Australian Government

National Anti-Scam Centre

National Anti-Scam Centre in action

Quarterly update

July to September 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

ACCC 04/23_23–18

www.accc.gov.au

Foreword

To counter the increase in sophistication and volume of scams, and the devastating consumer harm they cause, the Australian government has invested $58 million over three years to establish the National Anti-Scam Centre. Launched on 1 July 2023, the National Anti-Scam Centre is leading a whole of ecosystem scam prevention and detection approach that will ramp up Australia's capability to protect Australians from scams.

The National Anti-Scam Centre is leveraging collective expertise and intelligence across government, law enforcement, industry, and consumer groups to disrupt scams, empower consumers, and find real solutions to reduce losses to this type of financial crime.

This is the first National Anti-Scam Centre Quarterly Report. It provides insights into the most significant scams that impacted Australians in the first quarter of FY23/24 and highlights the key disruption and prevention initiatives put into action to date.

I thank all the organisations actively collaborating with the National Anti-Scam Centre on scam-prevention and disruption initiatives. I also acknowledge our partners that are voluntarily setting up initiatives to protect Australians from scams. It is the combined impact of these initiatives and working together that will make Australia a much harder target for scammers.

Catriona Lowe Deputy Chair, ACCC

Contents

Executive summary

The National Anti-Scam Centre and its partners in government, law enforcement, industry, and consumer groups are collectively committed to working together to reduce the devastating financial and emotional harm caused by scams, and making Australia a much harder target for scammers.

Australians reported losses of $111.4 million to the National Anti-Scam Centre through Scamwatch in the July to September 2023 quarter. This is a decrease of 16% compared to the same quarter in 2022. While the financial harm caused by the top two scam types – investment scams and romance scams declined by 6% and 28% respectively, false billing scams increased by 25%.

The quarter ended with scam losses of $29.8 million in September 2023, the lowest losses reported in a single month since October 2021.

Investment Scam Fusion Cell achievements

Fusion cells are short term taskforces that bring together expertise from government and industry to take timely action on specific, urgent problems. The National Anti-Scam Centre will coordinate up to six fusion cells over three years. This quarter the first fusion cell was established to target investment scams. Early initiatives include:

- using call diversion technology that makes it possible to break scammer-to-victim contact and is crucial in reducing financial losses and emotional harm
- collating best practice industry guidance on the use of intelligence to uplift and scale up investment scam disruption across the industry
- identification and take down of investment scam advertisements to prevent harm
- referral of investment scam websites to the Australian Investment and Securities Commission (ASIC), resulting in the takedown of 32 websites.

Scam disruption achievements

- initiating takedowns of more than 2,500 investment scam and phishing websites
- protecting elderly people from wire transfer scams resulting in $60,000 in blocked scam payments
- working with banks and digital platforms to disrupt fake World Cup ticket sales and streaming-service scams, resulting in groups being shut down on digital platforms and bank accounts blocked
- the Australian Communications & Media Authority (ACMA) directing multiple telcos to comply with the Reducing Scam Calls and Scam SMS rules.

Collaboration and awareness achievements

- 2,455 scam victims being referred from the National Anti-Scam Centre's Scamwatch reporting service for specialised support services through a new automated referral system
- alerting international students of a Chinese Authority Scam, facilitating support for the victims, and publishing a related media release that reached an audience of 10 million
- media alerts about loyalty points scams and World Cup ticket sale scams widely picked up by mainstream media.

Scams at a glance

Infographic data is sourced solely from Scamwatch. It does not include data collected by ReportCyber, AFCX, ATO, ASIC, ACMA, IDCARE or Services Australia.

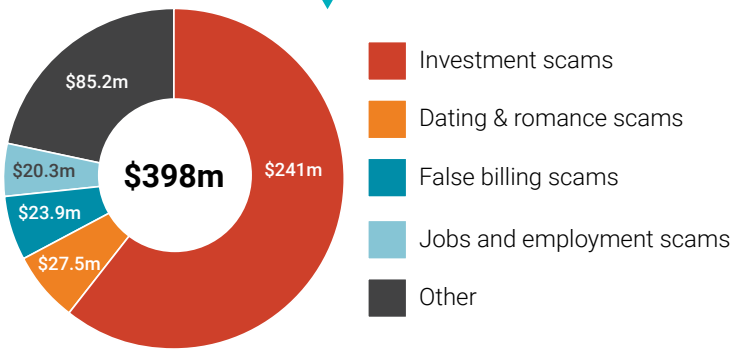
Scam losses

January to September 2023

Total losses
$398 million

▲9% on the same period last year

Average reported loss of **$16,845**

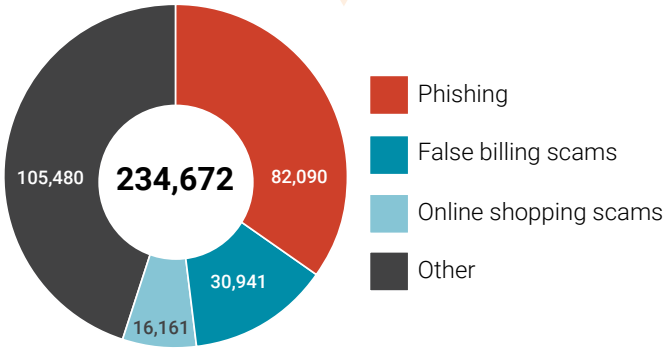


Scam reports

January to September 2023

Total reports
234,672

▲41.2% on the same period last year



The Quarter

July to September 2023

Total losses
$111 million

▼16% on the same period last year

Investment scams
▼6%

Dating and romance scams
▼28%

False billing scams
▲25%

Source: Scamwatch

Establishment of the National Anti-Scam Centre

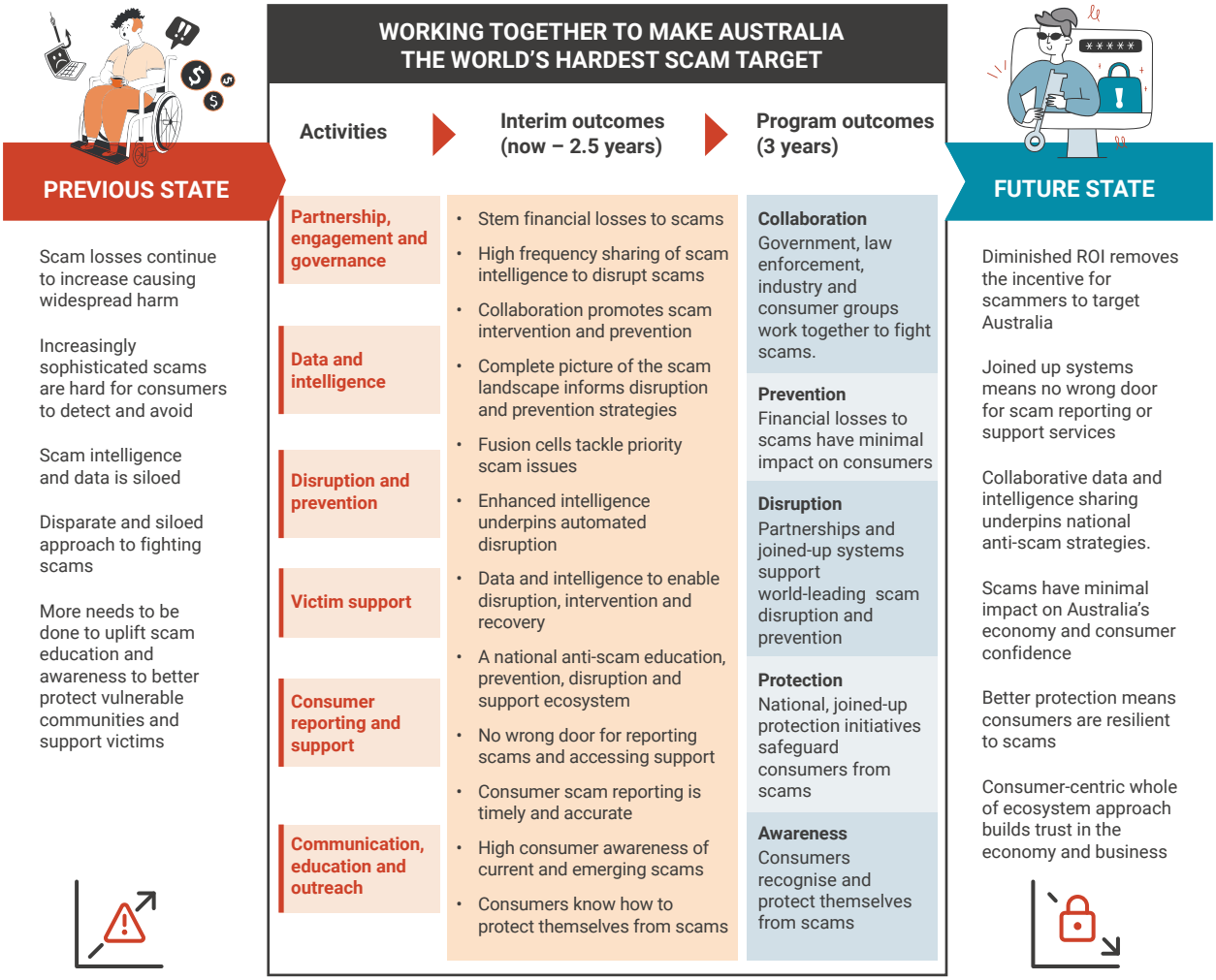
Last year Australians lost over $3 billion to scams. Scammers are becoming more sophisticated in their efforts, making it increasingly difficult for consumers to recognise and avoid scams. Victims are losing larger amounts of money through faster payment systems and cryptocurrency.

This is why, in July 2023, the government invested $58 million in a world-leading initiative to establish and run the National Anti-Scam Centre. Our remit is to facilitate partnerships across government, law enforcement, industry, and consumer groups to support the community in the fight against scams.

Our national, consumer centric, collaborative and coordinated approach will:

- protect vulnerable communities from scams
- improve consumers' ability to spot and avoid scams
- make it simpler for consumers to report a scam and victims to access support
- make Australia a less attractive target for scammers
- reduce the economic and social harm caused by scams.

Diagram 1: Australia's scam landscape Previous state and Future state



Vision

The vision of the National Anti-Scam Centre is to make Australia a much harder target for scammers. We will deliver consumer-centric, digitally enabled outreach, disruption and support services that are easy to access, simple to use and meet consumer and industry needs.

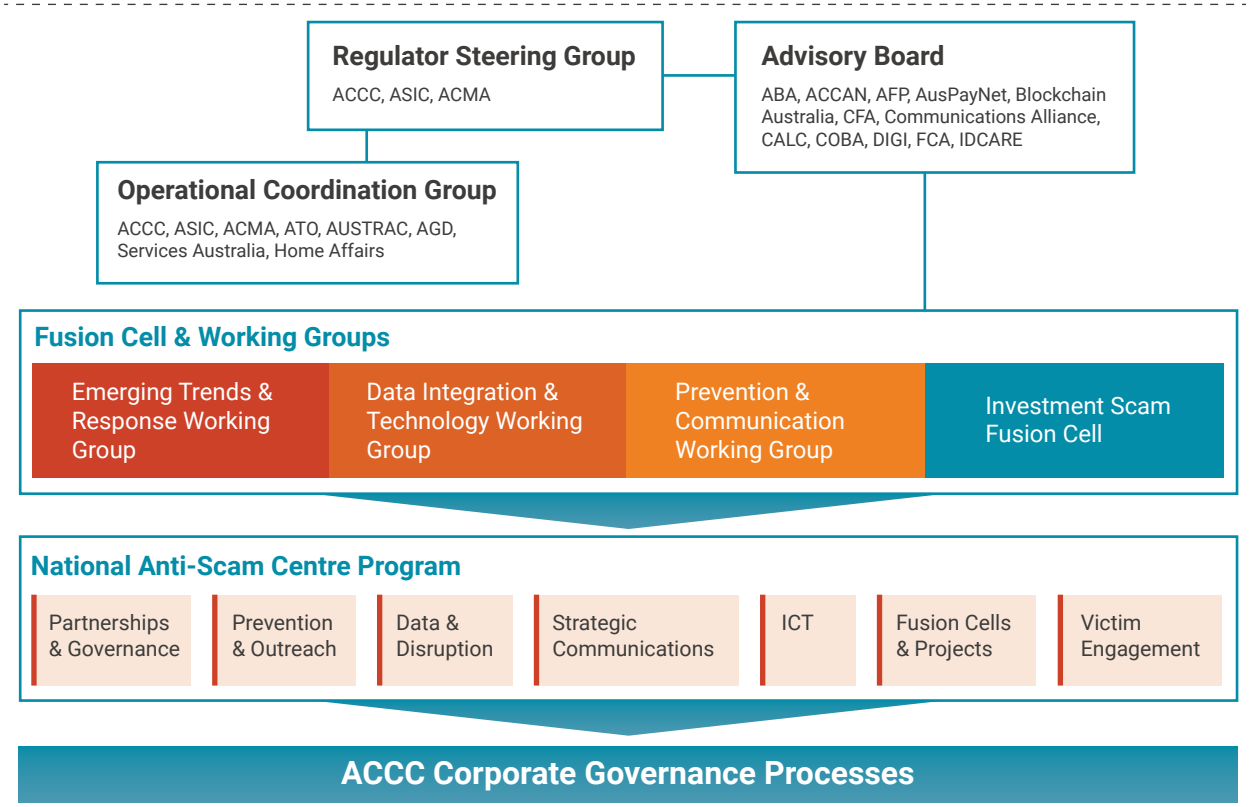
To deliver on our ambitious program of work we are focussing on three key capabilities:

1. **Collecting and sharing data and intelligence across the scam ecosystem:** to support the early identification of trends and use intelligence to inform education and disruption activities focusing on early intervention to reduce losses to scams.
2. **Coordinating scams prevention, disruption and awareness activities:** by drawing on expertise across government, law enforcement, industry, and consumer groups to lead a nationally coordinated, timely, anti-scam strategy.
3. **Helping consumers spot and avoid scams:** by collaborating with our partners across the scam ecosystem to support consistent messaging and provide better education resources to help consumers identify and avoid scams.

Governance

The National Anti-Scam Centre is led by the Australian Competition and Consumer Commission (ACCC). Our remit is to coordinate efforts across the scam ecosystem.

Diagram 2: National Anti-Scam Centre Governance Framework[1]



1 Refer Appendix A for full membership of the Advisory Board, Scams Regulator Steering group, working groups, and the Investment Scam Fusion Cell.

Scamwatch

Since 2002, Scamwatch has been run by the ACCC to raise awareness about how to recognise, avoid and report scams. The Scamwatch brand has a strong presence and is well recognised by consumers and supported by industry and government stakeholders.

To support our establishment, the ACCC has placed the Scamwatch brand within the National Anti-Scam Centre. This provides a strong platform to engage with consumers on awareness activities. We are in the process of developing a brand strategy to position the National Anti-Scam Centre and Scamwatch within the anti-scam ecosystem. The strategy will support website content, communication channels and education campaigns.

Advisory Board

The National Anti-Scam Centre is guided by an Advisory Board with representatives drawn from peak industry and consumer groups. The Advisory Board is chaired by the ACCC Deputy Chair, Catriona Lowe.

In July 2023, the Assistant Treasurer, the Hon Stephen Jones MP welcomed Advisory Board members to the first meeting. Members provide expert advice by sharing their relevant experiences and intelligence to minimise the threat and harm caused by scams.

Communiques following the monthly Advisory Board meetings are available on the ACCC website.

Regulator Steering group and Operational Coordination Group

The Regulator Steering Group comprises key regulatory agencies within the scam ecosystem and provides regulatory expertise to the Advisory Board, working groups and fusion cells. It is chaired by the ACCC Deputy Chair, Catriona Lowe.

An Operational Coordination Group, comprising senior staff from key government agencies, ensures we have a joined-up approach across government, focussing on consistent messaging and collaborative initiatives with a focus on integration, not duplication of effort.

Working groups and fusion cells

The National Anti-Scam Centre has established three working groups and a fusion cell with government, law enforcement, industry, and consumer group members. Working groups will inform our program of work, ensuring expertise is harnessed to deliver the best outcomes for consumers. Through the fusion cells we will deliver specific disruption strategies leveraging industry expertise and capabilities.

Diagram 3: Harnessing capability and capacity across the ecosystem

Emerging Trends & Response Working Group	Data Integration & Technology Working Group	Prevention & Communication Working Group	Fusion Cells
• Optimised processes for identifying emerging scams • More timely alerts about scams • Actionable Information to demographics targeted by scammers • Identifying opportunities for new data flows and collection methods	• Data outputs to focus and support the efforts of the other working groups • Taxonomy for scams common language • Enhanced data integration	• Coordinated and simplified protective messaging and calls to action • Scams awareness week • New products, some linked to the work of the fusion cell	• Early identification of scam campaigns and their enabling factors • Blocking identified enabling factors • Initiatives that stop consumers sending funds. • A sandbox for broader disruption strategies and techniques • Identify and report barriers to coordinated scam prevention and disruption

The **Emerging Trends and Response Working Group** brings together key partners to identify emerging scam trends and disruption approaches.

The **Data Integration and Technology Working Group** supports and informs our technology build to facilitate enhanced data sharing to support evidence-based anti-scam strategies.

The **Prevention and Communication Working Group** provides strategic input for effective communication, education and outreach for consumers and industry.

These three working groups have been established this quarter and we look forward to working closely on evidence-based, collaborative and integrated work.

The **Investment Scams Fusion Cell**, also established this quarter, is jointly led by ASIC and the National Anti-Scam Centre with representatives from banks, telcos, cryptocurrency firms and digital platforms. It is disrupting investment scams through early identification of scam campaigns; blocking enabling factors; and stopping consumers sending funds.

Key principles

The Advisory Board has endorsed governance principles for the National Anti-Scam Centre and our partners, most importantly:

- **To integrate, not duplicate:** Approaches will build on and integrate learnings and capabilities that already exist.
- **Consumers at the centre:** Our priority is protecting the community and designing solutions that work for people.
- **No wrong door:** Helping consumers find the answers and support they need wherever they report.

Performance

To assess performance, we will monitor and report on five benefits:

1. The National Anti-Scam Centre slows the acceleration of financial losses due to scams.
2. Greater collaboration between government and business improves scam disruption.
3. Near real-time data and timely trend reports improve understanding of the scam landscape.
4. Joined up systems improve support services for scam victims.
5. Increased scam awareness improves consumer ability to recognise, protect and report on scams.

In this quarter benefit measures have been agreed, and baselines and annual targets set.[2]

2 Refer Appendix B for Benefits, measures, baselines and Year 1 Targets.

National Anti-Scam Centre in action

Collaboration and engagement

The National Anti-Scam Centre has experienced strong engagement and willingness to collaborate. Many organisations have contacted us for advice on scam activities, to participate or provide information and ideas on how to combat scams. We have met with government, industry and consumer groups to build understanding of current anti-scam trends and initiatives; agree processes for data and intelligence sharing; and work together on ways to scale disruption initiatives in Australia and overseas.

Scams Awareness Week

This quarter the National Anti-Scam Centre and partners commenced planning for Scams Awareness Week to be held in November. The theme for the campaign is impersonation scams with the tag line Who's really there?

This theme was developed in consultation with stakeholders and informed by Scamwatch data which demonstrates:

- many scams include some form of impersonation
- both organisations and brands can be impersonated
- impersonation scams appear across a wide variety of channels.

Sharing resources

This quarter a National Anti-Scam Centre intelligence analyst joined the Joint Policing Cyber Crime Centre (JPC3). The JPC3 brings together domestic and international policing and intelligence agencies to combat cybercrime. This secondment is enhancing cooperation and information sharing between the National Anti-Scam Centre, Australian Federal Police (AFP) and other organisations participating in the JPC3.

We have also seconded staff from ASIC and the Reserve Bank of Australia to support the Investment Scam Fusion Cell.

Community engagement

We conducted nine outreach engagements to promote scams awareness, share key consumer protection messages, and gather valuable intelligence on scams impacting particular communities that may not be flagged in standard data analysis. Community engagement provides a unique opportunity to hear from people impacted by scams.

For example, at a community forum for older Australians, participants shared concerns about technology and fear of scams. Many avoid online shopping services and are overwhelmed with the number of scam text messages they receive. They shared that it would help to have more information about how to tell a real communication from a fake one and more assistance using technology safely. As a result, the Scamwatch website was updated to include information about impersonation scams and the Office of the eSafety Commissioner's *Be Connected* program that provides resources and services to support older Australians to build their digital confidence, has introduced scams prevention messages.

Industry engagement

National Anti-Scam Centre team members visited the scam and fraud centres of major banks to learn more about prevention and detection activities being undertaken and progress data sharing and collaboration opportunities. We look forward to similar discussions with other industry participants over the next quarter.

We have engaged with fintechs, telcos, digital platforms, banks and other financial institutions to discuss initiatives to support scam disruption and prevention. These initiatives include call and SMS blocking in the telco sector and working with fintechs to address the increasing prevalence of cryptocurrency and identity theft.

Disruption

Investment Scams Fusion Cell activities

The Fusion Cell meets fortnightly to tackle live investment scams drawn from Scamwatch and ASIC data. This has resulted in:

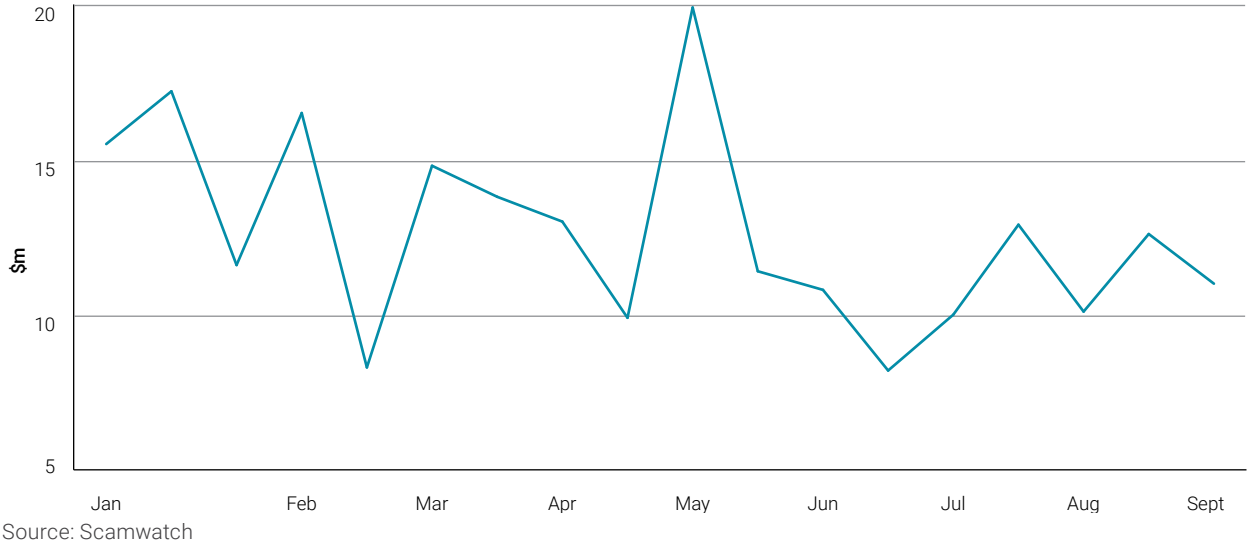
- flagging high-risk cryptocurrency payments
- better support for victims
- enhanced scam intelligence
- aversion of significant losses
- takedown of 32 websites.

Ongoing Fusion Cell initiatives include:

- strategies for identifying and taking down investment scam advertisements
- member protocol for investment scam website takedowns
- using call diversion technology to break scammer-to-victim contact, and provide scam warnings
- developing best practice guidance on using intelligence to disrupt investment scams.

The value of investment scams reported to Scamwatch in the quarter, was 6% lower than the same period of 2022. It is encouraging to see this downward movement. We will continue to monitor the data to see if this is a trend emerging through the work of the National Anti-Scam Centre.

Diagram 4: Reported Investment Scam Losses, January - September 2023



Source: Scamwatch

Other disruption activities

Where consent is provided, we share scam reports with the financial sector through the Australian Financial Crimes Exchange (AFCX), Meta (Facebook), and Gumtree. Each week lists of alleged scammer phone numbers are shared with the telco sector to inform call and SMS blocking activities.

Our work with a money remitter to implement new internal rules to detect scams targeting the elderly, resulted in $60,000 in payments being blocked.

To disrupt fake World Cup ticket sales, we provided several banks information about the accounts receiving ticket payments so they could be blocked and provided information to digital platforms resulting in posts being removed.

As many scams impacting Australians originate overseas, there is significant value in sharing intelligence and collaborating on disruption initiatives with international counterparts. In the quarter we shared relevant local intelligence with the Competition Bureau of Canada to assist their investigation of an international online shopping scam affecting Australians and Canadians.

Awareness

The National Anti-Scam Centre is committed to leading consistent messaging to help consumers identify and avoid scams. We are collaborating with partners to amplify messaging and provide better education resources to help consumers.

Chinese Authority Scam

This year there have been over 1,244 reports and $8.7 million in losses to a scam involving scammers posing as Chinese police targeting, intimidating, and stealing from young people studying in Australia. In August, the number of these reports doubled compared with previous months.

We responded with a media release that reached approximately 10 million people. It was run by national and regional television broadcasters, radio stations and newspaper mastheads. We shared the release with universities that have large international student communities. Interviews were conducted with the ABC and SBS World News (including Mandarin channels), newspapers and radio broadcasts.

> This type of scam is highly sophisticated and convincing because it involves multiple perpetrators who play on their victim's fears by threatening them and their family with years of jail time.
>
> In one case, a young man paid over $400,000 to scammers after he was told he would be arrested. He was also told he was under surveillance and was instructed to have Facetime open 24 hours a day.
>
> Catriona Lowe, Radio interview, August 2023

We provided an intelligence brief with scam intelligence from victims of Chinese Authority scams to the AFP via the JPC3. Information was shared with Interpol to be considered by a relevant transnational police operation.

Qantas Points scams

The National Anti-Scam Centre identified the largest phishing campaign to target a 'loyalty points' scheme in Australia. We received more than 200 reports of text messages complaining of phishing websites impersonating the Qantas brand. Consumers that clicked the link in the text message and provided their frequent flyer login details on the lookalike page had their accounts compromised and their frequent flyer points cashed out by scammers. We issued a media release, social media warning, and contacted Qantas requesting support to takedown the website.

Media

Media interest in new and emerging scams remained strong in the quarter. We responded to 93 media queries ranging from celebrity endorsement investment scams on social media to football ticketing and online shopping scams.

There were five media releases generating solid coverage, with scam alerts about loyalty points scams and World Cup tickets widely picked up by mainstream media across print, online, television and radio.

The Chinese Authority scam media release included coverage in both English and Mandarin via SBS and the ABC.

A highlight of this quarter was an interview with ABC's Behind the News – High School to talk about scams impacting students under 18.

Support

We are working closely with support services to help people affected by scams get the support they need to recover.

Victim support

The National Anti-Scam Centre implemented a new consumer referral process that refers people who report to Scamwatch and need support to IDCARE, an identity and cyber support service. This has resulted in:

- more timely referrals
- eliminating the need for scam victims to report twice
- increasing tailored support for scam victims.

Industry guidance

Fake online stores are the most common type of online shopping scam. To address this, we published guidance for business on how to use intellectual property rights to have fake websites removed if their website or brand is used for imposter scams.

Technology

We are building data sharing technology over the next three years to:

- receive a scam report from key institutions and centralise this intelligence
- distribute data to those who need it most – such as banks to freeze an account, telcos to block a call, and digital platforms to take down a website or account
- analyse and act on trends sourced from this data to disrupt scams and educate consumers.

Data sharing

Building on our emerging partnerships we have:

- an API on track to be up and running with Australian Signals Directorate's national policing initiative, ReportCyber to enable data sharing with law enforcement
- hosted data sharing workshops and meetings with the AFCX and major banks
- worked closely with ASIC to facilitate sharing of investment scam data.

Scamwatch website upgrade

Our technology and user-experience experts have made the Scamwatch reporting form simpler to use. Initial improvements are scheduled for delivery in mid-October.

Government partner initiatives

Law enforcement

Law enforcement plays a critical role in Australia's fight against scams. This quarter we worked actively with law enforcement partners through the Advisory Board and Investment Scams Fusion Cell.

Advisory Board members

- Australian Federal Police

Investment Scam Fusion Cell members

- Australian Federal Police
- New South Wales Police
- Northern Territory Police
- Queensland Police
- Victoria Police
- Joint Policing Cyber Crime Coordination Centre

The National Anti-Scam Centre joined the Commonwealth Strategic Cybercrime Officials Network, run by the Attorney-General's Department. Members discuss cybercrime work across the Commonwealth, including national plans and strategies.

On uncovering scammers posing as government agencies to extort the families of Chinese international students, we prepared and shared an intelligence brief with the AFP via the JPC3. This information was shared with Interpol to be considered by a relevant transnational police operation.

We provided information to South Australia Police in relation to a fake charity scam.

We share scam data with the US Federal Trade Commission's Consumer Sentinel Network which is available to enforcement agencies overseas.

Australian Communications and Media Authority

The ACMA is working to disrupt scams before they reach Australians, including supporting new disruption initiatives and enforcing anti-scam rules. Key initiatives are highlighted below.

Establishing a 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 by scammers. It will complement existing protections and make SMS with alphanumeric message headers trustworthy for consumers.

Enforcing rules: The ACMA has adopted a compliance priority to combat SMS scams due to evidence their prevalence and impact is increasing.

The ACMA has been auditing the compliance of SMS aggregators (telcos that send bulk SMS) as a potential conduit of SMS scams onto Australian networks. The ACMA has directed multiple telcos to comply with the Reducing Scam Calls and Scam SMS rules. Once a telco is directed to comply, it enlivens stronger enforcement action if future breaches are found, including civil penalties.

Engaging with industry: ACMA is engaging with telcos on a range of scam disruption initiatives, including:

- Providing de-identified complaint data to facilitate identification and blocking of scams.
- Monitoring and supporting telco efforts to trace the origins of scam traffic and telco capability uplift, including the introduction by key telcos of artificial intelligence (AI) or machine learning to automate and enhance the identification and disruption of scams.
- Sharing information and intelligence about current and emerging scam threats, including via regular intelligence reports and the ACMA's Scam Telco Action Taskforce, which last met in September.
- Assisting well-known brands and government agencies to engage with telcos to protect their numbers and SMS Sender IDs from impersonation.

Awareness raising: The ACMA has continued to disseminate a comprehensive suite of consumer education material informing consumers how to identify and protect themselves from phone scams, including material in Simplified Chinese, Traditional Chinese, Arabic, Vietnamese and Italian, and for First Nations Australians. The ACMA has also issued consumer scam alerts where there is a significant and/or emerging risk of harm.

Australian Securities and Investments Commission

ASIC has been allocated government funding to identify and take down investment scam and phishing websites. On 30 June 2023, ASIC entered into a contract with Netcraft, a private company specialising in cybercrime disruption, to take down investment scam and phishing websites that ASIC reports to them, and proactively identify and report to ASIC investment scam and phishing websites for takedown. Netcraft's takedown process involves removing, or limiting access to, fraudulent and malicious websites on the internet. It achieves this by collaborating with relevant parties, such as the organisation hosting the site, to request the site be taken down. ASIC is focusing on websites where unauthorised, fake or impostor entities offer financial services or investment scams to Australians.

Since July 2023, ASIC has disrupted scam activity by initiating takedowns of more than 2,500 investment scam and phishing websites. Those figures include:

- 2,100 sites that have been taken down
- over 400 sites in the process of being taken down.[3]

Websites taken down have included fake investment platform websites, crypto-asset investment scam websites, impersonation and phishing scams, fake news article and celebrity endorsement websites, fake cryptocurrency and investment comparison websites, fake credit product and fake bank scams.

3 ASIC's new website takedown capability knocks out over 2,500 investment scam and phishing websites, Media Release, 2 November 2023.

Looking forward – the next quarter

Scams Awareness Week

Scams Awareness Week will be held from 27 November – 1 December 2023. The theme for this year's campaign is impersonation scams with the tag line 'Who's really there?'.

We will be inviting campaign partners to make a pledge to remove hyperlinks in text messages by 30 June 2024. Several banks have already announced they will stop using links in unexpected texts to customers to reduce the impact of scams and fraud.

Industry Roundtable

An industry roundtable will be held in December with participants who are not currently involved in other National Anti-Scam Centre forums. As well as sharing our vision and remit, we will seek input on priorities and discuss scam-related issues.

National Anti-Scam Centre brand strategy

We will develop a brand strategy to position the National Anti-Scam Centre and Scamwatch within the anti-scam ecosystem. The strategy will support website content, communication channels and education campaigns to ensure our role is well recognised and understood.

Focus on communities

Research and consultation with key advocates and peak bodies will inform effective communications with First Nations, people with disability and small business audiences on scams awareness and protection. We will also develop an "Easy Read version" of the Little Black Book of Scams.

Technology and data sharing

The Report-A-Scam online form is being upgraded to improve the data quality received and to expand on the types of data collected. The expanded scope and improved quality of data will enable more timely and effective data sharing to aid scam disruption activities.

A beta release of enhanced scam statistics will be launched on the Scamwatch website. This will give public users and the media greater flexibility in accessing and analysing scam data, to improve scams education and awareness.

Work will continue with government and industry to establish automated scam data sharing arrangements and move toward a common view of scam activity.

Global engagement

Scams and scammers transcend national borders. We are engaged with our global counterparts to stay abreast of emerging trends, share best-practice anti-scam initiatives and work in partnership to tackle scams impacting Australians.

In October, the National Anti-Scam Centre will be presenting at the Global Anti-Scam Summit (GASS). GASS brings together governments, consumer and financial authorities, law enforcement, brand protection agencies, and cybersecurity companies to share knowledge and define joint actions to protect consumers from scams.

We will be participating in the International Fraud Council led by the UK Home Office. This Council brings together international counterparts to share information and coordinate global anti-scam initiatives.

Scamwatch statistics 2023[4]

Year to date

January to September

$398.7 million has been reported lost by Australians to scams between January and September 2023. This is an increase of 9.2% compared to the same period last year.

234,672 reports have been made to Scamwatch, up 41.2% compared to the same period last year.

- 10.2% of reports include a financial loss, with an average loss of $16,485.
- Financial loss via bank transfer has increased 15.2% to $175.2 million.
- Financial loss via cryptocurrency has increased 31.8% to $148.2 million.
- Losses to social media scams have increased 31.5% to $78.6 million.
- The most common contact methods are text message (36.0%) and email (28.2%).
- Phone is the highest loss contact method at $92.5m (23.2% of losses), followed by social media scams at $78.6m (19.7% of losses).

At $241.6 million, investment scams cause the most financial harm to consumers in Australia comprising 60.6% of reported losses. However, the growth is slowing, up just 4.1% compared to the same period in 2022. We will continue to monitor investment scam data to see if this is a trend emerging through the work of the National Anti-Scam Centre, and the Investment Scam Fusion Cell.

Losses to **Jobs & Employment** scams are the most significant 2023 development in overall scam losses and trends. Losses have reached $20.3 million, up 633.5% since last year. Victims usually accept a job via a social media or messaging app that allows them to work from home but requires them to make cryptocurrency payments or deposits which result in significant losses.

4 This data is sourced from Scamwatch only. The ACCC Targeting Scams report provides an annual aggregation of scam data from Scamwatch, ReportCyber, AFCX (6 financial institutions), ATO, ASIC, ACMA, IDCARE and Services Australia. The National Anti-Scam Centre is working closely with our partners so that we can soon provide this aggregated data more frequently.

Demographics – the people reporting scams

Age

Number of Scamwatch reports and losses by age group (January to September 2023)

Age Group	2023 reports	2023 losses	change on 2022 reports	change on 2022 losses
Under 18	1,492	$0.3m	34%	53%
18-24	9,469	$14.0m	29%	37%
25-34	23,198	$38.4m	20%	-10%
35-44	29,383	$58.1m	28%	-12%
45-54	29,864	$67.8m	31%	12%
55-64	34,077	$85.0m	53%	14%
65 and over	55,622	$101.6m	66%	16%
N/A	51,567	$32.8m	40%	-61%

Indigenous Australians

Number of Scamwatch reports and losses (January to September 2023)

Identifies as Indigenous	number of reports	losses
Yes	4,460	$3.4m
No	230,624	$395.3m

Top scams reported by Indigenous Australians (January to September 2023)

Scam type	losses
Investment scams	$1.1m
Identity theft	$757,349
Jobs & employment scams	$348,122
Online shopping scams	$231,583
Romance scams	$214,327

Indigenous Australians were over-represented in financial losses for identity theft and online shopping.

English as a second language

People with English as a second language made 4.8% of scam reports and accounted for 13.3% of losses to scams.

Top scams reported by people with English as a second language (January to September 2023)

Scam type	losses
Investment scams	$35.3m
Threats to life arrest or other	$4.5m
Jobs & employment scams	$3.5m
Romance scams	$2.1m
Identity theft	$1.3m

People with English as a second language were over-represented in financial losses for psychic scams and threat-based scams.

People with disability

People with disability made 7.3% of scam reports, and accounted for 6.3% of losses to scams.

Scams reported by people with disability (January to September 2023)

Scam type	losses
Investment scams	$13.6m
Phishing	$3.1m
Romance scams	$2.8m
Rebate scams	$832,885
Remote access scams	$745,498

People with disability were over-represented in health and medical scams.

The quarter

July to September

- **$111.4 million** in losses in the quarter. This is a decrease of 16% compared to the same quarter in 2022.
- The quarter saw a decrease in losses across most scam types compared with the previous quarter.
- At $29.8 million, losses in September were the lowest reported in a single month since October 2021.
- At $69.4 million, investment scams accounted for over 60% of total scam losses in the quarter.

Top 10 losses by scam type (July to September 2023 and July to September 2022)

Scam type	2023 losses	2022 losses
Investment	$69.4m	$74.1m
Romance	$9.1m	$12.6m
False billing	$6.5m	$5.2m
Phishing	$4.7m	$9.2m
Jobs & employment	$4.6m	$1.5m
Threats to life	$2.8m	$7.4m
Remote access	$2.8m	$4.3m
Inheritance & unexpected money	$2.4m	$3.4m
Classified	$2.0m	$2.6m
Rebate	$2.0m	$0.5m

Appendices

Appendix A – National Anti-Scam Centre partnerships

Advisory Board

- Australian Banking Association, Anna Bligh, CEO
- Australian Communications Consumer Action Network, Andrew Williams, CEO
- Australian Federal Police, Scott Lee, Assistant Commissioner,
- Australian Payments Network, Andy White, CEO
- Blockchain Australia, Simon Callaghan, CEO
- CHOICE representing Consumers' Federation of Australia, Rosie Thomas, Director of Campaigns and Communications
- Communications Alliance, John Stanton, CEO
- Consumer Action Law Centre, Stephanie Tonkin, CEO
- Customer Owned Banking Association, Michael Lawrence, CEO
- Digital Industry Group Inc. (DIGI), Sunita Bose, Managing Director
- Financial Counselling Australia, Peter Gartlan, National Coordinator
- IDCARE, David Lacey, Managing Director

Regulator Steering group

- Australian Communications and Media Authority, Nerida O'Loughlin, Chair
- Australian Competition and Consumer Commission, Catriona Lowe, Deputy Chair
- Australian Securities & Investment Commission, Sarah Court, Deputy Chair

Operational Coordination group

- Australian Competition and Consumer Commission
- Australian Communications and Media Authority
- Attorney-General's Department
- Australian Securities & Investment Commission
- Australian Taxation Office
- Australian Transaction Reports and Analysis Centre
- Department of Home Affairs
- Services Australia

Working groups

Data Integration & Technology

- Australian Communications and Media Authority
- Australian Cyber Security Centre
- Australian Financial Crimes Exchange
- ANZ Bank
- Australian Securities & Investments Commission
- Commonwealth Bank of Australia
- Customer Owned Banking Association
- CoinSpot
- DIGI
- IDCARE
- Meta
- NAB
- Optus
- Telstra
- TPG Telecom
- TRM Labs
- Westpac

Consultative members

- Australian Financial Complaints Authority
- Australian Federal Police /Joint Policing Cybercrime Coordination Centre
- Amazon
- Blockchain Australia
- Commonwealth Fraud Prevention Centre
- Cybercrime Joint Management Group
- Department of Home Affairs
- Western Union

Emerging Trends and Response Working Group

- Apple
- ANZ Bank
- Australian Banking Association
- Australian Communications and Media Authority
- Australian Cyber Security Centre
- Australian Federal Police
- Australian Financial Complaints Authority
- Australian Financial Crimes Exchange
- Australian Payments Network
- Australian Payments Plus
- Australian Prudential Regulation Authority
- Australian Securities & Investments Commission
- Australian Small Business and Family Enterprise Ombudsman
- Australian Taxation Office
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Bank of Queensland
- Bendigo and Adelaide Bank
- Blockchain Australia
- Chainalysis
- CHOICE
- Colonial First State
- Commonwealth Bank of Australia
- Consumer Action Law Centre
- Customer Owned Banking Association
- Department of Health and Aged Care
- eSafety Commissioner
- Equifax
- Financial Rights Legal Centre
- Financial Services Council
- Google
- Gumtree
- HSBC
- IDCARE
- Link Group
- Macquarie
- Mercer

- MoneyGram
- National Australia Bank
- New Payments Platform Australia
- PayPal
- Reserve Bank of Australia
- Seek
- Services Australia
- Tabcorp
- Telstra
- Treasury
- Western Union
- Westpac

Prevention and Communication Working Group

- ANZ bank
- Australian Communications and Media Authority
- Australian Communications Consumer Action Network
- Australian Federal Police
- Australian Taxation Office
- Behavioural Economics Team of Australia
- Customer Owned Banking Association
- Commonwealth Bank
- Consumer Action Law Centre
- Council on the Aging
- eSafety Commissioner
- Financial Counselling Australia
- Google
- Department of Home Affairs
- IDCARE
- Indigenous Consumer Assistance Network
- Meta
- National Australia Bank
- Optus
- Telstra
- Westpac Bank

Consultative members

- Adult Multicultural Education Services Australia
- Australian Small Business and Family Enterprise Ombudsman
- CHOICE
- Consumer Education Network
- Crimestoppers
- Interactive Advertising Bureau
- People With Disability Australia
- Pivotelindust
- Super Consumers Australia
- TPG
- WestJustice

Fusion Cell members

- AMP
- ANZ
- Apple
- Australian Transaction Reports and Analysis Centre
- Australian Federal Police
- Australian Financial Crimes Exchange
- Australian Payments Network
- Australian Taxation Office
- Bendigo and Adelaide Bank
- BTC Markets
- CoinJar Australia
- CoinSpot
- Commonwealth Bank
- Crypto.com
- Google
- HSBC Bank Australia
- HUB24 Limited
- Independent Reserve
- ING Banking Australia Limited
- Insignia Financial
- Macquarie
- Mastercard
- Meta
- Microsoft

- NAB
- NSW Police
- NT Police
- Optus
- Queensland Police
- Sapol
- Symbio
- Telstra
- TPG Telecom
- Vanguard Investments Australia
- Victoria Police
- WA ScamNet
- Westpac

Appendix B – Program benefits register

Benefit name		Benefit measure		Baseline FY22/23	Target FY23/24
B1	National Anti-Scam Centre slows the acceleration of financial loss due to scams	1i	Slower growth in financial losses to scams	17% growth on previous year	12% growth on previous year
		1ii	Fusion cell activities reduce financial losses to investment scams	329,768,693	320,000,000
B2	Greater collaboration between government and industry improves scam disruption	2i	Increase in the number of scammer identifiers shared across government and industry	277,594	700,000
		2ii	Collaboration improves scam intelligence, disruption and awareness	NA	Case Study - Emerging Trends & Response Working Group
		2iii	Increase in number of investment scam contacts prevented	0	500
		2iv	Increase in number of ASIC website takedowns completed	0	200
		2v	Fusion cells improve scam disruption	NA	Case Study - Investment Scams Fusion Cell
B3	Near real time data and timely trend reports improve understanding of the scam landscape	3i	Faster data cleaning of Scamwatch data alllows for accurate trend analysis in a more timely manner	NA	NA
		3ii	Faster turnaround for dissemination of Scamwatch data to external parties via imporvied ad-hoc reporting functionality	NA	NA
		3iii	Increase in automated data sharing arrangements to provision near real-time data to external stakeholders	6	10
		3iv	Increase in automated data sharing arrangements to consume near real-time data from external stakeholders	0	5
B4	Joined up systems improve support services for scam victims	4i	Better support for consumers who lose money to scammers	NA	Case Study - Victim support
B5	Increased scam awareness improves consumers ability to recognise, protect, and report on scams	5i	Increase in alignment of NASC messaging across Prevention & Communication Working Group members	NA	Establish baseline via working group survey
		5ii	Increase in average views per media-release	6,000,000	9,000,000
		5iii	Reduction in webform abandonment	54%	50% decrease on baseline
		5iv	Increase in the number of scam reports	450,000	10% growth on baseline


Australian Government


National
Anti-Scam
Centre