

**COMMUNICATIONS
ALLIANCE LTD**



**Treasury and the Department of Infrastructure,
Transport, Regional Development,
Communications and the Arts (DITRDCA)
Scams – Mandatory Industry Codes**

COMMUNICATIONS ALLIANCE SUBMISSION
JANUARY 2024

Disclaimer

The views contained herein are general in their nature and attributable to a subset of members of CA. CA are keen to engage further on this topic as the processes of stakeholder consultation continues within the Treasury and DITRDCA, and to engage wider with members.

About Communications Alliance

Communications Alliance is the primary communications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, platform providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to be the most influential association in Australian communications, co-operatively initiating programs that promote sustainable industry development, innovation and growth, while generating positive outcomes for customers and society.

The prime mission of Communications Alliance is to create a co-operative stakeholder environment that allows the industry to take the lead on initiatives which grow the Australian communications industry, enhance the connectivity of all Australians and foster the highest standards of business behaviour. For more details about Communications Alliance, see <http://www.commsalliance.com.au>.

INDUSTRY COMMENTS ON THE OVERARCHING FRAMEWORK PROPOSAL

Communications Alliance (CA) welcomes the opportunity to provide this submission in response to the Treasury and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) consultation into a proposed framework to combat scams across various key sectors, including the telecommunications, banking and digital communications platforms sectors. We look forward to future engagement in this area to ensure overall policy objectives are achievable and fit for purpose in helping to greatly reduce the impact of scams and their effects on consumers.

We and our members continuously engage in activities to reduce scam calls and SMS and share the Government's desire to address the growing threat of scams to Australian consumers and businesses. In this context, and bearing in mind the arguments put forward to date by Departments, we believe that an overarching multi-regulator Framework with new legislative obligations as proposed in the Consultation Paper is not the optimal way to tackle the issue of scams. As scams originate in a multitude of forms, so, too, must the strategies and solutions which attempt to reduce the volume of scams hitting Australian consumers and businesses and the consumer harms which arise when a scam is successful.

We note the different relationships scams can have within different sectors and the risk which can develop from having an overarching Framework with fundamental foundations and principles that may not be suitable for a particular industry. The way an industry or sector ultimately addresses scams may be subject to the technologies and channels available and / or currently being used and also by existing legislative measures (e.g. Part 13 of the *Telecommunications Act 1997* for Carriers and Carriage Service Providers).

CA members have highlighted the fact that the telecommunications industry has been involved in addressing scams since 2009, when it was recognised that SMS should not be used as a form of two factor authentication by banks, Government agencies and other transacting entities. Since then, members have offered various solutions to banks to share information to assist in risk management. These proposals have largely not been acted on. In particular, Treasury has not made the case for further obligations to be imposed on carriers/carriage service providers given the existing requirements under the:

- *Telecommunications (Consumer Complaints Handling) Industry Standard 2018;*
- *Telecommunications (Industry Standard for Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020*, requiring telcos to conduct stronger ID checks to stop mobile porting fraud;
- *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022*, designed to prevent unauthorised access by scammers to consumer's telco services and personal information; and
- *Reducing Scam Calls and Scam SMS (C661) Industry Code.*

Since the registration of the Reducing Scam Calls and Scam SMS industry code in 2020, it has been widely acknowledged that the processes developed in the code have had a positive effect on reducing the number of scam calls and scam SMS being delivered to consumers.

Figures taken from the ACMA report – Action on scams, spam and telemarketing: April to June 2023¹ show:

- approx. 750M scam calls and 257M scam SMSs were blocked between Jul 2022 to June 2023
- phone scam complaints have decreased by 72% since 2020–21 (with the blocking rules introduced in December of that period)
- SMS scam complaints have decreased 86% since 2021–22 (with the blocking rules introduced at the beginning of the 2022–23 period).

The proposed approach of legislating new obligations presents unnecessary regulatory duplication and burden for CSPs, with little benefit for consumers. It is not clear to us what the actual benefits of creating a new framework as proposed are, how the benefits will be measured and recognised, and whether the risks inherent in multi-regulator responsibility will be avoided.

Further, a number of the obligations proposed to be included in the *Competition & Consumer Act* are, we believe, not fit for purpose for CSPs, and appear to be more relevant to the banking sector.

As stated by us during the recent telco industry roundtable with departments, the review of the existing enforceable telco industry anti-scam code, scheduled to take place in 2024, provides an opportunity for industry, consumers, government and regulators to work together to craft any code-based improvements that may be warranted. We would be delighted if all stakeholders took up this opportunity to engage with us in pursuit of continuing better outcomes.

In addition to our overarching response set out above, Communication Alliance provides the following responses to relevant questions posed in the consultation paper:

Questions on the proposed Framework

Does the Framework appropriately address the harm of scams, considering the initial designated sectors and the proposed obligations outlined later in this paper?

We agree that, due to the widespread and evolving nature of the scam threat, there is a necessity for various industry sectors to strengthen their processes relating to the disruption of scams. We see the benefit, also, of a coordinated approach to combatting scams.

Nonetheless - and based in part on the useful discussions we have been able to have with Departments to date - CA members question the rationale behind the proposal for an overarching Framework. Frameworks to develop industry codes already exist and are regulated by the various sector regulatory bodies. It is not clear to us what the actual benefits of creating a new multi-regulator framework as proposed are, how the benefits will be measured and recognised, and whether the risks inherent in multi-regulator responsibility will be avoided.

It should also be reiterated, that members who are currently involved in the disruption of scam activity note there isn't a centralised body that supports government-to-industry, intra-industry, and cross-industry responses to and management of scams.

¹ <https://www.acma.gov.au/publications/2023-08/report/action-scams-spam-and-telemarketing-april-june-2023>

This lack of centralised coordination can result in the duplication of effort, errors, delays in response to emerging issues and missed opportunities to address scams. Rather than adding additional regulatory burden via an overarching Framework, it has been assumed by industry that the NASC would take the opportunity to fill this gap – as seems to be within its charter - and become the national, centralised body for scam co-ordination.

**Is the structure of the Framework workable – can it be implemented in an efficient manner?
Are there other options for how a Framework could be structured that would provide a more efficient outcome?**

In the telecommunications industry, at least, it has been the case over a number of years that a partially shared responsibility between regulators (the ACMA and ACCC) has been in place in relation to telco consumer protections. To date, this model has never been completely coordinated and has presented various challenges for industry, including requirements for near-duplicated effort by service providers and associated additional costs. The proposed Framework risks introducing unnecessary duplication and complexity.

While we support a more coordinated approach, the multi-regulator proposal may not provide an environment that is as agile and responsive as is intended.

Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?

Members agree that the current regulatory environment for code development and registration, which sits under the Australian Communications and Media Authority (ACMA) is an appropriate mechanism and should remain as is.

The other sectors proposed to be covered by the Framework should also be able to work within the remit of their applicable regulatory body to ensure a robust code development process is adhered to. With the introduction of the NASC under the ACCC, there should not be a need to develop the proposed Framework.

The Government could instead assist in ensuring the development of a robust centralised database within the NASC, promote cross industry collaboration between sectors via appropriate scam forums and fund a national education campaign informing consumers of the dangers of scams and where and how to report a scam or to seek assistance in times of need.

Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors?

Current regulatory mechanisms under the appropriate regulator for each sector should be sufficient to ensure code obligation enforcement. Where opportunities or a need for collaboration exists between sectors, this can perhaps be fed back to the respective regulatory bodies and codes updated/adapted to facilitate these outcomes.

Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?

While industry do not agree that a Framework as proposed is required, any additional measures should be appropriately targeted to address particular issues which exist or may arise in a sector. Current regulatory practices within sectors should be sufficient to approach the introduction of new measures if required in the future.

What future sectors should be designated and brought under the Framework?

Similar to the answer above, where the consideration of additional and appropriate measures within a sector is to be made, they should be based on the harms being presented to consumers at the time or based on a rising trend which may be seen from reporting and complaints data.

What impacts should the Government consider in deciding a final structure of the Framework?

Effectiveness and efficiency should be primary considerations as part of this process. Scammers are extremely agile and adept adversaries, and so any framework that manages our responses to their activities needs to be similarly flexible and not overly burdensome.

Questions on definitions

Is maintaining alignment between the definition of 'scam' and 'fraud' appropriate, and are there any unintended consequences of this approach that the Government should consider?

Under the Reducing Scam Calls and Scam SMS industry code, telecommunications Carriers and Carriage Service Providers (CSPs) follow a definition of 'Scam Call' or 'Scam SM' which in general terms are generated with the purpose of obtaining a dishonest benefit via misleading or deceptive means. Carriers and CSPs are unable to determine if an individual call or SM are a scam or fraud, but rather establish processes to identify a scam call or scam SM via particular characteristics or customer complaints.

Attempting to define a 'scam' or 'fraudulent' activity across various sectors is problematic in that each sector will have different use cases. Consumers themselves will also label these activities differently, and it is currently an activity that the NASC itself is having difficulty in finalising. It should be left for each sector to define these terms and appropriately address any differences when it comes to cross sector coordination.

Does a 'dishonest invitation, request, notification, or offer' appropriately cover the types of conduct that scammers engage in?

This is difficult to ascertain. Many scams are only recognisable through the patterns created by repetition. A definition that does not account for this means that businesses are liable for each scam, counting from the first occurrence. An organisations staff and consumers may be unable to precisely identify what may be a scam, Spam or a somewhat legitimate activity. Being too prescriptive can present difficulties. Again, this may be something which is best left for each sector to determine.

What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?

Consideration needs to be given to the fact that scammers are by nature, very agile. Limiting definitions to legislation can cause difficulties down the track if scams evolve in ways yet to be realised.

Will the proposed definitions for designated sectors result in any unintended consequences for businesses that could not, or should not, be required to meet the obligations set out within the Framework and sector-specific codes?

No response.

Should the definitions of sectors captured by the Framework be set out in the primary law or in the industry-specific codes?

Industry specific codes should be used to contain sector specific definitions. The process of a sector specific regulator requesting a code be developed to address an identified issue should also be followed.

Questions on overarching principles-based obligations

Are there opportunities to minimise the burden of any reporting obligations on businesses, such as by ensuring the same information can be shared once with multiple entities?

Examples of opportunities, such as a common database being built by the NASC, or currently in operation, such as the AFCX, for the capture of scam specific information could be utilised for reporting (but not limiting any future innovations). Any authorised business requiring access to the data should be linked via API's to those databases.

Questions on anti-scams strategy obligation

What additional resources would be required for establishing and maintaining an anti-scam strategy?

CSPs should already have existing anti-scam strategies in place as per the Reducing Scam Calls and Scam SMS industry code. Additional obligations under a Framework should not be necessary for the telecommunications sector.

Are there any other processes or reporting requirements the Government should consider?

CSPs already have reporting obligations under the Reducing Scam Calls and Scam SMS industry code. Any additional requirements should be considered only as part of a centralised database within the NASC.

Are there parts of a business's anti-scam strategy that should be made public, for example, commitments to consumers that provides consumers an understanding of their rights?

Educational materials should be public and available for consumers, but any specific anti-scam strategy material should be limited so as not to provide scammers with potential avenues for how to circumvent an organisation's anti scam measures.

How often should businesses be required to review their anti-scam strategies and should this be legislated?

This should not be legislated. It creates an unnecessary regulatory burden on businesses. Businesses should be updating strategies as part of internal processes to ensure they can meet their obligations under a sector specific registered code.

Are there any reasons why the anti-scams strategy should not be signed off by the highest level of governance within a business? If not, what level would be appropriate?

Generally, having a sign off process at the highest levels of a business can cause unnecessary delays. Sign off for any measures such as a regulatory compliance are likely sufficient at an appropriate executive level within a business. Businesses are likely to have differing requirements based on their size, structure and operating procedures.

What level of review and engagement should regulators undertake to support businesses in creating a compliant anti-scam strategy?

As above. Some reviews are also likely to take place at the same time as a scheduled review of any industry code to ensure compliance with obligations are still met.

Questions on information sharing requirements

Information sharing, while an important part of scam mitigation strategies, needs to be carefully considered. In the case of scams, it is not always the case that more is better. Apart from privacy considerations, information relating to potential scams needs to be verified, unique, actionable and timely. Often resources are best utilised in real time actioning and blocking of scams rather than working through an abundance of information to determine if it is new or useful.

Questions on consumer reports, complaints handling and dispute resolution

Should the Government consider establishing compensation caps for EDR mechanisms across different sectors regulated by the Framework? Should these be equal across all sectors and how should they be set?

Compensation should not be a legislated instrument under this type of proposed Framework, nor within an industry specific code. Compensation should be a consideration on a case-by-case basis for a business to determine as they are the ones with a customer relationship. Compensation under a Framework would also be very difficult to determine where, in a potentially sophisticated scam, the liability lies. CSPs for e.g. are unable to know the content of a phone call or SMS and cannot know if it is a scam. They provide a communication, how the details within a communication evolve are unable to be determined.

Caution should also be taken in developing any type of compensation system. This could potentially add another level for scammers to take advantage of, or at the least, provide them with the confidence that if consumers are not in effect 'out of pocket' then the fear of falling prey to a scam creates less of a financial harm.

Questions on sector-specific codes

Are sector-specific obligations, in addition to the overarching obligations in the CCA, appropriate to address the rising issue of scams?

In the telecommunications industry, the success of the Reducing Scam Calls and Scam SMS industry code is already being seen. While the code itself will not solve scams, the obligations being complied with by industry are having a positive effect. The telecommunications industry does not see the need for additional Framework obligations but would support other sectors developing their own codes to address the issues of scams.

Are there additional obligations the Government should consider regarding the individual sector codes?

The Government should seek to ensure that other sectors have appropriate multi factor authorisation and customer authorisation measures in place so that businesses 'know their customer'.



Published by:
**COMMUNICATIONS
ALLIANCE LTD**

Level 25
100 Mount Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507