Tel: +61 7 3237 5999
Fax: +61 7 3221 9227
www.bdo.com.au

Level 10, 12 Creek Street
Brisbane QLD 4000
GPO Box 457 Brisbane QLD 4001
Australia

Dr Sean Turner
Committee Secretary
Senate Economics Legislation Committee
PO Box 6100
Parliament House
Canberra ACT 2600
Via email: economics.sen@aph.gov.au

9 January 2025

Dear Dr Turner,

Inquiry into the Scams Prevention Framework Bill 2024

BDO refers to the invitation by the Senate Economics Legislation Committee to provide comment and recommendations for the Inquiry into the Scams Prevention Framework Bill 2024. BDO welcomes the Government's introduction into Parliament of the *Scams Prevention Framework Bill 2024* (the Bill) and the proposed Scams Prevention Framework (SPF).

In preparing this response, we have drawn on our experience investigating scams as well as our research and analysis on scam culture and in-depth multi-jurisdictional scam data analysis, including through BDO's quarterly Australian Scam Culture report.[1]

While we make no recommendations in this submission, our experience in regulatory compliance and investigations suggests three aspects that will be critical to the SPF's effectiveness:

- **Clearer definitions** - a refined definition of 'scam' supported with clear guidance and examples will support the effective application of SPF and a consistent reporting taxonomy for Australia's scam environment. Ongoing challenges in analysing and comparing Australia with other countries' publicly available scam data reinforces the importance of clear definitions to enable consistent application, reporting and benchmarking against international peers.
- **Data collection and reporting** - a streamlined and standardised approach to scam data collection, sharing and reporting can facilitate collaboration between ecosystem participants. An agreed common data sharing protocol could facilitate this process to deliver a 'single point of truth' for data on Australia's scam environment, supporting effective resource allocation.
- **Consumers at higher-risk** - an ecosystem approach should address the ever-shifting modes of scam delivery, scam typologies and vulnerable cohorts. Regulators and regulated entities have a critical role in informing and educating at-risk consumers about the ongoing and emerging risks so that the SPF remains responsive to the changing scam threat environment.

[1] Analysis for the September 2024 quarter can be found here: Australian Scam Culture Report: September 2024 quarter - BDO. BDO is regularly invited to appear on radio and TV to inform consumers on emerging scam trends and how members of the public can better protect themselves from scammers.

Should you have any questions or wish to discuss any of the comments made in this submission, please contact our team on 07 3237 5841 or at conor.mcgarrity@bdo.com.au.

Yours sincerely,

Conor McGarrity
Partner, Forensic & Integrity Services

Stan Gallo
Partner, Forensic & Integrity Services

Introduction

BDO welcomes the Government's introduction into Parliament of the *Scams Prevention Framework Bill 2024* (the Bill) and the opportunity to make a submission on the Bill to the Senate Economics Legislation Committee.

As outlined in our previous submission to Treasury on its consultation paper, 'Scams – Mandatory Industry Codes' (consultation paper), BDO supports the introduction of an ecosystem-wide framework to support relevant businesses and regulators to identify, prevent, detect and respond to scams.[2]

The introduction of the Scams Prevention Framework (SPF) is a positive, proactive measure to curb the financial and emotional toll of scams on Australians, aiming to reduce financial losses to scams. The proposed Framework is far-reaching; but its success will require a comprehensive, collaborative approach between the public and private sectors, and consumers at large.

BDO's work on scams and related economic crime

BDO provides a range of advisory services related to scams and other economic crime, primarily through the specialists in our national Forensic and Integrity Services team. These relevant services include end-to-end expertise in prevention, detection, response and reporting across the scope of economic harms, including:

- Scams
- Fraud and corporate misconduct
- Corruption
- Money-laundering
- Regulatory non-compliance
- Privacy breaches
- Whistleblower matters
- Cyber breaches to perpetrate scams and fraud

Our multidisciplinary team includes certified and forensic accountants, certified fraud examiners, forensic technology professionals, licensed investigators, financial analysts, and former members of law enforcement and Australian regulatory bodies.

Summary

Our submission builds on BDO's previous Treasury submission and addresses the key aspects of the SPF. In preparing this response, we have drawn on our experience investigating scams as well as our research and analysis on scam culture and in-depth multi-jurisdictional scam data analysis, including through BDO's quarterly Australian Scam Culture report.[3]

---

[2] BDO's public submission to Treasury is available on Treasury's website, Scams Prevention Framework – exposure draft legislation | Treasury.gov.au

[3] Analysis for the September 2024 quarter can be found here: Australian Scam Culture Report: September 2024 quarter - BDO

In preparing this submission, we have also considered relevant commentary from the Senate Standing Committee for the Scrutiny of Bills in its (November) Scrutiny Digest 14 of 2024. This submission is intentionally succinct and aims to address the critical aspects where we consider there to be opportunities for enhancement to the SPF, or challenges to consider for its efficient and effective implementation, including:

1. Clearer definitions - key to the success of the SPF will be ensuring a consistent definition of what constitutes a scam and that it is consistently applied. It will be important to ensure that the same definition doesn't reach too far and inadvertently encompass broader economic crime considerations (e.g. fraud) that do not fit the intent of the definition of scam, and by extension to the definition of 'actionable scam intelligence'.

2. Data collection and reporting - there are advantages to streamlining the approach to scam data collection, sharing and reporting. While it is likely that the SPF will generate a significant volume of actionable scam intelligence reports, the Bill provides for authorised third parties to operate data gateways, portals or websites. This will allow regulated entities to leverage existing scam data collection and reporting mechanisms, which should increase efficiency and effectiveness, particularly for those regulated entities with fewer resources. An agreed common data sharing protocol could facilitate this process.

3. At-risk consumers - regulated entities may also be required to identify its SPF consumers who are at risk (or who have a 'higher risk') of being targeted by a scam. BDO's scams analysis and research highlight the importance of an ecosystem approach to address the ever-shifting modes of scam delivery, scam typologies and targeted cohorts. Digital platforms in particular are used by scammers to target their victims and will have a lead role to play in ensuring the effectiveness of the SPF. Regulators and regulated entities will also have a continuous role in informing and educating consumers about the ongoing and emerging risks.

Definitions: 'scam'

The current application of the term 'scam' varies across the Australian economic crime ecosystem and from country to country. This creates inconsistency in scam data reporting in Australia and makes it difficult to compare scam regulatory frameworks across international jurisdictions on a 'like-for-like' basis.

For example, in the UK when the victim is themselves not involved in initiating or facilitating the transaction, the instance may be deemed a 'fraud', and thereby not captured or reported as a scam. In contrast, the Australian data collection and reporting currently includes this type of broader fraud activity in the government's reported Australian Competition and Consumer Commission (ACCC) compiled data.

The definition of a 'scam' is set out in the Bill at 58AG. The proposed definition is (understandably) broad to capture a range of potential scam-related activities. However, difficulties may arise due to the expansive scope of the definition, particularly where there is limited guidance or examples of what types of activity may fall within, or outside of, the definition of scam.

Our initial global research indicates that there is an opportunity to set out specific scam typologies that fit within the definition of scam (potentially in sector codes), and to also provide examples of adjacent economic crime – such as fraud – that are not intended to fit within the definition.[4] In clarifying the definition of scam, careful consideration may need to be given to potential unintended consequences for consumers and regulated entities:

- Impact on Financial Inclusion: The introduction of new scam definitions and any potential reimbursement models may have unintended consequences on financial inclusion (e.g., where definitions or reimbursement models are complex or not easily understood by culturally and linguistically diverse groups), potentially affecting vulnerable customers and their access to financial services.
- Adaptation of Scam Techniques: The addition of a new scam definition may lead to scammers adapting their techniques to circumvent the proposed SPF, potentially leading to the emergence of new scam methods. This risk requires ongoing and close monitoring by ecosystem participants.

On balance, a clearer definition will help ensure consistent application of the SPF and reduce the risk of under/over identification of scam activity. This will ultimately improve the integrity of scam data collection and reporting (discussed below) and provide greater clarity for Australian consumers. Ongoing review and consultation with stakeholders will be crucial to ensure definitions remain effective and relevant in the ever-evolving world of scams.

Data: collection and reporting

The lack of an agreed and applied definition of a scam means the current approach to identifying and categorising scam intelligence is inconsistent, and scam data collection and reporting has the potential to be inaccurate, duplicated or incomplete. Currently, national scam data may be compiled by the ACCC from various sources, including from Scamwatch, ReportCyber, IDCARE, the Australian Securities and Investments Commission (ASIC) and bank-reported data through the Australian Financial Crimes Exchange (AFCX).

While steps may be taken to address and remove duplicate or non-scam data in the current reporting regime, challenges remain with this multi-stream approach. Like other economic crime-related reporting mechanisms currently operating,[5] there may be advantages to streamlining the approach to scam data collection, sharing and reporting:

- **Centralised reporting can deliver efficiencies:** Like the national cyber security hub, there may be efficiencies gained through establishing a centralised reporting mechanism where all stakeholders can share scam intelligence, incident data, and relevant information with a single responsible entity.

[4] For example, a scam may involve psychological manipulation of the victim via contact, whereas fraud may not necessarily involve the victim's permission or knowledge.

[5] For example, AUSTRAC's mandated reporting regime for its regulated entities' 'suspicious matter reports'.

- **Secure platforms can reduce duplication**: Exploring the use of secure information sharing platforms or databases where businesses can input data once, and authorised entities can access the information as needed. This information can be used for developing standardised reporting formats and protocols that are accepted by multiple entities to ensure consistency and facilitate the sharing of information without the need for businesses to tailor reports for different SPF regulators.
- **Data streamlining promotes collaboration**: Facilitating collaborative industry initiatives where businesses within the same sector collaborate to share relevant scam intelligence and incident data. This collective approach can reduce the individual reporting burden on businesses while ensuring comprehensive information sharing while building the ecosystem.
- **Clear data protocols ensure consistency:** Defining clear protocols are essential for reporting cross-sector scam activities. Regulated entities may encounter situations where scams span multiple industries, so establishing procedures for cross-sectoral reporting can simplify the process for involved entities.
- **Leveraging technology supports timely intervention:** Streamlining data collection and analysis centrally will enable future development of automated reporting tools and systems. Automated reporting can help regulated entities submit required information efficiently, reducing manual effort, minimising the reporting burden and enabling timely responses to scam activity.[6]

The Bill stipulates that regulated entities must give the SPF general regulator reports of any actionable scam intelligence.[7] When operational, it is likely that the SPF will generate a significant volume of actionable scam intelligence reports, particularly as the framework and regulated entities come to terms with reporting expectations (i.e. what is and isn't reportable as a scam). This may require a major increase in SPF regulator capacity to meet this demand, and to ensure timeliness in maximising the received actionable intelligence for better consumer protection.

The Bill provides that the rules may prescribe a scheme for authorising third parties to operate data gateways, portals or websites that give access to reports provided by regulated entities containing actionable intelligence about scams.[8] One potential solution to the expected growth in actionable intelligence is therefore to leverage existing scam data collection and reporting mechanisms that exist in the various sectors, such as the Australian Financial Crimes Exchange (AFCX).

Consumers at risk: an ecosystem approach

The Bill introduces the possibility that some sector entities may also be required to provide their consumers with information arising from their scam intelligence.[9] Regulated entities may also be

---

[6] For example, the Australian Financial Crimes Exchange (AFCX) currently aggregates financial crime data from public and private sector contributors including banks, payment providers and telcos.

[7] Proposed Subdivision E

[8] Proposed section 58BT

[9] Proposed section 58BK(2)(c)

required to identify its SPF consumers who are at risk (or who have a 'higher risk') of being targeted by a scam.[10]

It could be reasonably expected that much of the information and intelligence to support these requirements may be drawn from entities' mechanisms by which consumers report activities that may be scams, plus from broader available data relevant to that entities' functions and consumer base. For completeness, it may also come from a comprehensive scam risk assessments by the entity, so that it identifies and manages the kinds of scam risks its services face (which is also relevant to whether the entity has taken 'reasonable steps' for compliance purposes).

BDO's quarterly Scam Culture Report[11] has been tracking changes in Australia's scam landscape since 2023. Some of the most recent report's insights into at-risk consumers include:

Scam category

Since the inception of our Australian Scam Culture Report, investment scams have consistently accounted for the highest dollar amount lost to scams, with cryptocurrency playing a significant role. Cryptocurrency schemes - and the ensuing scams - are becoming more popular amongst younger populations and could be contributing to this increase.

With the recent uptick in cryptocurrency and Bitcoin value in the wake of the U.S. presidential election, the cryptocurrency investment market has become an attractive target for scammers due to its increasing value and the difficulty in the identification and tracking of participants.

Delivery methods

In the September 2024 quarterly report, we observed a shift in scam delivery methods, with emails overtaking text messages as the top reported scam delivery method. This shift marks the first quarter since we began the Australian Scam Culture Report where text messages were not the predominant channel for delivering scams.[12]

Age groups at risk

While individuals over-65 remain the primary targets for scammers, we noted a 12 percent decrease in incidents among the 55-64 age group from the previous quarter's data, indicating some potential improvement in scam awareness and detection for this age group. Together with improving detection measures tailored to the demographic, this suggests that they are becoming more savvy and increasingly aware of scam tactics. This trend is encouraging, as it indicates that awareness campaigns and educational efforts are likely having a positive impact. Several factors could be contributing to this reduction (Figure 1 below).

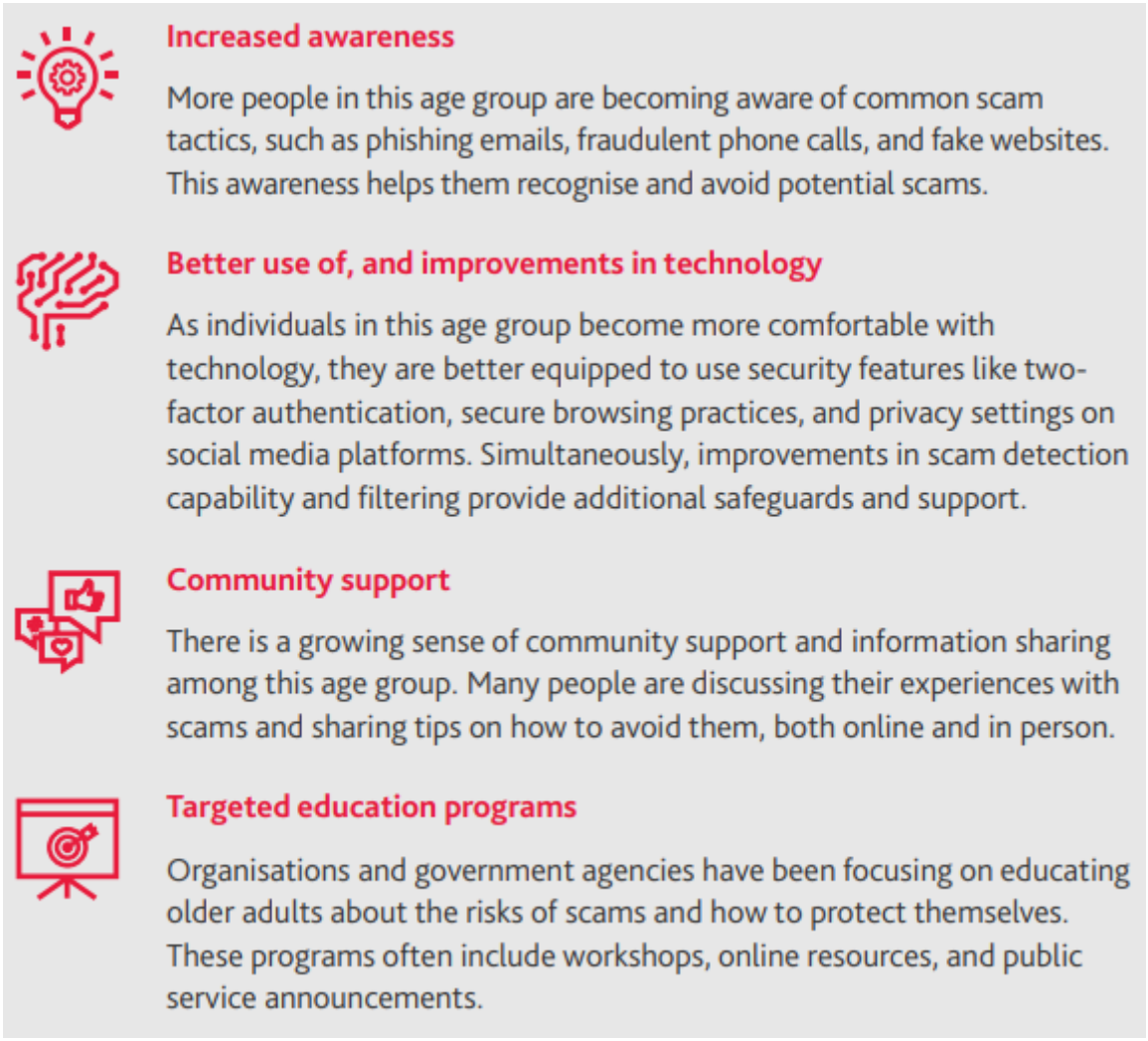
---

[10] Proposed section 58BK(2)(b)

[11] This is a link to the September 2024 quarterly report

[12] It's possible that individuals may no longer be reporting all text message scams they receive to Scamwatch

Figure 1. Contributing factors: reduction in scam losses among the 55-64 age group



The results from our ongoing quarterly reports and multi-jurisdictional scam analysis and research highlight the importance of an ecosystem approach to address the ever-shifting modes of scam delivery, scam typologies and targeted cohorts. Digital platforms are being used by scammers to target their victims and will have a lead role to play in ensuring the effectiveness of the SPF. Regulators and regulated entities will also play a critical ongoing role in informing and educating consumers about the persistent and emerging risks so that all relevant sectors and consumer groups contribute to making Australia unattractive to scammers.

Concluding comment

While the Australian Government's Scam Protection Framework is a proactive step in protecting consumers and organisations against scams, implementation may not be as easy across the board, which in turn can impact its overall effectiveness. Smaller and mid-tier proposed regulated entities in Australia are grappling with significant challenges due to their limited resources in comparison to the larger industry entities. They often find themselves at a disadvantage, particularly when it comes to the costs and expertise required to design and implement economic crime risk frameworks to meet regulatory and legislative compliance.

As larger entities with greater capacity and capability bolster their defences against scams and fraud, scammers increasingly pivot to target the smaller institutions which are perceived to have less robust prevention, detection and response capabilities. Additionally, many of the smaller entities have a client demographic, such as older Australians, that also make them attractive targets. If unaddressed, the resulting cascading effects – where scammers target the 'weakest link' in the ecosystem - can be profound.

The Australian government should consider the scale of the impact of its regulatory and legislative decisions across the regulated community. Ensuring that affected entities have the support and resources they need to comply with regulations is crucial to the success of the SPF. Without this support, the ecosystem may become unbalanced, with smaller institutions bearing a greater burden of the associated risks.

By considering the needs of all players in the scam targeted sectors, the government can help create a more secure and equitable environment that hardens Australia's scam ecosystem and protects all Australian consumers.