Scams – Mandatory Industry Codes

Telstra Response

Public submission

2 February 2024

Introduction

We welcome the government's intent to introduce a more coordinated cross-sector approach to scam mitigation. Scam calls and messages at best annoy, and at worst defraud our customers, harming our reputation and adversely impacting our customers' perceptions of, and confidence in, our services. Vulnerable customers are at the highest risk of being defrauded, but even well informed and sophisticated customers can fall prey to scammers. Or they can become annoyed when their phone service is used persistently to deliver scam to them or in some cases use (spoof) their number to make scam calls without their knowledge.

It is relatively easy for scammers to use modern technology to generate phone calls, messages and emails in their attempts to defraud consumers. By their very nature, scammers are opportunistic so taking action to remove or inhibit their ability to scam using one approach is unlikely to stop them. They will move on to other more easily executed forms or methods of scam, including as new technologies and tactics emerge. In this environment there cannot be a single solution to reduce the amount of scam. Instead, a multi-faceted, flexible, and cross-sector approach is required. Industry, across multiple sectors, regulators and government all having a role to play.

The telecommunications industry has had a registered (and therefore enforceable) industry code aimed at reducing scam since 2020. Originally with a focus on reducing scam calls, in 2022 it was expanded to include obligations for short message services (SMS). As a result of this code, the telecommunications industry blocked more than one billion scam attempts in the year to 30 June 2023.[1]

We support a more coordinated approach to scam mitigation. The National Anti-Scam Centre (NASC) has been operating since July 2023 and the high level of participation in its first fusion cell and other working groups demonstrates the good will and commitment of industry participants, across multiple sectors, to cooperate in the fight against scam.

We comment below on aspects of the proposed cross-sector legislative framework (by the elements outlined in the consultation paper), primarily as they relate to the telecommunications sector.

Guiding principles

We support a more coordinated cross-sector approach to scam mitigation and the three proposed key principles outlined in the consultation paper that would guide this regime of:

- A whole-of-ecosystem approach to address scams.
- The Framework must be flexible and responsive.
- The Framework will complement and leverage existing interrelated regimes, systems and initiatives.

The development of sector-specific industry codes provides an effective and efficient means to introduce sector specific obligations to monitor for and disrupt scam. Registered industry codes can be amended more easily than legislated obligations and so will be more flexible and responsive; a necessary feature of any approach to scam mitigation given the dynamic behaviour of scammers and technological advancements.

We submit that the NASC is well placed to perform a coordination role to ensure there is consistency and that there are 'no gaps' in the coverage of the sector specific codes. The individual sector regulators could assess proposed industry codes for scam mitigation against the proposed principles and only register codes that meet these objectives.

[1] The Honourable Michelle Rowland MP, Media Release, *Over one billion telco scams blocked in the last year*, 8 August 2023.

Definitions

Proposed definition of scam

The proposed definition appears to be sufficiently broad to capture scam attempts:

> *A scam is a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means.*

However, we offer three observations. First, the phrase 'invitation, request, notification or offer' could be replaced with 'communication' to simplify the definition without significantly altering its meaning. Second, consideration could be given to adding a 'call to action' element to the definition. This would limit scam communication to instances where the potential victim is being specifically asked, or enticed, to take an action likely to result in the scammer obtaining personal information or a financial benefit. It would also make it clear a message or communication is not scam if there is no explicit action required by the potential victim.

Finally, we note that an invitation, request, notification or offer (or communication) is actually an attempt to scam. The potential victim is not 'scammed', or a scam does not occur, unless the potential victim follows or complies with the invitation, request, notification or offer. The distinction is important when considering reporting and recording obligations discussed further below. The recording of reported scam (and of actions taken in response to such reports) should vary according to whether a scam has actually occurred. It would be impractical to keep individual records of (and resultant actions from) each individual attempted scam identified or reported. In contrast, when there has been a financial loss, or a customer has been scammed, more detailed recording and reporting is appropriate.

Variations necessary to accommodate the meaning of scam within the different sectors

We note that, if implemented, the definition of scam in the overarching legislation will need to be wider than that used in sector specific codes. For example, the current definitions of scam in use in the telecommunications sector are limited to scam carried by telecommunications networks:

> ***Scam Call***
>
> *means any voice telephony call which has been generated for the purpose of dishonestly obtaining a benefit, or causing a loss, by deception or other means.*[2]
>
> ***Scam SM***
>
> *means any SM where:*
>
> *a) the SM contains a link or a telephone number; and*
>
> *b) the purpose, or apparent purpose, of the SM is to mislead or deceive a recipient of the SM into using the link or telephone number; and*
>
> *c) the recipient would be likely to suffer detriment as a result of using the link or telephone number.*[3]

This definition of scam short messages reflects the definition of a malicious SMS in Telecommunications (Interception and Access) Regulations 2017. This regulation was amended in 2021[4] to provide an explicit exception to the prohibition on intercepting short messages for the purpose of identifying and blocking short messages.

> *For the purposes of this section, an SMS message is a **malicious SMS** message if:*
>
> *(a) the SMS message contains a link or a telephone number; and*

[2] C661:2022 Reducing scam calls and scam SMs.
[3] C661:2022 Reducing scam calls and scam SMs.
[4] Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021.

(b) *the purpose, or apparent purpose, of the SMS message is to mislead or deceive a recipient of the SMS message into using the link or telephone number; and*

(c) *the recipient would be likely to suffer detriment as a result of using the link or telephone number.*[5]

The proposed definition of scam is wide enough to include these, more specific, scam definitions.

We expect the other sectors to be captured by the proposed new framework will need to similarly limit the definition of scam to their relevant circumstances. For example, there is little a bank can do to prevent a scam that involves a cash payment, rather than an electronic bank transfer.

Defining the telecommunications sector

We agree that the existing definitions of carrier and carriage service provider from the *Telecommunications Act 1997* are suitable and appropriate to define the scope of the telecommunications sector.

Proposed ecosystem-wide obligations in the CCA

As proposed, the ecosystem wide principles to be inserted into the CCA appear to, in some cases, duplicate the type of obligations that should be included in the sector specific codes. For example, *C661:2022 Reducing scam calls and scam SMs* already contains many of the obligations proposed for inclusion in the CCA. It requires carriers and carriage service providers to monitor for and to disrupt the delivery of scam. It requires provision user friendly, easy to understand information about scams and simple mechanisms for consumers to report scams. Under the proposed changes to the CCA, these obligations would also be included in the primary legislation, leading to duplication and the possibility of two regulators taking different action over the same breach of obligation.

If legislative change to the CCA is made to implement the cross-sector code framework, the obligations in primary legislation should not be as detailed as proposed and should be principles-based. Legislated obligations should be limited to the sectors that must register codes and very high-level areas which the codes must address. Further levels of detail and prescription, such as those set out in the consultation paper, should then be left to the sector-specific codes which will be more flexible and responsive.

Anti-scams strategy obligation

There is merit in requiring businesses having an obligation to develop, maintain, and implement a high-level anti-scam strategy, and to have this documented and agreed at a senior level within each business captured by the proposed framework. Businesses should also be required to regularly review this strategy and report to senior levels within the business.

That said, making strategies 'board approved' risks making them less responsive and adaptable than would otherwise be the case. Requiring board approval of a comprehensive anti-scam strategy, will result in a document that is difficult to change. In contrast Telstra's approach to identifying and disrupting scam calls and short messages is constantly evolving. This process is managed by the senior management accountable for compliance with *C661: Reducing scam calls and scam SMs*. The process is adaptive and flexible. Introducing board oversight would restrict flexibility and limit opportunities for change.

We support the position outlined in the consultation paper that organisations should not be required to publish anti-scam strategies. Doing so would risk providing information on 'how to avoid' these strategies to scammers.

[5] Telecommunications (Interception and Access) Regulations 2017.

Information sharing and reporting requirements

Information and intelligence sharing, both within and between different sectors and regulators, can be a useful weapon in the fight against scam. In this regard, we understand that one of the central objectives in setting up the NASC is to build its data-sharing capability to enhance scams information sharing across the ecosystem to improve the quality, timeliness and coverage of across government and the private sector. This may also lead to more innovative solutions for sharing information and intelligence across key players in the scam prevention and disruption ecosystem.

However, information sharing should not be a goal in itself. The sharing of intelligence is only useful if the information/data being shared is unique, verified, timely and actionable. If the data is available to everyone at the same time, there is likely to be little benefit in sharing the data. For example, all major mobile network operators (MNOs) in Australia use the same, or very similar, short message filtering software. By the time one MNO has identified a new scam variant, had time to verify it and share it with the other MNOs via the traceback process in *C661:2022 Reducing scam calls and scam SMs*, it is very likely the receiving MNO has already identified the scam and added it to its own scam filtering software. In these circumstances, sharing the data can result in overhead for all MNOs without improving scam blocking outcomes. Similarly, the sharing of unverified, or out of date information imposes administration costs on all parties that need to verify the information.

For these reasons, we submit that information sharing and reporting obligations would be best dealt with via the sector specific codes. While there will also be need to share information and data across sectors, this can be accommodated without legislative requirements. There are already good examples of data being shared across industry sectors through the NASC and the Australian Financial Crimes Exchange.

Consumer reports, complaints handling and dispute resolution

We submit that there should not be a ‘one size fits all’ approach to consumer reports, complaints handling and dispute resolution across all sectors. Participants in different sectors are likely to receive consumer reports about very different instances of ‘scam’.

A telecommunications provider is likely to receive tens of thousands of ‘scam’ reports per day. Many are false positives: they are simply unwanted political and marketing messages/calls. It is not practical or desirable to keep individual records of these ‘reports’, even for the ones that are indeed scam. Keeping records on the volume of these reports would divert resources away from actions to disrupt scam.

Dispute resolution processes should be limited to instances where there has been consumer loss and the non-compliance with anti-scam obligations has directly contributed to that loss. The non-compliance should also involve an element of negligence or reasonably avoidable failure, given scammers always seek to be one step ahead of anti-scam actions.

Sector-specific codes

The focus should be on sector specific codes and obligations. The function different sectors play within the scam ecosystem vary significantly. Similarly, the opportunities to detect and disrupt scam vary according to the sector and the tools they have available.

The meaning of scam can (and should) vary between sectors (while still fitting within the overarching definition). Telecommunications providers must focus on scams delivered by their networks and services. Digital platforms have a responsibility to ensure scam advertisements are promptly removed (and/or not accepted). There would be little that a telecommunications provider can do to disrupt a romance or employment scam where the interactions are undertaken in person. Banks need to ensure suspicious transactions, or transactions to suspicious accounts are appropriately investigated or questioned. Accordingly, it’s likely that the sector specific codes will focus on the types of scam that they are able to disrupt.

The focus of sector specific obligations should be related to the role each sector has in the in the scam ecosystem. For telecommunications, that is in disrupting communications carried over our networks that can be identified as scam. Communications are private and are, rightly, subject to protection under Part 13 of the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979*.

Review of C661:2022 Reducing scam calls and scam SMs

C661:2022 Reducing scam calls and scam SMs is due to be reviewed in the second half of 2024. We will work with our industry colleagues to conduct this review to ensure it meets the expectations and principles determined by the cross-sector framework.

Oversight, enforcement and non-compliance

We submit that there should be a clear single regulator responsible for enforcing each sector code. If there are overarching obligations introduced into CCA as part of this framework, they should be principles based and at a sufficiently high level to ensure they do not duplicate or overlap with obligations which will be included in sector-specific codes. Otherwise, there is a real risk of confusion and regulatory duplication.

Penalties should be for non-compliance with code obligations. Dispute resolution processes should be limited to where non-compliance with an industry code requirement has contributed to the financial loss suffered by the victim and there is an element of negligence of reasonably avoidable failure.