investor alert list on 22 December 2023.

The investor alert list is available on ASIC's Moneysmart website. Moneysmart is a trusted source of financial information and tools for Australians to help manage their money and make everyday money decisions. Moneysmart provides detailed information on financial scams and how they work, including investment scams, superannuation scams, and cryptocurrency scams.

Law Enforcement Partner Initiatives

All state and territory police forces, along with the AFP and the Joint Policing Cybercrime Coordination Centre (JPC3) are represented on our boards and working groups, providing opportunities for intelligence sharing to support investigation and prosecutions.

State and territory law enforcement continued their work addressing scams through various investigations and initiatives, including in partnership with their overseas counterparts.

Australian Federal Police

The AFP continues to target cross-jurisdictional and international scams.

Key initiatives in the quarter included:

- Identifying an emerging scam where criminals claiming to be United Nations officials offered travellers money to transport illicit drugs.
- Infiltrating a scam ring operating out of Malaysia, which developed phishing kits designed to
 deceive users of Australian Government websites. The JPC3 developed and provided intelligence
 to the Royal Malaysian Police, identifying a Malaysian national advertising phishing kits targeting
 the Australian Government's myGov website.

State and Territory Police

Victoria Police's Cybercrime Intelligence Assessment Unit worked with other law enforcement jurisdictions to change how ReportCyber reports are referred and allocated to the appropriate district. This new process is a 'victim-centric' approach in which the reports are allocated to the victim's region as opposed to the nominated or identified Person of Interest as per the data provided in the ReportCyber report.

This means that Victoria Police can quickly provide support and attention to victims when recovering their identity. This also helps the Cybercrime Intelligence Assessment create more accurate reporting to understand the effect on Victorians.

Tasmania Police continue to focus on disruption techniques to aid in victim recovery. Strong relationships with other law enforcement authorities and external organisations have ensured success in this area. The prevalence of investment scam victims and total losses highlight the importance of strong relationships nationally and globally.

Tasmania Police have invested significant resources and training in digital currency tracing that has seen immediate results and increases in referrals to overseas law enforcement authorities to detect offenders and disrupt losses.

New South Wales Police warned that the 'virtual kidnapping' scams targeting international students from China had spread to the Vietnamese community. Victims received phone calls from scammers who attempted to convince them their identity had been stolen.

Northern Territory Police charged two people in December 2023 in relation to online scam activity. Online scams remain one of largest priorities for the Northern Territory Police's Cyber Crime Unit.

Looking Forward

As the National Anti-Scam Centre continues to grow, we are undertaking more targeted disruption work with our partners.

Targeting Scams Report

The 2023 Targeting Scams Report will be released in April 2024. This report brings together scam data from ReportCyber, AFCX, ATO, ASIC and the ACMA to provide a complete picture of the impact scams had on Australians and the economy.

Mandatory codes

In January 2024, we provided a public submission to the Treasury's consultation on the proposed Scams Mandatory Industry Codes, welcoming the introduction of a mandatory framework and providing targeted feedback on aspects of the proposed Codes. Work will continue with the Treasury and other regulators specified in the proposed framework on the implementation of the Codes.

The government will consider whether to make registration voluntary or mandatory for alphanumeric sender IDs. The Department of Infrastructure, Transport, Regional Development, Communications and the Arts is seeking feedback by 20 March 2024 on support for the introduction of a mandatory SMS Sender ID Registry or a voluntary registry.

United Kingdom Global Fraud Summit

The International Fraud Council is holding a Global Fraud Summit in London in March 2024. The Summit brings together ministerial and senior official participants from relevant portfolios to build consensus for action. Key representatives from Australia have been invited to participate.

Technology & data

Scam reports will continue to be improved in both user experience and data collection with work to refine the data captured for scammer bank account details. The public beta for scam statistics and an accompanying survey will remain open for public feedback.

The survey will improve understanding of the different reasons people access these statistics and improve our reporting capability.

Our intelligence will be supported by a series of data sharing initiatives with our partners, bringing improved access to scam reports as well as greater depth and capability across the anti-scam ecosystem.

Scamwatch web form

Further simplification and research into alternative reporting methods are in progress for Australians wishing to report rapidly. Instead of a more detailed report, a rapid report will focus on how the criminal reaches a person and the vital details needed to find and disrupt the scam. Encouraging Australians to report a scam, whether the scammer was successful or not, is at the forefront of this work.

Fusion Cells

The Investment Scam Fusion Cell will be wound up in March. An Investment Scam Fusion Cell report will be published in April 2024. The work of the Investment Scams Fusion Cell will be evaluated with findings used to support a culture of continuous learning across the ongoing fusion cell work. The next fusion cell is expected to begin in May 2024.

Awareness

We are currently planning the 2024 Scams Awareness Week campaign in consultation with Scams Awareness Network members and the Prevention and Communications Working Group. The collaboration will identify the campaign theme for 2024 and joint promotional opportunities.

Collaboration with the Consumer Awareness Working Group to improve the consistency of scams messaging is in progress.

Victim Support

We will continue our program of work to improve our understanding of scam victim experiences and the services required to support those who are recovering from a scam.

Appendix 1 – Scam Data

Top losses by scam type (\$ million)

Sc	am Type	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
1	Investment	84.59	69.42	52.36
2	Dating & romance	11.76	9.11	6.90
3	Jobs & employment	6.93	4.56	4.28
4	False billing	8.79	6.45	4.16
5	Phishing	10.68	4.73	4.08
	Other	21.52	17.12	10.34
	Total	144.27	111.39	82.12
	Average reported loss (\$)	1,971.50	1,421.18	1,223.56

Top reports by scam type (Number of reports)

Sc	am type	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
1	Phishing	24,619	28,369	26,542
2	False billing	11,070	10,028	8,650
3	Online shopping	4,823	5,583	5,190
4	Identity theft	4,690	5,578	4,368
5	Hacking	2,774	3,745	2,498
	Other	25,200	25,077	19,868
	Total	73,176	78,380	67,116

Top losses by contact method (\$ million)

Co	ntact method	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
1	Phone calls	37.73	27.27	24.52
2	Social media	20.54	25.06	15.94
3	Email	20.11	13.96	15.53
4	Internet	20.19	15.85	8.91
5	Mobile Apps	20.87	15.63	8.95
	Other	24.83	13.63	8.27
	Total	144.27	111.39	82.12

Note: Phone contact not including SMS.

Online Forums include social media sites, some online trading sites such as Gumtree and eBay, professional forums like LinkedIn and Seek.com, and online dating sites.

Top 5 reports by contact methods (Number of reports)

Co	ntact method	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
1	Text message	28,888	23,772	25,242
2	Email	18,872	26,000	19,900
3	Phone calls	12,498	15,931	11,278
4	Social media	4,398	4,229	3,792
5	Mobile Apps	2,775	1,734	1,412
	Other	5,745	6,714	5,492
	Total	73,176	78,380	67,116

Impact of scams on First Nations people

Number of reports

Identifies as First Nation person	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Yes	1,160	1,597	1,735
No	72,016	76,783	65,381
Total	73,176	78,380	67,116

Reported losses (\$ million)

Identifies as First Nation person	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Yes	1.41	0.96	0.54
No	142.84	110.43	81.58
Total	144.25	111.39	82.12

Top scams reported by First Nations people (number of reports)

Scam type	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Phishing	314	508	925
False billing	173	222	167
Online shopping	79	137	130
Identity theft	88	161	87
Hacking	53	53	54
Other	993	1299	372
Total	1,160	1,597	1,735

Top scams reported by First Nations people (\$ million)

Scam type	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Investment	0.33	0.41	0.17
Dating & Romance	0.33	0.08	0.14
Phishing	0.24	0.09	0.06
Online shopping	0.09	0.06	0.05
Jobs & employment	0.24	0.01	0.03
Other	1.11	0.30	0.10
Total	1.44	0.96	0.54

Impact of scams on people living with disability

Number of Scamwatch reports

Identifies as person with disability	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Yes	4,960	5,758	5,055
No	68,216	72,622	62,061
Total	73,176	78,380	67,116

Reported Scamwatch losses (\$ million)

Identifies as person with disability	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Yes	6.33	9.07	6.47
No	137.92	102.32	75.65
Total	144.25	111.39	82.12

Top scams reported by people with disability (scam type)

Top Scams	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Phishing	1,258	130	1,756
False billing	658	144	714
Identity theft	335	87	400
Online shopping	274	1,670	270
Hacking	256	784	260
Other	1,909	2,943	1,655
Total	4,690	5,758	5,055

Top scams reported by people with disability (\$ million)

Top Scams	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Investment	3.78	5.63	3.63
Dating & romance	1.15	1.45	1.32
Inheritance & unexpected money	0.05	0.05 0.07	
Phishing	0.15	0.94	0.20
False billing	0.15	0.14	0.20
Other	1.05	1.51	0.72
Total	6.33	9.76	6.47

Impact of scams on culturally and linguistically diverse communities

Number of Scamwatch reports

Identifies as CALD	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Yes	3,560	2,928	3,159
No	69,616	75,452	63,957
Total	73,176	78,380	67,116

Reported Scamwatch losses (\$ million)

Identifies as CALD	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Yes	13.87	16.88	8.06
No	130.38	94.51	74.06
Total	144.25	111.39	82.12

Top scams reported by CALD communities (scam type)

Scam type	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Phishing	936	951	993
False billing	560	355	322
Identity theft	292	436	314
Online shopping	300	316	270
Classified	152	157	153
Other	1,320	1,320	1,107
Total	3,560	3,535	3,159

Top scams reported by CALD communities (\$ million)

Scam type	Oct-Dec 2022	Jul-Sep 2023	023 Oct-Dec 2023		
Investment	1.80	7.73	3.01		
Threats to life, arrest or other	6.35	1.50	2.73		
Jobs & employment	1.37	1.37 0.47			
Phishing	0.42	0.37	0.41		
Dating & romance	1.05	0.77	0.24		
Other	2.88	2.20	1.15		
Total	13.87	13.04	8.06		

Impact of scams on older Australians

Number of Scamwatch reports

Age Group	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Under 18	433	440	410
18-24	3,182	2,807	2,403
25-34	7,943	6,808	5,461
35-44	9,846	8,962	7,416
45-54	9,890	9,661	8,331
55-64	10,119	11,989	10,301
65 and over	15,597	21,349	16,901
N/A	16,166	16,364	15,893
Total	73,176	78,380	67,116

Reported Scamwatch losses (\$ million)

Age Group	Oct-Dec 2022	Jul-Sep 2023	Oct-Dec 2023
Under 18	0.11	0.07	0.18
18-24	5.85	2.85	2.24
25-34	14.95	7.88	7.34
35-44	24.96	17.06	16.33
45-54	28.05	21.04	15.64
55-64	25.29	22.18	17.01
65 and over	33.42	35.53	20.49
N/A	11.61	4.79	2.91
Total	144.25	111.39	82.12

Appendix 2 – Program Benefits Register

	Benefit name		Performance measure	Baseline FY22/23	Target FY23/24	Target FY24/25	Target FY25/26	First Half FY23/24 Actual
B1	National Anti-Scam Centre slows the acceleration of financial loss due to scams	1i 1ii	Slower growth in financial losses to scams	17% growth on previous year	12% growth on previous year	8% on previous year	5% growth on previous year	-29%
			Fusion cell activities reduce financial losses to investment scams	358,549,140	320,000,000	310,000,000	300,000,000	122,450,910
B2	between government and industry improves scam disruption and prevention	2i	Collaboration improves scam intelligence,	Not applicable	Case Study - Emerging Trends	Case Study - Data Integration &	Case Study - Prevention &	In progress
			disruption and awareness		and Response Working Group	Technology Working Group	Communication Working	
							Group	
		2ii	Fusion cells improve scam disruption	Not applicable	- Case Study Investment Scams	Case Study - Fusion Cell 2	Case Study - Fusion Cell 4	In progress
					Fusion Cell	Case Study - Fusion Cell 3		
		with priority	Increased collaboration with priority government and industry	Not applicable	Establish baseline using new Stakeholder Management Tool:	to be determined	to be determined	200 government engagements 162 Industry engagements
			partners		# government engagements			
					# industry engagements			
		2iv	Increased outreach and engagement with	22 presentations	26	26	26	9
			'at risk' groups					

	Benefit name		Performance measure	Baseline FY22/23	Target FY23/24	Target FY24/25	Target FY25/26	First Half FY23/24 Actual
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	Not applicable	Establish baseline	ТВА	TBA	In progress
		3 ii	Increase in automated data sharing arrangements to provision near realtime data to NASC partners	6	10	20	40	7
		3ііі	Increase in automated data sharing arrangements to consume near realtime data from NASC partners	0	5	10	40	1
B4	Joined up systems improve support services for scam	4 i	Improved support for consumers who lose	Not applicable	Case Study - Victim Engagement	Case Study - Victim Engagement	Case Study - Victim Engagement	Complete
	victims		money or identity to scammers					
B5	Increased scam awareness improves consumers ability to recognise, protect, and	5 i	Increase in alignment of anti-scam messaging across Prevention & Communication	Not applicable	Establish baseline via Working Group survey	80%	100%	In progress
	report on scams		working group members					
		5ii	Increase in average views per mediarelease	6 million	9 million	11 million	11 million	8,806,338
		5iii	Reduction in webform abandonment	54% abandonement	50% decrease on baseline	50% decrease on FY23/24	50% decrease on FY24/25	49% abandonement



Australian Government

