BDO

IDEAS | PEOPLE | TRUST

Forensic Services

Australian Scam Culture Report

December 2024 quarter

Introduction

In our latest edition of the Australian Scam Culture Report for the December 2024 quarter, we delve into the most recent scam trends and developments, highlighting the evolving landscape of current activities and the measures being taken to combat them. This report provides a comprehensive analysis of the current scam environment, offering valuable insights into the tactics employed by scammers and the sectors most affected.

The total dollars lost by Australians to scams in this quarter increased by an estimated $7.9 million to just over $94.4 million. Interestingly, the number of reported scams fell to 51,322 from 55,020 in the September 2024 quarter. This paradox of fewer reports but higher financial losses underscores the increasing sophistication and impact of scams.

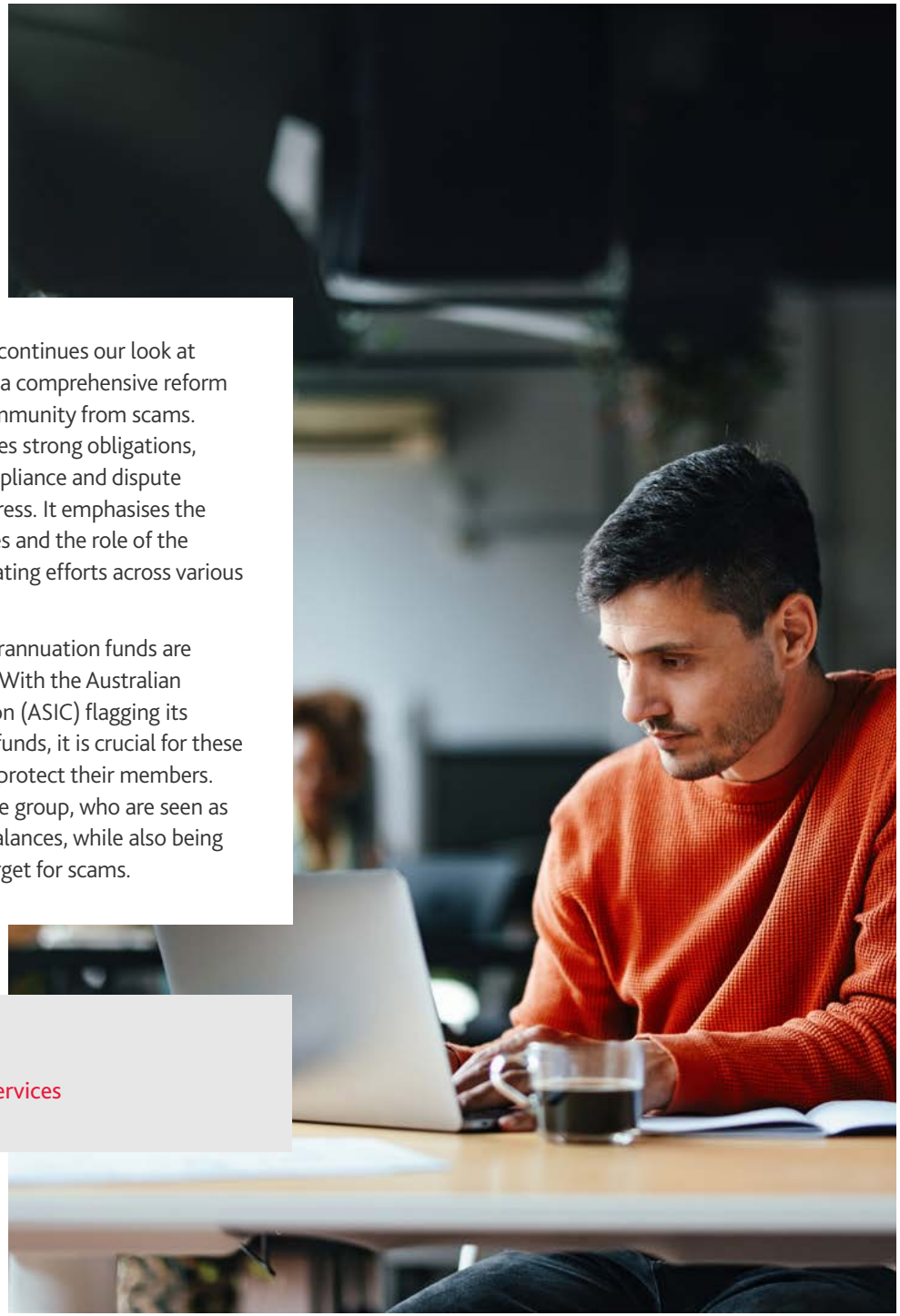
One of the most alarming trends observed this quarter is the rise in investment scams, which has become the leading category for reported financial losses. Scammers are employing more complex and convincing methods to deceive individuals into fraudulent investment schemes, often promising high returns with minimal risk. This trend highlights the need for enhanced public awareness and education on recognising and avoiding such scams.

In addition to these trends, the report continues our look at the Scams Prevention Framework Bill, a comprehensive reform aimed at protecting the Australian community from scams. The recently passed framework enforces strong obligations, including tough penalties for non-compliance and dispute resolution pathways for consumer redress. It emphasises the importance of sector-specific initiatives and the role of the National Anti-Scam Centre in coordinating efforts across various sectors to combat scams.

We've also seen this quarter that superannuation funds are becoming a new target for scammers. With the Australian Securities and Investments Commission (ASIC) flagging its interest in the scam risks facing super funds, it is crucial for these funds to adopt proactive measures to protect their members. Scammers often target the over-65 age group, who are seen as likely to have access to higher super balances, while also being less tech savvy, making them a rich target for scams.

Remember: Stop – Think – Act.

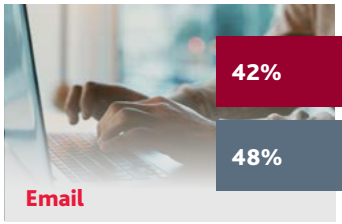
Stan Gallo
Partner, Forensic Services



Top contact methods (two-quarter comparison)

Text message

20%	September 2024 quarter
17%	December 2024 quarter



Email

42%	September 2024 quarter
48%	December 2024 quarter

Phone calls

21%	September 2024 quarter
15%	December 2024 quarter

Throughout the final two quarters of 2024, emails have consistently served as the primary channel for reported scam delivery, continuing to rise as per the trend we have seen in previous reports.

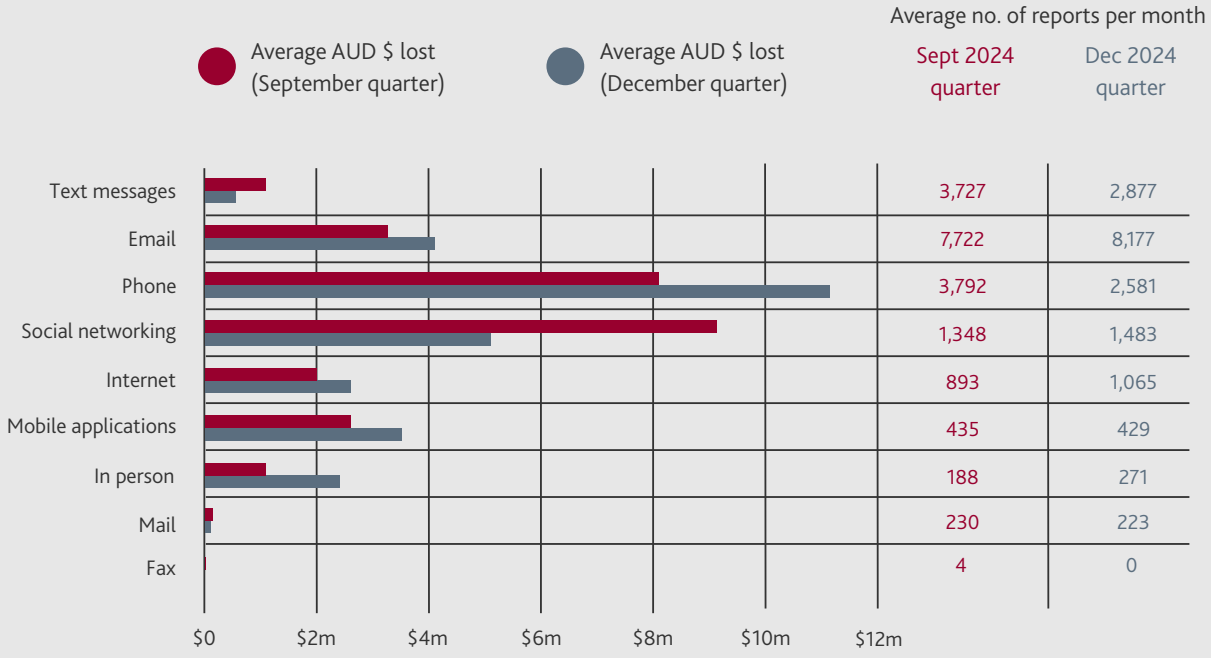
AUD$ lost by delivery method (two-quarter comparison)

Although the number of reports decreased by seven per cent in the December quarter, the amount of money reported as lost increased by an estimated $7.9 million. As noted in the previous quarter, while it's encouraging to see an increase in consumer awareness, the amount lost to scams has again risen this quarter by nine per cent.

During the December 2024 quarter, text messaging scams continued to decrease in reports. The trend identified last quarter persisted, with the average number of individuals reporting text message scams decreasing by 850. The average number of reported scams per month for this contact method was 2,877, a decrease from the September 2024 quarter, where the average number of reported scams per month was 3,727.

The number of reported scams delivered via email continued to rise this quarter. In the December 2024 quarter, there was an average of 8,177 reports per month, compared to 7,722 reports per month in the September 2024 quarter.

While phone calls only amounted to 15 per cent of the reported monthly scam methods, phone scams resulted in the highest average dollar amount lost per month, accounting for 37 per cent of the total dollars lost throughout the December 2024 quarter. The average number of reports per month was 2,581, down from 3,792 in the September 2024 quarter, but the average loss per month increased significantly to $11,759,354 from $8,132,909.



Source: 2024, All scam types stats – Scamwatch, Australian Competition and Consumer Commission, ©Commonwealth of Australia

AUD$ lost by scam type (December quarter totals)

For the December 2024 quarter, scam types that fall under 'investment scams' were the leading category for reported total dollars lost, with over $57.6 million lost to this category. Scams that fall under this category include general investment scams and betting and sports investment scams.

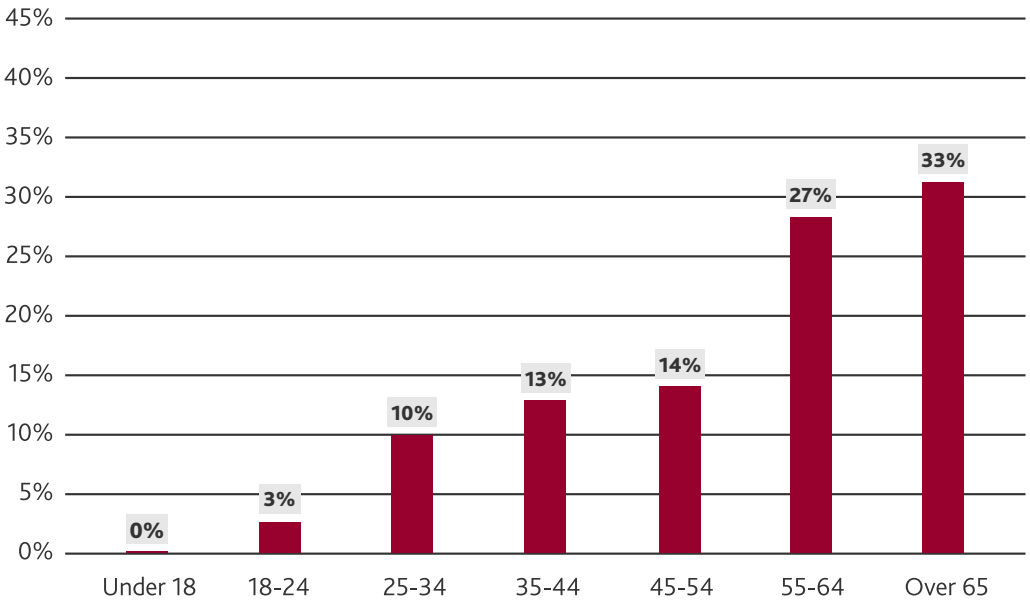
The next leading category for reported dollars lost was 'attempts to gain an individual's personal information' scams, with over $11.8 million lost to this category. Scams in this category include hacking, identity theft, phishing, and remote access scams.

Reported losses from fake charities rose by $52,967, reaching a total of $63,074, likely due to increased holiday season generosity, which scammers often exploit. Reported losses from unexpected winnings scams more than doubled, reaching $555,411, possibly due to the surge in online shopping and promotions around December, making people more susceptible to fraudulent offers.

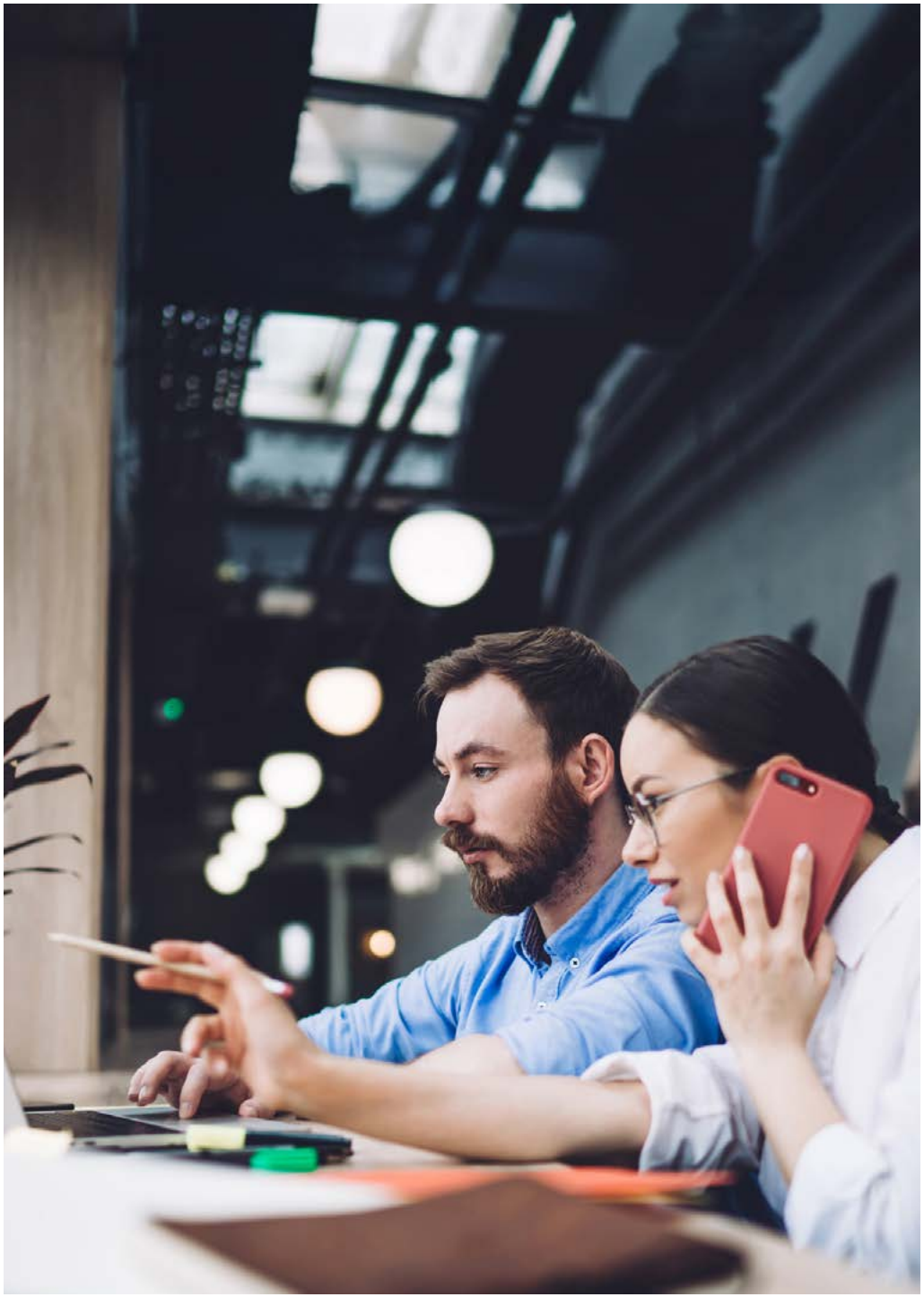
Scam category	Amount lost
Investment scams (includes betting and sports investment scams, investment scams)	**$57,643,168.50**
Attempts to gain your personal information (includes hacking, identity theft, phishing, remote access scams)	**$11,824,546.29**
Buying or selling (includes classified scams, false billing, health and medical products, mobile premium services, online shopping scams, overpayment scams, psychic and clairvoyant)	**$7,294,570.51**
Dating and romance	**$4,855,033.50**
Jobs and employment (includes jobs and employment scams, pyramid schemes)	**$4,048,288.48**
Threats and extortion (includes ransomware and malware, threats to life, arrest and other)	**$4,046,249.87**
Unexpected money (includes inheritance and unexpected money, rebate scams)	**$3,326,354.96**
Other	**$743,865.23**
Unexpected winnings (includes travel, prizes and lottery scams)	**$555,411.84**
Fake charities	**$63,074.57**

Age groups targeted in scams (December quarter)

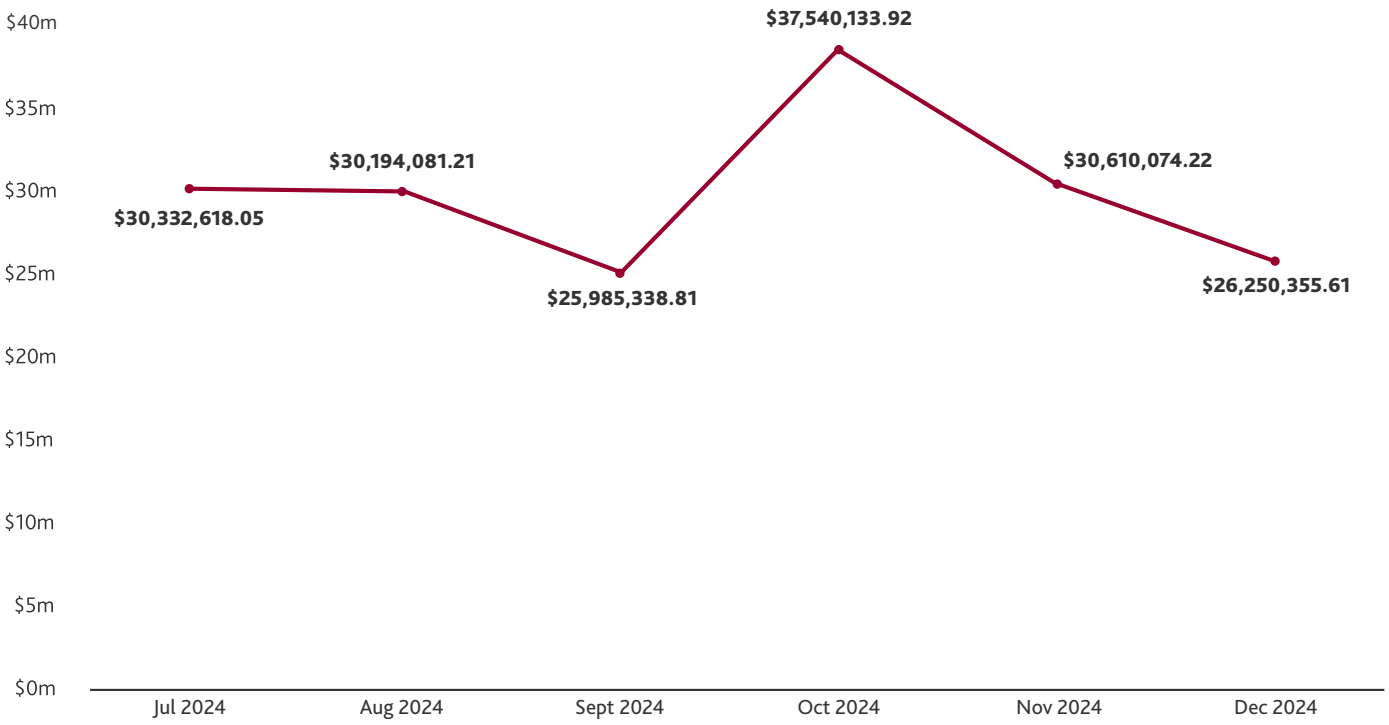
The 55-64 age group experienced a reversal of the 12 per cent decrease from the previous quarter which notably includes the festive season. The over 65 age group showed a decrease of eight per cent which could be an indicator of greater awareness combined with ongoing targeted enhancements in scam detection.



Source: 2024, All scam types stats – Scamwatch, Australian Competition and Consumer Commission, ©Commonwealth of Australia



Exposure level of different scam types (two-quarter comparison)



Source: 2024, All scam types stats – Scamwatch, Australian Competition and Consumer Commission, ©Commonwealth of Australia

Total funds lost throughout the quarter increased sharply in October to $37,540,133.92 before falling back to September like levels of $26,250,355.61 in December. There was an overall increase in total funds lost through the period of $7.9 million over the previous quarter.

This quarter did see a very sharp rise in October with a subsequent fall rather than more moderate changes noted in previous quarters. The substantial increase in October could coincide with an increase of pre 'holiday season' online activity buildup including arranging travel plans, shopping for gifts, and contributing to charities, all of which are common targets for scammers.

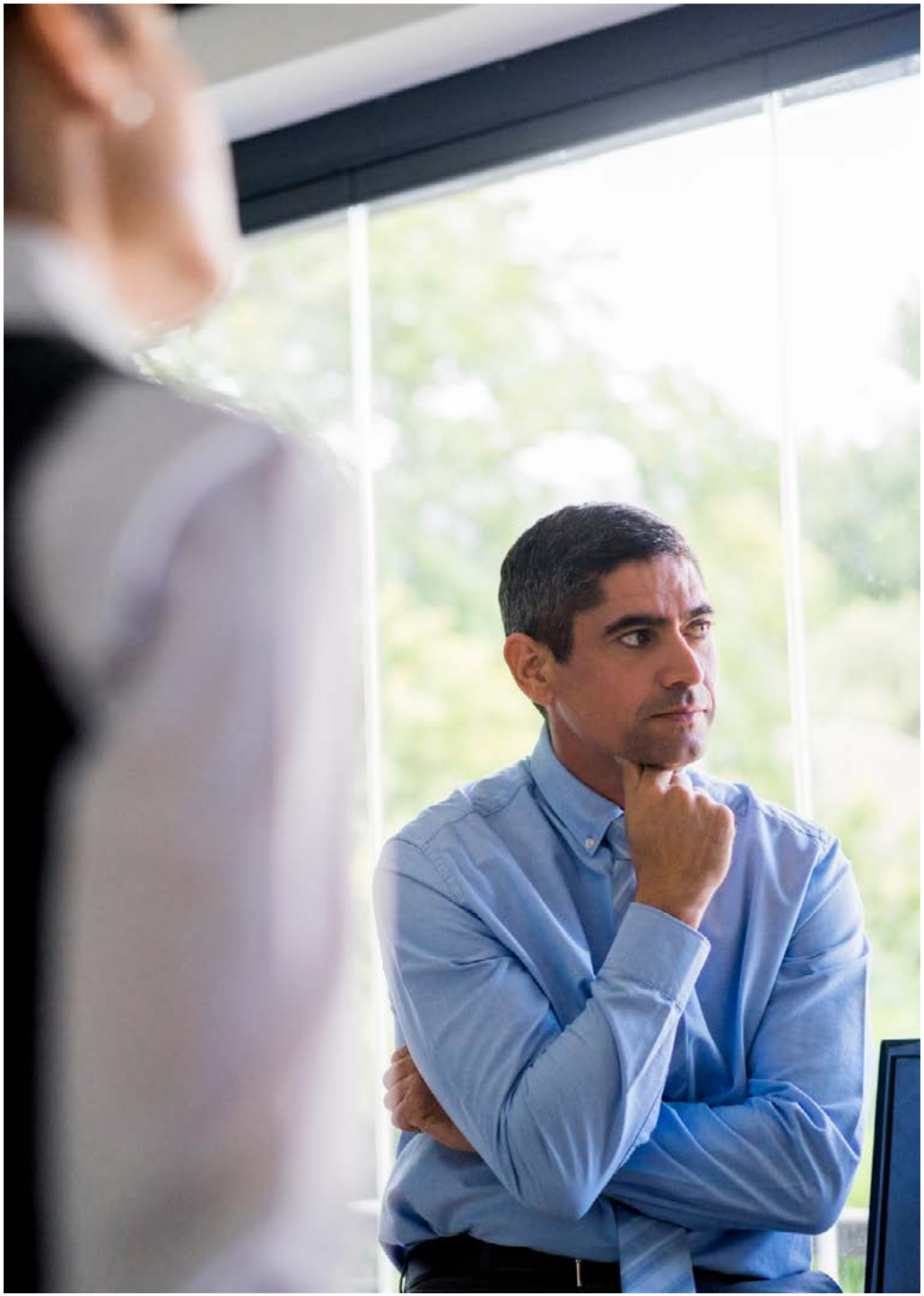
Super scams

With banks and social media companies continuing to face intense scrutiny over their handling of scams, superannuation funds could soon encounter similar challenges. The Australian Securities and Investments Commission (ASIC) has flagged its interest in the scam risks facing super funds with an open letter regarding the need to proactively address these risks. A recent ASIC review of 15 superannuation trustees found none had an organisation-wide strategy to address scams. Given that investment scams are a priority focus area for ASIC, super funds are likely to be subject to regulatory scrutiny sooner rather than later.

How do scammers target super funds?

Greater access to retirement savings on reaching retirement age, coupled with higher balances for the over-65 age group make an attractive target for scammers. According to the Australian Financial Complaints Authority, superannuation fund related scam complaints averaged $89,000 in losses per victim for the 2023 financial year, with the highest individual scam loss reaching $344,000.

Scammers use a combination of techniques, including 'investment advice', building trust over time, planting doubt about future financial security and a sense of urgency to act to attack super funds. Many super funds outsource operational activities such as IT systems, security, payments processing, and investment strategy, leading to third-party risk issues. These areas are exploited through attacks like business email compromise and false websites. Super funds cannot outsource responsibility and need to ensure that their third-party due diligence and risk profiles are acceptable and meet compliance requirements.



What can super fund companies do to get ahead of this?

Educate and inform:

Super funds should provide their members with case studies about the techniques and different ways scammers may attempt to gain access to their funds.

Stay updated on emerging scam techniques:

With the ongoing proliferation of AI and constantly changing scam techniques, it is crucial for super funds to stay updated to protect their members and their organisation.

Outsourced administrators and providers:

Super funds must ensure that their external administrators have effective anti-scam strategies and a detailed understanding of prevention, detection, and response measures.

Don't be complacent:

Past activity is not an indicator of the future. Super funds should not rely on current relatively low levels of reported scams as an indicator of safety.

Be proactive:

Conduct evaluations of anti-scam measures, including those of external service providers, and ensure that scam prevention, detection, and response receive the same attention as other financial crime risks.

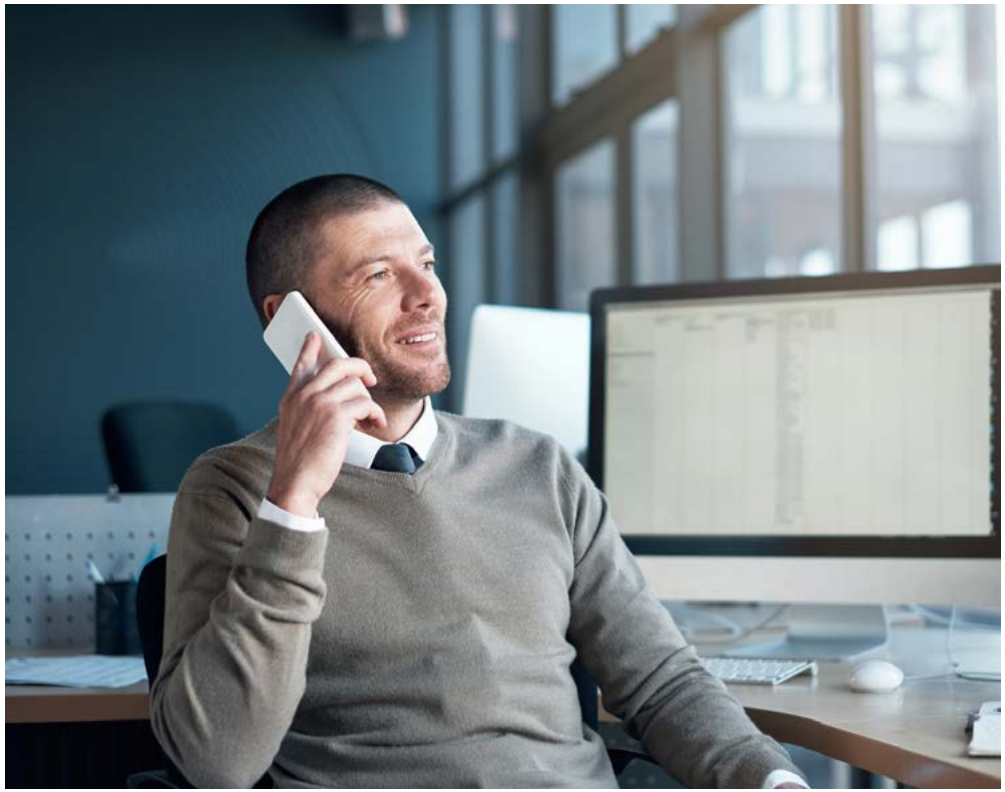
What can consumers do?

Report scams:

If you think you have been scammed, report it to the Australian Cyber Security Centre and Scamwatch. Your report helps disrupt scams, monitor trends, and warn others about new and emerging scams.

Seek support:

IDCARE provides support for individuals and organisations to reduce the harm from identity information compromise. Services like Lifeline (13 11 14) and Beyond Blue (1300 22 4636) offer crisis support for those experiencing significant mental health impacts from scams.



Scams Prevention Framework Bill

On 13th February the Scams Prevention Framework Bill 2025 passed both Houses of Parliament and came into effect on 21 February following royal assent.

The Scams Prevention Framework Bill is a comprehensive reform aimed at protecting the Australian community from scams. It adopts a whole-of-ecosystem approach to close gaps that scammers exploit. The framework enforces strong obligations, including tough penalties for non-compliance and dispute resolution pathways for consumer redress.

The framework highlights the importance of sector-specific initiatives, such as those by banks and telecommunications entities, to bolster scam defences. It also emphasises the role of the National Anti-Scam Centre in coordinating efforts across various sectors to combat scams. There is a significant focus on the need for consumer protection and avenues of redress when scams do occur. Additionally, the framework discusses the regulatory and compliance obligations for different sectors, including banks, telecommunications, and digital platforms, under the proposed framework. There is the potential for significant additional compliance requirements should the framework be enacted in its entirety.

The passing of Australia's new Scams Prevention Framework is a positive step forward. However, there are concerns about oversimplifying the issue based on misleading statistics. It has been highlighted that differences in scam definitions can significantly impact the reported statistical outcomes, potentially skewing the true picture of the problem. The key to success will be genuine collaboration and effective intelligence sharing across sectors, with support for entities struggling with the resources to implement necessary compliance reforms.

Five key takeaways

1. **Decline in scam losses:**

   The document notes a decline in scam losses in Australia, attributed to coordinated efforts by various sectors and the National Anti-Scam Centre.

2. **Sector-specific codes:**

   The importance of developing sector-specific codes to address the unique challenges and responsibilities of different sectors in preventing scams is highlighted.

3. **Consumer redress mechanisms:**

   The document emphasises the need for effective consumer redress mechanisms, including internal dispute resolution and external dispute resolution through the Australian Financial Complaints Authority (AFCA).

4. **Regulatory coordination:**

   The need for coordination between different regulators, such as the ACCC and ACMA, to ensure a cohesive approach to scam prevention is discussed.

5. **Industry accountability:**

   The importance of holding industries accountable for their role in preventing scams and protecting consumers.

Suggestions to improve the proposed legislation

1. **Clarification of obligations:**

   There were recommendations to clarify the obligations of different sectors under the framework to avoid conflicting and uncertain obligations.

2. **Information sharing:**

   Suggestions were made to refine the information-sharing requirements to ensure that actionable intelligence is targeted, practical, and effective in combating scams.

3. **Harmonisation with other laws:**

   Recommendations were made to ensure harmony with other obligations, such as anti-money-laundering laws and the Spam Act, to avoid impeding collective scam-prevention efforts.

4. **Consumer redress:**

   There were calls for a clear and effective consumer redress mechanism, including the need for a primary entity responsible for compensating victims to avoid the burden on consumers to chase multiple businesses.

5. **Penalties for non-compliance:**

   Recommendations included imposing penalties for senior officers who make false or reckless statements regarding compliance with their companies' obligations.

What to do if you've been scammed

1 If you think you have been scammed, **make a report to Scamwatch.** Your report helps to disrupt scams, monitor trends, and warn others about new and emerging scams.

2 You could also **make a report to ReportCyber,** a cybercrime reporting platform hosted by the Australian Cyber Security Centre of the Australian Signals Directorate. This platform was developed as a national policing initiative.

3 **IDCARE** provide support for individuals and organisations to reduce the harm they may experience from the compromise and misuse of identity information. This registered charity can provide advice and support on how to respond to data breaches, scams, identity theft and cyber security concerns.

4 Many Australians experience significant harm to their mental health after experiencing a scam or financial crime.
Consider accessing services such as **Lifeline – 13 11 14** and **Beyond Blue – 1300 22 4636** for crisis support.

About BDO

BDO's forensic experts work with organisations to effectively prevent, identify and respond to suspicious activity. The multidisciplinary team includes certified accountants, certified fraud examiners and forensic accountants, forensic technology professionals, licensed investigators, financial analysts, and former members of law enforcement.

Stan Gallo
Partner, Forensic Services
stan.gallo@bdo.com.au
+61 7 3237 5995

Conor McGarrity
Partner, Forensic Services
conor.mcgarrity@bdo.com.au
+61 7 3237 5841

Karyn Lander
Partner, Forensic Services
karyn.lander@bdo.com.au
+61 8 6382 4914

Michael Tarnawsky
Forensic Technology Specialist, Forensic Services
michael.tarnawsky@bdo.com.au
+61 7 3237 5693

Katie Bourne
Director, Forensic Services
katie.bourne@bdo.com.au
+61 2 8221 2266

John Karamoschos
Director, Forensic Services
john.karamoschos@bdo.com.au
+61 2 8221 2235

1300 138 991
www.bdo.com.au

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES
NORTHERN TERRITORY
QUEENSLAND
SOUTH AUSTRALIA
TASMANIA
VICTORIA
WESTERN AUSTRALIA

AUDIT • TAX • ADVISORY

25-01-1831