

Scams Prevention Framework – exposure draft legislation

October 2024



Contents

1.	Overview	2
2.	Key recommendations	2
3.	Response in detail	3
3.1	Conflicts between the Framework and sector-specific codes.....	3
3.1.1	Remove regulatory duplication	3
3.1.2	Clarify 'reasonable steps'	3
3.2	Confused dispute resolution processes	3
3.2.1	Improve dispute resolution processes and compensation.....	3
3.3	Reporting overload	4
3.3.1	Effective reporting requirements	4
3.4	Insufficient information sharing protections	4
3.4.1	Add 'limited use' protections to safe harbour	4
3.5	Profligate scope	5
3.5.1	Refine definition of 'scam'	5
3.5.2	Refine definition of 'social media services'	5
3.5.3	Refine definition of 'Actionable Scam Intelligence'	5
3.6	Unclear extraterritorial application	6
3.6.1	Explain how the Framework intends to apply overseas	6

1. Overview

The Business Council of Australia (BCA) represents over 130 of Australia's leading businesses. Our members include some of Australia's largest banking, telecommunications and technology companies. We champion the role that responsible businesses play in generating sustainable economic growth and advocate for policy settings that are in the national interest.

We welcome this opportunity to provide a submission to the *Treasury Laws Amendment Bill 2024: Scams Prevention Framework* (Framework). Business appreciates the opportunity to provide comment on the exposure draft of the Framework, prior to the Bill being introduced to Parliament.

Scams are a growing problem. Businesses are already investing heavily to protect consumers—from voluntary codes like the Scam-Safe Accord for banks to AI-driven tools that detect fraud. But tackling scams requires a whole-of-economy approach. Every sector has a role to play, and the proposed Scams Prevention Framework must be flexible enough to evolve as scams do. This means not locking in rigid structures but allowing the system to adapt. It is also essential to empower consumers to protect themselves through education, with government and businesses working together.

The BCA sees regulation and industry codes as a part of the solution. Sector-specific codes have the potential to empower organisations to apply their expertise to their own problem space. However, regulation must be carefully co-designed with affected sectors so that it is simple and effective.

For this reason, the BCA believes the proposed legislation is rushed, heavy-handed, complex and unclear. It is a prescriptive approach that reflects a compliance mindset rather than seeking to improve practical approaches to stopping scams.

The BCA prefers a collaborative approach. We believe this will deliver better outcomes as ultimately, businesses, government, and consumers must work together to combat this ever-evolving threat.

2. Key recommendations

We recommend the Framework be amended as follows:

1. Remove regulatory duplication. The role of the Scams Prevention Framework should remain simple and not overloaded with obligations—it should be the guiding structure that only obligates entities to follow clear, well-defined mandatory codes. Then, these mandatory codes should be co-developed, sector-by-sector, at a later date.
2. Clarify 'reasonable steps'. Make this much more clearly defined in the mandatory codes.
3. Improve the dispute resolution process, including developing clearer guidelines on proportionate liability so any compensation system is clear and transparent to businesses and consumer.
4. Ensure the reporting requirements are effective, focused on areas of risk and can be actioned.
5. Add 'limited use' protections to safe harbour. A safe harbour is a step in the right direction, but it should be paired with clearer definitions and more refined obligations. Government should consider integrating a 'limited use' obligation on government, similar to what is in the cyber legislative reforms for ASD and the National Cyber Security Coordinator in response to cyber incidents.
6. Refine definitions:
 - a. Narrow the definition of 'scam' by removing 'personal information' from the definition of a scam to improve targeting and reduce unneeded reporting.
 - b. Redraft the definition of 'actionable scam intelligence' to only apply to confirmed scams, not suspected.
7. Explain how the Framework is intended to apply overseas. The Framework should be amended to specifically set out the intended extraterritorial operation.

3. Response in detail

3.1 Conflicts between the Framework and sector-specific codes

3.1.1 Remove regulatory duplication

The BCA is not supportive of the current Framework whereby an organisation can be in breach of the primary legislation while complying with all the obligations in its sectoral industry code.

The proposed Framework creates a problem of complexity. It introduces prescriptive obligations in legislation that apply broadly across industries, while also adding another layer of obligations through sector-specific codes. What we end up with are two potentially conflicting regulatory layers. This is a fundamental oversight and not how you build clarity or trust.

Instead of creating overlapping responsibilities, we need a unified, clear approach that empowers industries to act decisively, without the confusion of competing regulations. Because when the rules are simple, everyone can focus on what really matters—stopping scams.

The BCA recommends that the role of the Scams Prevention Framework remain simple and not overloaded with obligations—it should be the guiding structure that only obligates entities to follow clear, well-defined mandatory codes. Then, these mandatory codes should be co-developed, sector-by-sector, at a later date.

3.1.2 Clarify ‘reasonable steps’

Several principles within the Framework require regulated organisations to take ‘reasonable steps’ to do certain things, such as preventing persons from committing scams, identifying classes of consumers at higher risk of being targeted, detecting and disrupting scams and preventing loss and harms arising from scams. What are ‘reasonable steps’ are not defined, but a failure to take them renders a regulated entity liable to significant civil penalties under the Framework.

It is essential therefore, that what is required by ‘reasonable steps’ in the context of each relevant principle in the framework, be much more clearly defined in the mandatory codes.

Accordingly, the BCA recommends that where the Framework specifies that an SPF Code *may* include details about what will be ‘reasonable steps’ in relation to a specific principle, this be changed to a requirement that the SPF codes ‘*must*’ provide detail of what constitutes reasonable steps in the relevant context. Government should also include a date by which the codes must be finalised.

The Framework, as it stands, places unclear obligations on businesses, requiring them to take ‘reasonable steps.’ What is reasonable to one person might look entirely different to another. The danger here is that without clarity in sector-specific codes, businesses could be left vulnerable to endless challenges. A company could be facing claim after claim, not only from regulators but also from anyone questioning whether they have done enough to prevent scams. That is burdensome and risks exposing sensitive internal strategies that could harm the company and the industry’s ability to combat scams effectively.

If government wants an effective process whereby individuals can seek compensation for scam-related losses, the first step must be to define these obligations in the sector-specific codes. Leaving this concept in primary legislation without proper definition opens the door to confusion and misinterpretation.

3.2 Confused dispute resolution processes

3.2.1 Improve dispute resolution processes and compensation

The BCA is not supportive of the proposed arrangements for External Dispute Resolution (EDR) and Internal Dispute Resolution (IDR) due to the lack of clarity as to areas of liability and as such, how any compensation system would apply.

Boundaries between platforms, services, and sectors are increasingly blurred. Scams today exploit the interconnectedness of our systems, weaving through regulated and unregulated spaces alike.

Yet, the legislation offers no clear framework for determining who bears the burden of compensation. It may be the digital platform where the scam was initiated, the telecommunications provider that facilitated the communication, or a financial service that processed the fraudulent transaction. Each plays a role, yet none can be held wholly responsible in isolation. The draft legislation does not reference proportionate liability, such as the misleading and deceptive conduct proportionate liability rules in Part VIA of the Competition and Consumer Act.¹

The BCA recommends government develop clear guidelines on proportionate liability so any compensation system is clear and transparent for businesses and consumers,

The proposal to prescribe the Australian Financial Complaints Authority (AFCA) as the single EDR scheme for the initial sectors designated under the framework will create challenges as it does not have the expertise in the digital platforms and telecommunications sectors.

Its lack of experience with these industries – and its new need to access technical information and advice – could lead to ineffective handling of disputes and extended delays in resolution.

If ACFA is to be the overarching body, then it will need to have the appropriate upskilling and resources.

Telecommunications entities may already be members of The Telecommunication Industry Ombudsman. The AFCA would then become a second EDR scheme, introducing confusion around what applies and when. Clarity will be needed as to how this will operate, for both businesses and consumers.

3.3 Reporting overload

3.3.1 Effective reporting requirements

Reporting requirements are positive if they lead to actions to reduce scams.

The BCA is not supportive of the reporting requirements as currently proposed which risk a large number of reports to the regulator, without the capacity to action them.

When penalties are high but the thresholds for reporting are vague, the Australian Competition and Consumer Commission (ACCC) could end up flooded with millions of reports about potential scams, drowning in data without a clear plan on how to use it effectively – more noise than signal.

The BCA recommends focusing the reporting requirements to make them realistic and to enable the real risks to be identified, prioritised and acted on.

Under the proposed framework, companies face penalties of at least \$10 million for not sharing information about potential scams. But if the ACCC is overwhelmed by endless reports, how they will process it all and extract valuable insights is unclear. More importantly, the ACCC will find it increasingly difficult to distinguish between real threats and noise when it's buried in data about "potential" scams.

There is another cost, too. By forcing companies to prioritise documentation over action, we are pulling resources away from where they matter most – teams that are focused on disrupting scams in real-time. Already, these sectors must deal with excessive reporting, and this will impose greater demands on capacity. When you slow down these teams with excessive reporting, you create more room for scams to thrive.

3.4 Insufficient information sharing protections

3.4.1 Add 'limited use' protections to safe harbour

Sharing of information can provide an important mechanism to identify, respond and quickly mitigate the spread of scams,

However the Exposure Draft Explanatory Materials mentions that if a regulated entity wrongly flags a website as part of a scam, it must "reverse its actions promptly". It is difficult to see how a company could effectively undo the damage caused by erroneously flagging a website as part of a scam. When trust is on the line, impacts can be swift, severe and irreversible. Government should look at designing much stronger protections against this risk of false positives.

¹ <https://www.kwm.com/au/en/insights/latest-thinking/unpacking-the-scams-prevention-framework.html>

The BCA is also concerned about how government deals with shared information. The Summary of Reforms states that the ACCC may “share this information across the ecosystem to support disruptive action”. It is unclear how this would occur in practice.

The BCA believes that a safe harbour is a step in the right direction, but recommends it be paired with clearer definitions and more refined obligations. Currently, the safe harbour concept is limited. It does not protect regulated entities from claims in other jurisdictions, which leaves businesses exposed. With greater clarity on this issue, businesses can focus on taking legitimate, thoughtful action against scams—driven by evidence, not fear of penalties—minimising the risk of error before it even happens.

The BCA recommends that government consider integrating a ‘limited use’ obligation on government, similar to what is in the cyber legislative reforms for Australian Signals Directorate (ASD) and the National Cyber Security Coordinator in response to cyber incidents:

Such a ‘limited use’ obligation would restrict how scam information shared with the ACCC can be used by other Australian Government entities, including regulators. This obligation would only allow scam information to be used to disrupt scam activity. This means that scam information reported to the ACCC could not be used for regulatory purposes.

3.5 Profligate scope

3.5.1 Refine definition of ‘scam’

The BCA is not supportive of the definition of ‘scam’ and recommends removing ‘personal information’ from the definition of a ‘loss or harm’ within the defined meaning of scam.

The BCA is concerned about how the Exposure Draft’s definition of a scam includes ‘personal information’. This increases the scope of the regulation and potentially conflates data breaches with scams, meaning obligations under the Notifiable Breaches Scheme also become conflated.

This definition could become further expanded with ongoing reforms to the Privacy Act. Government has indicated that it intends to take an expansive definition of personal information that includes technical and inferred information. There is a potential interaction here with the serious invasion cause of action in the Privacy Act that should be clarified.

On the other hand, the expected future reforms of the Privacy Act will tighten sharing of information which will inhibit the ability of businesses to detect scams. This is difficult considering the significant increased penalties that now apply. It is unclear if business will still be penalised if future legislation prohibits access to information, or which disincentivises people from allowing access, resulting in an increase in scams.

The BCA recommends that the Framework must align with initiatives elsewhere, including the Privacy Act, which may run counter to the objectives of this proposed legislation.

The BCA is also concerned about what constitutes a scam. For example, a significant amount of impersonation takes place on messaging services, social media platforms and email that purport to be from an organisation to leverage its brand. It is unclear if this counted as a scam. If a scammer sends out an email scam to a mailing list of one million emails, it is unclear if this counts as one scam or a scam per email. Current wording implies that every communication is a separate scam.

3.5.2 Refine definition of ‘social media services’

The definition of ‘social media services’ under the Online Safety Act is notably expansive. It extends beyond merely encompassing major, mainstream platforms to include any service that facilitates interaction between two or more users.

The BCA recommends a narrowing of this definition.

3.5.3 Refine definition of ‘Actionable Scam Intelligence’

The BCA does not support the proposed definition of ‘actionable scam intelligence’ in s 58AI of the Exposure Draft. It is far too broad and will result in over regulation and reporting. Sectors will waste time and resources attempting to assess what is and is not ‘actionable scam intelligence’.

The Explanatory Materials provides the following definition of ‘actionable scam intelligence’:

A regulated entity will have actionable scam intelligence when there are reasonable grounds to suspect that an activity on or related to a regulated service of the entity is a scam. Whether there are reasonable grounds for such a suspicion is an objective test. Rather than a requirement to have formed a suspicion, the test is whether it is reasonable in the circumstances for the regulated entity to form a suspicion.

This claims that whether there are reasonable grounds for such a suspicion is an ‘objective test’. However, far greater detail is needed about what is ‘reasonable in the circumstances’. It should also be explained whether there is any retrospective assessment. That is, if a regulator or other party determines that an entity *should have* formed a suspicion.

The BCA recommends redrafting the definition of ‘actionable scam intelligence’ to only apply to confirmed scams, not suspected.

3.6 Unclear extraterritorial application

3.6.1 Explain how the Framework intends to apply overseas

The BCA recommends that the Framework be amended to specifically set out the intended extraterritorial operation.

Section 58AJ states that the provisions ‘apply to acts, omissions, matters and things outside Australia’. Does this mean the Framework requires regulated entities to alter the services they provide anywhere in the world?

However, “the standard Competition and Consumer Act extra-territoriality provisions in section 5 – which limits the operation of the extended jurisdiction to bodies corporate incorporated in or carrying on business in Australia – is not being amended to apply to the SPF provisions.”²

² <https://www.kwm.com/au/en/insights/latest-thinking/unpacking-the-scams-prevention-framework.html>

BUSINESS COUNCIL OF AUSTRALIA

GPO Box 1472, Melbourne 3001 T 03 8664 2664 F 03 8664 2666 www.bca.com.au

© Copyright October 2024 Business Council of Australia ABN 75 008 483 216

All rights reserved. No part of this publication may be reproduced or used in any way without acknowledgement to the Business Council of Australia.

The Business Council of Australia has taken reasonable care in publishing the information contained in this publication but does not guarantee that the information is complete, accurate or current. In particular, the BCA is not responsible for the accuracy of information that has been provided by other parties. The information in this publication is not intended to be used as the basis for making any investment decision and must not be relied upon as investment advice. To the maximum extent permitted by law, the BCA disclaims all liability (including liability in negligence) to any person arising out of use or reliance on the information contained in this publication including for loss or damage which you or anyone else might suffer as a result of that use or reliance.



BCA

Business Council of Australia