Tech Council of Australia

Scams – mandatory industry codes

Tech Council of Australia Submission

February 2024

techcouncil.com.au

1. Introduction and overview

Thank you for the opportunity to make a submission regarding the potential introduction of mandatory industry codes in relation to scams. We recognise 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 Government's 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 the Government's efforts to address scams and has provided observations on the proposals in the Consultation Paper to ensure that new regulation is effective and fit for purpose. This includes offering alternatives to the proposals outlined in the Consultation Paper that we believe would better grapple with the complexity and diversity of tech businesses to ensure that measures to address scams are targeted, clear and effective.

Scams are highly complex and differentiated. As a general point, new regulation should be capable of dealing with scams in a way that reflects this complexity, rather than through a 'one size fits all' approach. Further, new regulation should encourage and incentivise businesses to adopt innovative approaches to dealing with scams, which we believe will lead to better outcomes for consumers than a minimum compliance or check-a-box based model.

2. Regulatory model for dealing with scams

The TCA agrees with the three principles outlined in the Consultation Paper for the proposed framework. However, we are concerned by some of the complexity in the proposed framework, and encourage consideration of other options.

Concerns with the dual-regulator model

In particular, we are concerned about the level of complexity imposed by a dual regulator system, where all businesses captured by the Scams Code Framework would deal with the ACCC in relation to the overarching framework and anti-scam strategy, and another regulator for the industry-specific codes. Implementation of the framework in such a way is likely to be inefficient and increase the complexity of the framework considerably. Given that the framework will apply to SMEs, any opportunity to reduce the complexity of the framework and of the obligations that apply to businesses will dramatically improve the likelihood of success.

We consider that a single regulator should be nominated for both the overarching framework and the sector-specific codes. This single regulator should have significant expertise in the sector for which they are responsible, and be funded and skilled accordingly. This would enable the efficient and effective enforcement and oversight of the framework.

Co-regulation as an alternative model for dealing with scams

We encourage the Government to consider alternatives to the Scams Code framework set out in the Consultation Paper. In particular, we consider that there are benefits to adopting a co-regulation model with industry, that would allow for:

- Increased adaptability and innovative solutions that reflect the constantly evolving nature of both digital businesses and of scams
- Greater collaboration and utilisation of the breadth and depth of industry expertise and knowledge in creating obligations that would meaningfully address scams, and lead to more effective strategies for detecting and preventing scams
- The involvement of consumer advocates and other stakeholders in the process to ensure that the interests and needs of consumers are considered, and
- An appropriate level of accountability and transparency, for example, by introducing public reporting that holds all parties accountable, and builds trust with the public.

This co-regulatory model would still enable Government to set the broad expectations and overarching framework, but place the responsibility on businesses for drafting sector-specific codes in the first instance, with Government having the power to step-in and mandate requirements if industry-led initiatives do not meet expectations or prove ineffective.

There are other examples of successful co-regulation with industry in Australia to address a range of consumer harms, such as the Telecommunications Consumer Protection Code, and online safety industry codes covering social media services, app distribution, hosting services, internet carriage services, equipment and internet search engine services. Co-regulatory models allow for flexibility for firms to implement meaningful actions that apply to them, based on their unique business models, rather than trying to group highly differentiated businesses together and imposing obligations that reflect the lowest common denominator between the businesses.

There are also other models internationally, such as the UK Online Fraud Charter, that we should consider learning from in Australia.

In the event that a co-regulatory model is not adopted by government, we make observations in the rest of this submission that are relevant to the proposed framework in the Consultation Paper.

3. Definitional issues

Definition of scams

The Consultation Paper outlines the proposed definition of scam as a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means.

We are concerned that the inclusion of 'designed' as an element of the definition risks both under- and over-inclusion by potentially raising questions of the structure or outward presentation of scams, rather than the motivation of the scammer, which appears to be the point of that element. We suggest the language be changed to more common legal terms such as intent or purpose.

We note that the definition of scams attempts to separate out scams from other types of fraud. We consider that practically, it can be very difficult to differentiate between fraud and scams. However, one of the key characteristics differentiating fraud and scams is a victim's knowledge: for a scam, victims are knowingly misled into giving up money or information, whereas for a fraud, victims are typically unaware of the illegal activity that results in the loss of information or money.

We consider that if Government intends to delineate clearly between scams and fraud, then the level of knowledge of a victim should be incorporated into the definition. We consider that clear guidance, with detailed examples, will need to be provided to businesses to enable them to consistently determine what activity is a scam and for them to comply with the associated obligations in the framework and industry codes.

Definition of digital communications platforms

A key concern that we have with the proposed framework is the definition of Digital Communications Platform that is outlined in the Consultation Paper. We consider that the definition is unclear and potentially extremely broad, and does not grapple with some of the key differences between platforms that would fall under the definition. It also creates further complexity and inconsistencies in the overall regulatory framework for tech in Australia, given this is a new definition that is not used in other laws.

The definition of Digital Communications Platform is unclear and does not refer to specific services that are commonly understood. For example, while content aggregation services would typically refer to services such as media aggregation services (where users are shown news from a variety of services in a single feed), subsequent discussion indicates that content aggregation services could be read as broadly as to include any website that shows display advertising to users. The definition also lacks any element of a 'dominant purpose' which would assist in clarifying for businesses when they would be captured by the framework. For example, a business may provide functionality that enables communication between end users, without that functionality facilitating scams. It is essential that the definitions are clearer.

Further, the services captured by the Digital Communications Platform definition are broad and highly differentiated. The services captured by the definition have different business models, different ways that users engage with the services, and varying degrees of risk. As a result, the definition is not appropriately targeted to businesses that have the highest degree

of misuse by scammers, and any industry code developed for such a broad range of businesses is not likely to be sufficiently specific in how scams are to be identified, targeted, and dealt with.

We recommend that Government consider options to narrow the definitions to capture specific digital platforms that currently have the highest incidence of risk of scams, with the intention that other types of businesses be brought into the framework in the future. For example, we consider the current definitions capture businesses that predominantly provide B2B services and that initially the framework should capture specific types of platforms that interface directly with consumers.

It is also important to provide guidance to businesses that offer a range of services about what happens when part of their business is captured by the framework, but other parts of the business are not. Similarly, where a business is captured by multiple definitions (in particular, in the future where further sectors are added to the framework), we consider it is important to be clear about which codes apply. To the extent possible, duplication should be avoided so that businesses can clearly identify their obligations and not be dealing with different obligations under different codes.

4. Obligations for businesses under the proposed framework

Overall, we note that the obligations that would be imposed on businesses by the proposed framework and the sector-specific codes would carry significant costs and some may have unintended consequences. In considering the obligations imposed on businesses, we recommend the Government further consider their costs and impacts and whether they are commensurate to the risk of scams on those services.

Anti-scam strategy

As a starting point, we consider that businesses' anti-scam strategies should not be made public, as this would undermine efforts for businesses to get ahead of scammers.

We also consider that the obligations for all businesses regulated under the proposed framework to develop, maintain and implement an anti-scam strategy could have a particularly significant impact on SMEs. While large enterprises typically have resources that are dedicated or can be deployed to an anti-scam strategy, the burden is likely to be particularly acute for SMEs complying with the proposed framework. We consider that there is a role for government in assisting SMEs to develop and implement the anti-scam strategy. This assistance could take the form of:

- Clear guidance about what should be in the strategy, and how it should be implemented
- Template strategies for businesses to adopt as is relevant to their business
- Incentives, such as grants, subsidies or tax incentives that encourage SMEs to invest in developing and deploying their anti-scam strategy.

Ecosystem-wide obligations

We also consider that many of the potential obligations that could apply under the proposed ecosystem-wide obligations require careful consideration, for example:

- The obligations to "seek to verify and trace scams where scam intelligence has been received" and "act in a timely manner on scam intelligence received" could be practically difficult to execute. However, given the illegitimate nature of scams, it may be difficult to prove.
- The ability for platforms to detect and disrupt scams can be challenging where scammers move contact off the platform (for example, by moving communication to email).
- Determining what level of confidence is required in relation to intelligence before it is shared or acted upon – intelligence should be credible before it is acted upon.
- A requirement to treat customers fairly and consistently should not restrict businesses from making goodwill payments in relevant circumstances – an obligation such as this could have the perverse effect of preventing businesses from making payments when they do not want to set a precedent that would apply to all customers.
- What the meaning of 'effective, efficient, transparent and accessible' means to businesses that are regulated under the framework.
- The obligation to 'notify other businesses' is unclear, where there is ambiguity about the scope of the obligation and what types of businesses would require notification. We note, for example, if many businesses have to be notified, then it can reduce businesses' ability to act on relevant notifications when they are flooded with irrelevant notifications.
- The proposed information sharing requirements should be confidential and anonymous, outside of providing to regulators. It must be clearer when information should be shared between businesses.
- Requiring businesses to take 'all reasonable steps' to act on scams is a high threshold, and clear guidance should be provided about what steps businesses should take to address scams.
- The ability for businesses to provide consumers with tools to verify information in real time differs significantly across different types of platforms, and it is unclear what these verification tools would look like (and whether they would be effective in preventing scams, particularly where scammers use legitimate, verified accounts to access consumers).
- IDR and EDR obligations could have a significant impact on businesses, especially where legitimate content is reported as being a scam. Legitimate content can be reported as a scam where a user is seeking to vexatiously interfere with the business of another company or individual (for example, where a user does not get a job as a result of a job listing, and where they disagree with the company or a political or social group).
- Government should consider compensation caps for EDR mechanisms across the different sectors regulated by the framework. There should also be express requirements that complainants must act in good faith, with clear penalties where

complainants do not – this will help avoid the mechanisms being 'gamed' by vexatious complainants.

Sector-specific codes

We consider that, compared to the primary legislation, the sector-specific codes are the appropriate place to contain as much detail about the obligations for businesses regulated under the framework. This ensures that the codes can be flexible, and quickly adaptable to changing strategies from scammers.

We also note that experience with existing scams codes for telecommunications service providers shows that industry codes (when developed) should focus on platforms knowing and identifying their customers (and, by extension, scammers), rather than identifying potential scam content, especially where the scam content appears in one-to-one communication with a consumer. We consider that obligations regarding proactive monitoring for scams by platforms also needs to be balanced against privacy obligations to users.

We also have some specific comments on the potential obligations in the sector specific codes:

- The obligation for digital communications platforms to identify and share information where 'an Australian user is likely to be or is a scammer' refers to Australian users, whereas we understand that many (or most) scammers are located overseas.
- Obligations to identify and share information about likely scammers requires careful consideration about how potential scammers are identified, in a way that is consistent across platforms. Further detail about the information that is to be shared by businesses should be clearly set out, and careful consideration should be given to the burden associated with the information sharing requirements.
- Businesses sharing information should be protected if they share information that they believe to be accurate, and businesses should be protected for actions they take based on that information.
- The sector specific codes should also recognise that users may get multiple warnings about not doing something, and then proceed to do it anyhow, and that users may act outside of the reasonable use of a platform, in both cases making them more vulnerable to scams. In these circumstances, platforms should be able to show that they are in compliance where they have taken reasonable steps to protect their users from scams.

5. Penalties

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.

We consider that government should carefully consider 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 over-correcting

to avoid the risk of breaching the framework and facing fines. Obligations that would result in the delay to delivery of communications services to consumers can also have negative consequences where consumers rely on these services for timely communication.

6. Interaction with other regulation

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. Government should provide clear guidance 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. We also consider that it is important to understand the interaction with the OAIC in the context of the proposed sharing of scam data.

We also note that government has agreed in-principle to the ACCC's regulatory reform recommendations for digital platforms, which include targeted measures for digital platforms that relate to scams. We consider that, to the extent that government is considering additional scam measure in response to the ACCC's regulatory reform recommendations, that government should consider the potential cumulative impacts, duplication and risks that could arise across its consumer protection agenda before making decisions on individual reform proposals.

7. Other government action will assist in the successful rollout of any scams strategy

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 (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:** The TCA recommends that Government consider adopting a co-regulatory model within its proposed Scams Code Framework, with Government to set the broad expectations and overarching framework, and industry to lead the drafting of sector-specific codes that set out expectations and commitments for dealing with scams on their respective platforms. This would allow for increased adaptability and innovation, encourage collaboration, utilise the considerable breadth of industry expertise and knowledge, ensure accountability and transparency through reporting requirements, and could involve consumer advocates and other stakeholder groups in the process. A co-regulatory model would also provide Government with capacity to step-in and mandate requirements if the codes do not meet expectations or work effectively

2. **Recommendation 2:** If Government is not inclined to proceed with a co-regulatory model for dealing with scams, then we recommend further refining key aspects of the proposed framework to ensure that new regulation is capable of effectively addressing scams in a way that minimises unnecessary costs and reflects the complexity and differentiated nature of scams and regulated businesses, including:

    a. Narrowing and refining the definition of "Digital Communications Platform" to focus more clearly on the types of consumer-facing platforms that have the highest risk of scams (and exclude lower-risk services such as B2B platforms).
    b. Further considering the costs, impacts and potential unintended consequences of the proposed obligations for businesses under the proposed framework, including the desirability of making anti-scam strategies public.
    c. Considering alternative and more proportionate penalty structures to the existing consumer law penalties.
    d. Ensuring regulation encourages and incentivises businesses to adopt innovative approaches to dealing with scams, rather than a bare minimum compliance-based model.

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