Tech Council of Australia

Scams Prevention Framework Bill 2024 – submission to Senate Economics Legislation Committee

Tech Council of Australia

January 2025

Tech Council of Australia
www.techcouncil.com.au

Tech Council

1. Introduction and overview

Thank you for the opportunity to make a submission regarding the Scams Prevention Framework Bill 2024 (Scams Bill). The Tech Council of Australia (TCA) recognises the importance of strong consumer laws as a foundation for consumer trust in businesses, leading to economic growth and innovation. In particular, we recognise the increasing problem of scams affecting Australian consumers, and the challenges scams pose to maintaining consumers' trust in businesses, including businesses in the tech sector. The TCA supports the objectives to protect Australian consumers from scams and to make Australia a less attractive target for scammers.

The TCA is Australia's peak industry body for the tech sector. The tech sector is a key pillar of the Australian economy, and Australia's seventh largest employing sector. The TCA represents a diverse cross-section of Australia's tech sector, including startups, scale-ups, venture capital funds and global tech companies, many of whom provide services directly to consumers.

We acknowledge the harm suffered by consumers from scams in Australia, with available figures likely to significantly underestimate the scale of Australia's scam problem, given scam victims may often not report scams due to a sense of shame or embarrassment.

In this context, the TCA supports efforts to address scams and has provided observations on the Scams Prevention Framework, including the principles that service providers must comply with, and the mandatory service-specific obligations set out in codes.

Scams are highly complex and differentiated, with often a complex supply chain connecting scammers with scam victims. The TCA considers that there are a range of improvements that should be made to the Scams Bill that will, first and foremost, operate to protect consumers' interests by protecting them more effectively from scams, and ensuring that ordinary, essential communications are not disrupted.

In order for the proposed framework to be effective, the Scams Bill should:

- Provide greater certainty to businesses subject to the legislation about compliance with their obligations
- Reduce duplication between regulators, and simplify the dual regulatory model
- Ensure that legitimate communications are not blocked or limited
- Provide appropriate boundaries around the external dispute resolution process, and
- Ensure a whole-of-economy uplift to disrupt the scams supply chain.

At a high level, the TCA supports the six principles that are outlined in the Scams Bill, which aims to bolster businesses' ability to deal with scams through requirements to prevent, detect, report, disrupt, respond to and put in place suitable governance arrangements.

The TCA acknowledges that there have been positive changes to the proposed framework since the Exposure Draft that seek to address some of the concerns raised in earlier consultation. In particular, the TCA acknowledges the improvements to the Scams Bill in relation to:

- A mechanism by which entities can be excluded from the operation of the Scams Prevention Framework, and
- Requirements for a Minister to consult before designating a sector.

Tech Council

However, the TCA continues to have concerns about elements of the Scams Bill. In particular, the TCA is concerned that the breadth of the Scams Bill (including the definitions of what constitutes a scam and the reporting obligations for potential scams) is not appropriately targeted to key areas of harm, and is likely to incentivise businesses to over-correct to blocking or restricting legitimate communications. The dual-set of compliance obligations established by the principles and sector-specific codes are also likely to cause regulatory uncertainty and unnecessary costs.

A key policy objective here should be to ensure that consumers retain the benefit of communications platforms and systems, while ensuring that businesses are appropriately incentivised to pro-actively deal with scams at a systems level. A systems level approach will ensure that businesses put in place the right processes and safeguards to deal with the issue of scams at a systems level.

2. The model for dealing with scams introduces complexity and uncertainty

We acknowledge that the Scams Bill contains improvements which mean that the codes that fall under the Scam Prevention Framework are likely to contain more detail about the implementation and expectations for each regulated sector and provide for the regulator to publish guidance material. We consider that this is important, and that it is important that the codes that are developed are consistent both with the framework, and across the different codes.

We are concerned that the model proposed in the Scams Bill legislation for dealing with scams introduces significant complexity and uncertainty for businesses that would be subject to the obligations. In particular, we are concerned by the interaction between the codes and the overarching framework, and the interaction between codes, framework, EDR obligations and private action.

The interaction between the overarching principles-based framework and the mandatory sector-specific codes adds significant complexity for designated sectors. In particular, there is no comfort for businesses that comply with the obligations in the relevant code that they have complied with the framework obligations set out in the legislation (which itself contains vague, uncertain obligations, set out in further detail below). Given the codes are designed to be adaptable to the dynamic nature of scams, and responsive to the issues facing consumers, we consider that it is inappropriate that businesses could be separately penalised for non-compliance with the framework principles when they are complying with obligations set out in the mandatory codes.

The Scams Bill also sets out a model for dealing with scams that places businesses at potential risk of consequences arising from the operation of sector-specific codes, framework legislation, external dispute resolution processes (EDR), and private action. Together, this is likely to introduce significant complexity and risk for businesses, and will result in businesses over-correcting in response to scams, that is likely to block legitimate traffic. This could have serious consequences for consumers, who rely on these businesses to provide essential communications services, and who require these services in a timely, consistent manner.

Tech Council

3. Definitions are overly broad

Scams definition

The definition of scam, as set out in the Scams Bill, is intended to capture conduct that 'involves deception' and 'would, if successful, cause loss or harm including obtaining SPF personal information of, or a financial or other benefit from, the SPF consumer or the SPF consumer's associates'. While we understand the intention for the definition to reflect the wide range of activities scammers engage in, and is designed to capture evolving behaviours over time, we consider that the definition of scam is overly broad. We consider that the definition of a scam should focus on the financial impact to a consumer, rather than on personal information.

To the extent that the definition of a scam is not appropriately targeted, it is likely to result in regulatory overlap with other consumer protections, that operate to protect consumers from fraud, unconscionable conduct, misleading and deceptive conduct, among other protections.

Definition of designated services

We consider that the Committee will need to give further consideration to the definition of the services and sectors that are designated as part of the Scams Prevention Framework. Particularly in the context of digital services, it is often difficult to draw clear lines around particular services and there are complicated supply chains involved in the delivery of services. It is vital that it is clear to businesses whether they are captured by a designation or not.

For example, the Scams Bill refers to the definition of social media service used in section 13 of the *Online Safety Act 2021* (Cth). We consider that this broad definition of social media service is broad, and not appropriately targeted to services that are the target of scam activity. The Scams Bill contemplates the designation of sectors as a result of a risk-based approach, which we strongly support, however, the use of this definition undermines a risk-based approach by attaching comprehensive, complex requirements on businesses and platforms that are not a key target of scammers.

We consider that the designation of services, and the articulation of which businesses fall within that designation, should focus on the potential harms arising from scams, and be clearly communicated by Government when a designation decision is made.

Consumers captured by the code

The Scams Bill seeks to apply to protect consumers that are in Australia or ordinarily reside in Australia, applying to Australians that are overseas.

We are concerned about the extra-territorial application of the obligations that would mean that businesses would have obligations that relate to any Australian overseas. This has significant consequences for technology companies, who operate across many different jurisdictions, and are likely to supply different products and services in different jurisdictions (with particular features available in some countries but not others, for example).

This is likely to overlap with scams legislation in other jurisdiction, creating complexity and confusion where there are overlapping regulations from different jurisdictions. It also introduces significant complexity where features that are available or not within Australia differ to those in other countries.

Tech Council

4. Obligations for businesses are likely to further introduce complexity and uncertainty

We consider that the obligations set out in the Scams Bill for businesses that would be designated are likely to further introduce complexity and uncertainty.

The framework legislation relies on businesses taking 'reasonable steps' to address scams. This is an inherently uncertain measurement, and combined with the significant penalties attached for breaches of the framework legislation, is likely to result in businesses over-correcting for scams and unintentionally blocking legitimate traffic. This has serious consequences for the consumers and businesses that rely on designated sectors for communication and as critical pieces of infrastructure for their business.

We welcome the definition of 'reasonable steps' in the legislation, however, we consider that 'reasonable steps' should be further clarified in the codes, with specific reference to what it means for the designated businesses. We also consider that the Committee should consider an approach that (consistent with anti-money laundering and counter-terrorism financing regulations) focuses on businesses putting in place the appropriate risk-based systems and controls to address scams, rather than focusing on the individual scam level.

Scams Bill does not adequately consider the complexity of scam supply chains

In addition, the Scams Bill does not contemplate the complex supply chains to which scams are a part of. For example, the proposed designation of search engine advertising ignores the complex supply chain that results in targeted ads being shown to consumers. The Committee should consider the extent to which the search engine is the appropriate entity to be caught by the obligations set out in the Scams Bill, or whether there is a need for obligations to apply across the ad tech supply chain.

As another example, in telecommunications there can be a complex supply chain involving multiple carriers or carriage service providers (or over IP technology) in the provision of a call or SMS to an end-user. It is not clear whether or how the proposed framework will account for this in terms of assigning responsibility or accountability for scams. We consider that the obligations to prevent and detect scams should not apply to every stage of the supply chain. For example, carriage service providers provide important services to businesses in Australia, and can be used for essential, time-sensitive notifications (such as emergency SMS alerts). Applying these obligations to every stage of the supply chain increases the risk that while carriage service providers have vetted and confirmed the identity of their customer, that the traffic could still be blocked by a carrier using pattern detection that detects a new, high volume of traffic coming from particular numbers.

It is essential that the Scams Bill be amended to ensure that obligations do not overlap, greatly increasing the likelihood of legitimate, essential traffic being blocked.

5. Penalties and External Dispute Resolution

We note that the proposed penalties for breach of the framework are significant, and there is the risk that a single breach could result in multiple enforcement actions and multiple penalties, in addition to private action that would hold businesses liable for compensating consumers for scam-related losses.

Tech Council

We consider that the Committee should carefully consider the quantum of the proposed penalties to ensure that they are appropriate and targeted, especially given the pathways for consumer redress for scam-related losses.

The proposed penalties for breaches of the framework, and that the existing consumer law penalties are not appropriately applied in this context. The quantum of these penalties is likely to result in platforms and telecommunications providers over-correcting to avoid the risk of breaching the framework and facing fines. Obligations that would result in the delay or disruption to delivery of communications services to consumers can also have negative consequences where consumers rely on these services for timely communication.

We also consider that the Committee should give further consideration to the External Dispute Resolution model and consumer redress process. The model proposed does not have a precedent internationally and differs significantly from that in the United Kingdom, which is focused on the banking sector and sets clear boundaries and exceptions around consumer redress. The model also creates significant uncertainty around how compensation would be proportionately shared across a complex supply chain.

6. Reporting obligations

We consider that the obligations on businesses to report potential scams to the ACCC, and the potential penalties that attach if they do not, is likely to incentivise significant over-reporting of scams to the ACCC. This is unworkable for industry and likely to include many reports for activity that is not ultimately a scam. We consider that this is likely to have significant implications for the ACCC who are likely to receive a flood of scam reports, making it difficult to monitor and action responses to genuine scams. Ultimately, this will impeded efforts to protect consumers from scams.

Given the framework is designed to facilitate information-sharing about scams across platforms, we are concerned about the potential privacy implications of sharing detailed information about scams. Notwithstanding the changes to the legislation that provide some further guidance about the sort of personal information that should not be disclosed, we consider that there are still privacy risks from this information sharing.

Government should provide further clear guidance, in subordinate legislation, to businesses about the type of data that should be shared, and how to maintain best practice privacy policies while also facilitating information sharing about scams. This is especially so given the framework contemplates the sharing of personal information about potential scammers and their victims, including their name, email address, phone number, bank account details or credit card details. We also consider that it is important to understand the interaction with the OAIC in the context of the proposed sharing of scam data.

7. Combatting scams requires a whole-of-economy approach

We consider that successfully protecting consumers by combatting scams in Australia will require a whole-of-economy approach that will ultimately need to go well beyond businesses contemplated by the Scams Bill. We consider that there is a range of other government actions that are essential to deal with scams in Australia. This includes:

- Education and outreach for businesses and other areas of government that use designated services to reach consumers to ensure that they ensure they avoid legitimate communication being blocked, and explore alternatives where necessary

(for example, the use by the ATO of one-time-use access codes, which are frequently mimicked by scammers).

- Education and outreach for businesses (especially targeted at SMEs) that will be regulated under the framework to explain their obligations, and provide resources to deal with scams on their platform, in compliance with the framework. Businesses should also be provided with guidance about appropriate actions to take when consumers disagree with a platform's assessment that the consumer is being scammed.
- Education and outreach for consumers, in particular, to vulnerable consumer groups should be prioritised. Where compliance with the framework comes at a cost to user experience (for example, slower payments, or friction in the use of communications platforms), consumers should be educated to understand why this might be the case.
- Incentivising small and medium sized businesses to invest in anti-scam technologies and practices through grants, subsidies, and tax incentives.
- The ACCC being given takedown capabilities to deal with scams, consistent with ASIC's takedown powers to remove or limit access to fraudulent or malicious websites on the internet.

8. Recommendations and conclusion

1. **Recommendation 1:** compliance obligations under the framework legislation principles and sector-specific codes should be made consistent so that businesses complying with the obligations set out in the mandatory codes will not be caught by potential breaches of the framework legislation. Obligations should be focused on incentivising businesses to proactively deal with scams at a systems-level, rather than an individual scam-by-scam approach.
2. **Recommendation 2:** simplify the obligations contained in the codes, framework legislation, EDR and private action. These obligations should be consistent with other legislation (such as the Privacy Act) and clear guidance should be provided to ensure that businesses have confidence in complying with obligations.
3. **Recommendation 3:** simplify and ensure consistency between penalties arising from the codes, framework legislation and private action for consumer losses. Penalties should be proportionate and should not incentivise businesses to block legitimate traffic.
4. **Recommendation 4:** definitions (e.g. of a scam and of designated services) should be appropriately targeted to specific harms and avoid regulatory overlap.
5. **Recommendation 5:** reporting obligations should be targeted, clear, privacy-safe and guidance should be provided to businesses about the information required in reporting obligations that balances privacy obligations.
6. **Recommendation 6:** The External Dispute Resolution model and consumer redress should be refined, including by inserting appropriate boundaries and ensure proportionate liability across the complex supply chain.

We appreciate the opportunity to contribute feedback to these proposed reforms and look forward to an ongoing consultation on them.