BCA
Business Council of Australia

Scams – Mandatory Industry Codes

Mandatory Industry Codes

February 2024

Contents

1. Overview

Scams are a plague on modern society, and the Business Council of Australia welcomes the opportunity to make this submission regarding how mandatory industry codes can help address the issue.

Businesses are making substantial investments to protect consumers from scams. This ranges from existing voluntary codes and sector wide commitments (such as the Scam-Safe Accord for Australian banks) through to deploying AI-driven technologies to proactively detect and prevent suspicious behaviour.

We support an approach that recognises that scams require a whole-of-economy solution, with all parts of the ecosystem doing their part. To properly tackle scams, the new Scams Code Framework must be appropriately targeted and flexible. This means recognising the differing roles and capabilities of different sectors, and within these sectors.

The framework must also be flexible enough to evolve as scams evolve. This means not building in rigid structures within the system, like requiring the ACCC to approve all changes to anti-scam strategies.

Moreover, while the framework is focused on industry sectors, wider anti-scam activity also needs to recognise the important role played by consumers, who have a critical role to play in protecting themselves against scams. The role of government and business in this is to empower them to do so. This may involve government working with businesses on a coordinated education campaign to lift the ability of all Australians to detect and avoid scams.

Fundamentally, a collaborative and adaptable approach is the only way to address scams. Businesses and governments have a common interest in addressing and mitigating these constantly evolving threats. For this reason, the regulatory posture adopted by individual sectoral regulators and the ACCC must be collaborative.

The proposed framework must support and be supported by other work underway, including the implementation of the Cyber Security Strategy, the establishment of the digital ID system, and the wider reforms to the Privacy Act.

The implementation of this work will be critical to tackling and reducing scams. The Government's response to the Privacy Act Review agreed-in-principle to a review of requirements imposed on businesses to collect and retain personal information. This must be undertaken urgently and used to identify reforms to enable businesses to use digital ID to confirm an individual's identity, as we have argued in our submissions on the Digital ID Bill.

Businesses are compelled to collect information by government through a range of legislation and regulation that has built up over many years, including to tackle criminal use of the financial system or telecommunications networks, or for national security requirements.

To help reduce the risk of scams, enabling businesses to safely minimise the amount of data they are required to collect and hold will be critical.

2. Key recommendations

The Business Council recommends:

1. Government continue to collaborate with businesses to reduce scam activity.
2. Government work with businesses on a coordinated education campaign to lift individual awareness and resilience.
3. Government undertake the review of requirements for businesses to collect and retain personal information, as recommended by the Privacy Act Review, as a matter of urgency.
4. If Government is minded to designate additional sectors, it begin with digital currency exchanges.

5. The approval for anti-scam strategies be flexible, to allow for sign-off by the most relevant executive.

3. Scope and definitions

The Government has committed to introducing new mandatory industry codes focused on three sectors: telecommunications, banking, and digital communications platforms. The proposed framework will include the provision for the Minister to designate additional sectors. The paper suggests sectors such as superannuation or other payment providers may be considered next.

The initial sectors and many of the suggested sectors are already highly regulated and subject to a range of requirements imposed by government. If the Government is contemplating future designations, it would be sensible to prioritise cryptocurrency exchanges. This would support other government initiatives focused on crypto exchanges, such as the ongoing work underway through AML/CTF, and lift the overall resilience of the economy given digital currencies are used frequently for scams and malicious activity, as reflected in the Government's response to ransomware in the recently released Cyber Security Strategy.

In addition, the requirements imposed on different sectors should recognise that these are not homogenous groupings, both between and within sectors. Telecommunications providers, for example, can effectively disrupt scam activity at scale. However, it may be less appropriate for them to manage individual scams, which would require intruding into private communications. And even within this sector, resellers of telecommunications services rely on wholesale providers of carrier services but also for information enabling the blocking or reduction of services providing suspected scams.

Indeed, the definition of 'digital communications platform' identifies three distinct types of activity with little in common with each other, beyond all types occurring online.

The paper also sets out the definitions of scams and the types of industry sectors proposed to be covered by the Code. We support a single definition of 'scams' being used across the economy.

For the definition of 'scams', the paper suggests these would be "dishonest invitation, request, notification or offer". It would be useful to consider whether it is sufficiently broad to also capture customer identity takeovers.

4. Anti-scam strategies

Under the proposed framework, businesses will be required to develop, maintain and implement an anti-scam strategy. Businesses would be required to seek high-level sign-off of these strategies, with the paper suggesting this be at board level.

There should be flexibility for signing off and approving anti-scam strategies. This is both at the point of inception and for updates to any strategies.

While major updates may require approval by boards or CEOs, in practical terms the framework should have flexibility to allow sign-off by the most relevant executive, particularly where the relevant business may be a smaller part of a large group. This would ensure that accountability and oversight is driven by the officer with the greatest ability and expertise to implement anti-scam measures.

To ensure this flexibility, the ACCC's review of all anti-scam strategies should be carefully scoped. It would be challenging if approval from the ACCC was required for all changes to a strategy. This would introduce unnecessary delays and reduce the ability to respond to emerging threats.

The paper suggests the publication of the anti-scam strategy would not be required. This is sensible. Publication of these details may be useful for scammers while providing little value for the wider community.

5. Dispute resolution

The paper proposes requiring businesses to have both internal dispute resolution (IDR) and external dispute resolution (EDR) processes. This paper proposed further leveraging existing EDR and IDR mechanisms (such as the Australian Financial Complaints Authority and Telecommunications Industry Ombudsman) to resolve customer complaints related to scams.

From the paper, it is not clear how any new requirements will work. Government must act cautiously in establishing any new requirements – cohesiveness between various schemes will be critical, as will clarity about the types of disputes that can be reasonably referred.

As the Government's approach recognises, scams can traverse multiple sectors. A fragmented approach risks inconsistent or suboptimal outcomes between sectors and may in fact create the potential for scams specific to the code: where a consumer raises separate claims with businesses between two sectors, effectively seeking to be paid twice.

BUSINESS COUNCIL OF AUSTRALIA

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