INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

30 January 2024

Scams Taskforce
Market Conduct and Digital Division
The Treasury

Langton Crescent
Parkes ACT 2600

By submission: https://app.converlens.com/treasury/scams/consultation-industry-codes

RE: Mandatory Industry Codes on Scams

INTRODUCTION

The Internet Association of Australia Ltd (**IAA**) thanks the Treasury for the opportunity to respond to the consultation on the proposed Mandatory Industry Code Framework on Scams (**Framework**).

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized Internet Service Providers (**ISPs**), many of whom also provide other telephony services, and are therefore already subject to the *Reducing Scam Calls and Scam Short Messages Code* that applies to the telecommunications sector (**Telco Scam Code**). Therefore, this response to the consultation is primarily in representation of those members, as well as generally for the public good of the telecommunications sector.

Overall, IAA and our members recognise that the ever-increasing scam activity in Australia is a serious problem and thus welcome this initiative to introduce a multi-sector and multi-stakeholder approach to protect Australia. We equally believe that in order for a legislative framework to be effective, it must be practicable, proportionate and measured. In particular, it is important that legislators and regulators keep in mind the disproportionate difficulties faced by smaller entities in implementing legislative obligations. We also believe that simple and efficient legislation is also in the best interest of consumers who also struggle in understanding their legal rights and remedies available to them. To that end, we are concerned that the proposed Framework may cause some confusion for both industry and consumers.

Furthermore, we appreciate that the Consultation Paper recognises the importance of educating consumers on scams as part of a broader approach to tackle the issue. We understand that as the Consultation Paper is primarily concerned with the legislative Framework to regulate relevant sectors, it predominately focuses on enforcement measures and the obligations on industry. However, we strongly believe that there needs to be greater consideration had by the Treasury and the respective regulators for each sector in raising awareness for both consumers, and industry to address scams. We strongly recommend more investment into undertaking education

campaigns that are tailored to consumers, and industry to ensure the whole-of-ecosystem approach proposed.

OUR RESPONSE

KEY FEATURES

1. ***Does the Framework appropriately address the harm of scams, considering the initial designated sectors and the proposed obligations outlined later in this paper?***
5. ***Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?***
6. ***What future sectors should be designated and brought under the Framework?***

Overall, we understand why the proposed sectors that will be initially subject to the framework have been identified as such and we appreciate the Framework allows for expansion into other sectors in the future as needed. Using this model, basic principles for scam protection and remediation could be set that apply across all sectors in a consistent manner.

However, we also note that the named sectors do not necessarily reflect the scam trends identified in the recent ACCC report[1] wherein the top 5 categories of losses for 2022 were investment, remote access, payment redirection, romance and phishing. This would therefore suggest that sectors that require greater attention is finance more generally, as opposed to banking) and digital platforms more generally, as opposed to digital communications platforms.

2. ***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?***
3. ***Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?***
7. ***What impacts should the Government consider in deciding a final structure of the Framework?***

In general, we understand the rationale of the proposed structure of the Framework in having an overall framework under which there will be sector-specific instruments to implement relevant and tailored obligations for businesses to take actions against scam activity. In principle, we support this approach to the extent that we agree that allowing industry to take part and perhaps drive the drafting of the legislation will result in clearer, more practical and relevant obligations suitable for the industry.

However, while we understand the potential benefits of using of the *Competition and Consumer Act 2010* (**CCA**) as the overarching legislation, we are also concerned that the penalties provided for under the CCA is very large and may be disproportionate, as will be discussed further below. The CCA is also a very dense and complex legislation already and we believe it may be difficult for both industry (particularly smaller entities) and consumers to navigate.

Secondly, we understand that in its current conception, a business will face substantive obligations under at least two legislative instruments. We believe this is confusing for both

[1] https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf

industry who have to comply with their regulatory obligations as well as for consumers who seek to understand what rights and redress are available to them.

An alternative approach could be to develop a new overarching anti-scam legislation (separate to the CCA) which would only contain general and high-level requirements such as the obligation for an entity in a designated sector to take all reasonably practicable steps to prevent, disrupt, respond to and report scam activity. Then the relevant regulator for each sector could work with industry to develop guidance material that sets out the expectations on that sector, while also allowing for some flexibility. In effect, this would operate in a similar way to the Office of Australian Information Commissioner's Australian Privacy Principle Guidelines[2] to provide further information on the Australian Privacy Principles under the *Privacy Act 1988*.

Some of the benefits of the above approach include:

- It would allow flexibility as entities can take steps that are relevant to its business;
- Given the nature of language used in guidelines, this would be more accessible for consumers, and industry;
- This would allow government to keep up with technology changes and other developments as it is easier to amend guidelines than having to go through a formal process to amend legislation.

Given the Telco Scam Code already exists for telecommunications industry, this could be folded in and serve as the basis of the telecommunications sector guidance material, plus other additional mechanisms such as the proposed ecosystem-wide obligations set out in the Consultation Paper.

In any case, regardless of our suggestion, and even if the currently proposed Framework is maintained, we would strongly recommend the development of ancillary guidance material to assist business' compliance with the Framework. Moreover, in order to allow for flexibility, these guidance materials could be drafted and used similar to provide further information and examples on what the government and regulators expect of a business according to its nature, size and maturity.

However, should the proposed Framework be retained, we strongly recommend that as it pertains to the telecommunications industry, the industry code is maintained, as opposed to the drafting of a new standard. Industry is best placed to draft the instrument given its relevant knowledge and understanding. Moreover, as the Telco Scam Code already exists, it will be easier for industry to adopt any new obligations, should they arise, rather than having to familiarise themselves with a new legislative instrument. Accessibility is an important factor that affects effective and meaningful compliance, especially for smaller entities such as many of our members. As such, any regulatory burden should be minimised where it can.

Furthermore, we are not convinced that having a multi-regulator approach would be beneficial for either industry or consumers for reasons that will be discussed below.

---

[2] https://www.oaic.gov.au/__data/assets/pdf_file/0030/40989/app-guidelines-combined-December-2022.pdf

DEFINITIONS

12. ***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?***
13. ***Should the definitions of sectors captured by the Framework be set out in the primary law or in the industry-specific codes?***

The proposed definition for 'telecommunications providers' is too broad and would also capture other entities, including entities that may be covered under the definition of 'digital communications platform', or is otherwise irrelevant for the purposes of prevention of scam activity. For example, as IAA operates internet exchange points, and offers related services such as peering, we are a licensed carrier, and would therefore be subject to the Framework. However the link for which we require the carrier license operates for fundamentally different basis to the standard telephony services that are used for scam activities. As such, the anti-scam measures proposed in the Framework would be irrelevant for our services and systems.

This understanding is already reflected in the Telco Scam Code which has limited the definition of 'carriage service' for the purposes of the Code. We recommend that definition of sectors should be set out in the industry-specific instrument for this purpose.

PRINCIPLES BASED OBLIGATIONS

16. ***Are the obligations set at the right level and are there areas that would benefit from greater specificity e.g., required timeframes for taking a specific action or length of time for scam-related record-keeping?***
17. ***Do the overarching obligations affect or interact with existing businesses objectives or mandates around efficient and safe provision of services to consumers?***
19. ***What changes could businesses be expected to make to meet these obligations, and what would be the estimated regulatory cost associated with these changes?***

We understand and appreciate the intention of the Framework is to be principles-based and allow for flexibility to account for varying business sizes, models and maturity. However, we do not believe this is reflected in the principles set out in the Consultation Paper and overall, they are still too prescriptive in nature. Furthermore, not all the measures may be relevant to an entity or sector. As will be discussed further below with regard to enforcement, this will also result in duplication and overlaps that are not in the best interests of industry, consumers or regulators and government.

Therefore, we recommend that the legislation itself should state broader principles. For example, as it pertains to prevention, we recommend the following:

- *As far as reasonably practicable, an entity must comply with the prevention mechanisms set out in the relevant sector-specific instrument.*

Any actual requirements should be then set out in the sector-specific instrument.

Or, as noted above, rather than having additional legislative instruments, the sector specific material could be dealt with via industry guidelines.

Moreover, in general, we also recommend that references to "all reasonable steps" or "all reasonable actions" should be replaced with "reasonably practicable". This is a clearer term often favoured by industry (so far as telecommunications is concerned).

The regulatory burden faced by industry, in particular, smaller entities in the telecommunications sector would be great. Smaller businesses do not have the resources or capacity to unpack, interpret and implement measures in compliance with complex legislation. Most likely, entities will have to seek external legal advice as most small telecommunications providers are unlikely to have in-house legal personnel.

As such, ensuring the simplicity and clarity of the legislation as much as possible, as well as its proportionality and providing as many necessary carve-outs to ensure the Framework would also ensure higher rates of compliance.

18. ***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?***

We would support the minimisation of any reporting obligations, including a mechanism via which entities can report to multiple agencies, regulators, and/or other relevant persons and bodies simultaneously.

ANTI-SCAMS STRATEGY OBLIGATIONS

20. ***What additional resources would be required for establishing and maintaining an anti-scam strategy?***
21. ***Are there any other processes or reporting requirements the Government should consider?***
23. ***How often should businesses be required to review their anti-scam strategies and should this be legislated?***

While we understand the intent and value of requiring businesses to establish and maintain an anti-scam strategy, we are concerned that the current considerations proposed in the Consultation Paper will result in prescriptive rules that are difficult for industry to meaningfully engage with and implement. Rather than requiring entities to maintain a standalone anti-scam strategy, we recommend that in line with the intent to be principles-based, the requirements allow for flexibility in an entity's approach to its anti-scam strategy. Furthermore, we recommend avoid adding yet another policy that businesses have to develop, which can sometimes become merely a tick-box exercise.

As such a possible alternative could be that an anti-scam strategy could form part of an entity's risk management plan and process. This will allow for an easier process through which entities can meaningfully consider risks associated with scam activity, and their steps to mitigate such risks via a holistic approach. We do not consider it necessary to prescribe specific timeframes for review of an entity's anti-scam strategy. Rather, again, this could be dealt with via guidelines prepared by the government or relevant regulators to set expectations or provide advice on what is a reasonable time for businesses to review their anti-scam activity. We believe annual review would be reasonable, and following major developments or trends in scam activity relevant to the sector.

22. ***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?***

The publication of a business' anti-scam strategy should be voluntary. The types of things that a business should make public in respect its anti-scam efforts should be limited to:

- Contact details for consumers to make reports/complaints in regards to scam activity;
- Recourse available to consumers; and
- Direction to the NASC and other relevant bodies to assist consumers with respect to scams.

24. ***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?***

Requiring sign-off of an anti-scam strategy by the highest level of governance seems to be impractical and inefficient. This would likely result in delays in the creation of an anti-scam strategy and for future iterations of a strategy should they be updated in the wake of a major incident, development or trends in an industry. There may be a lack of knowledge or skill, or other logistical obstacles (such as an update to an anti-scam strategy having to be approved in accordance with board processes) that may make this requirement inefficient. We recommend that the requirement provide that the anti-scams strategy should be developed by persons with the relevant skills, knowledge and/or experience and that it is signed off by senior level personnel, and not necessarily the highest level of governance.

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

The Consultation Paper is unclear as to what the 'review' by the ACCC of an entity's anti-scam strategy, on what basis or frequency and which entities would be subject to having its anti-scam strategy reviewed. We consider reviewing a business' anti-scam strategy would be relevant as part of a broader investigation into a complaint about an entity to ascertain the business' compliance with its anti-scam obligations. However, we do not otherwise see the need for regulators to review each entity's anti-scam strategy. At the most, a similar approach to the recent Critical Infrastructure Risk Management Program Rules could be taken where an annual attestation must be submitted to the regulator confirming a critical infrastructure entity has maintained a risk management program for that financial year. However, this requirement is still relatively new and there is not evidence to support that such a requirement has been effective in ensuring compliance.

As above, we recommend that regulators support businesses by creating guidance material. This should be sector specific with numerous examples for the range of businesses and their structures.

INFORMATION SHARING REQUIREMENTS

26. ***What resources would be required for establishing and maintaining additional information sharing arrangements with other businesses, the NASC and sector-specific regulators under the Framework?***

27. ***What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?***

We support the operation of NASC as a central information hub across the designated sectors. While it is important to ensure segmentation between sectors for some legislative aspects, it is also equally necessary to have cross-sharing of information between the sectors.

As above, we would also support a mechanism in which entities could share information and notify multiple entities and agencies simultaneously for efficiency purposes. However, we agree that it is unlikely to be beneficial nor efficient and practicable to share each individual scam instance, not only across the ecosystem, but also to its respective regulator for an entity. We expect that the regulator for each sector would collate the information to derive findings and trends that should be shared for the sector and with the NASC which can then be further analysed by the NASC and disseminated more broadly, including to consumers.

Furthermore, the government may wish to consider the leveraging of the existing Trusted Information Sharing Networks (**TISN**) administered by the Department of Home Affairs for this purpose. Although the TISN is related to critical infrastructure, there may be some cross-over.

CONSUMER REPORTS, COMPLAINT HANDLING AND DISPUTE RESOLUTION

28. ***What are the limitations or gaps that need to be considered in leveraging existing IDR requirements and EDR schemes for the purposes of this Framework?***
29. ***If the remit for existing EDR schemes is expanded for complaints in relation to this Framework: a) what criteria should be considered in relation to apportioning responsibility across businesses in different sectors? b) how should the different EDR schemes operate to ensure consumers are not referred back and forth? c) what impacts would this have on your business or sector?***

Firstly, we consider that a dispute resolution scheme may not be necessary. The Framework could operate similarly to the operation of the privacy law framework in Australia which does not include a direct dispute resolution scheme, apart from allowing for individuals to make direct complaints to the relevant entity, and to the Office of the Australian Information Commissioner.

Secondly, we are concerned that reliance on the existing respective External Dispute Resolution bodies for each sector will be inefficient, and in the case of digital communication platforms, not possible. In particular, we believe it would cause difficulties for consumers understand which is the appropriate body to which it should complain. For example, customers may be unable to discern which entity is responsible for the scam activity being successful (such as between the telecommunications provider which failed to disrupt a scam SMS or the bank failing to detect a high risk transaction) to then complain to the relevant industry EDR body. Moreover, there may be instances where a complaint should be brought for multiple entities across the eco-system, which would result in a consumer having to bring separate complaints to multiple EDR bodies.

Furthermore, we note it is currently out of the remit of the Telecommunications Industry Ombudsman (**TIO**), to deal with matters related to scam activity despite the existence of the Telco Scam Code. As such, rather than requiring existing EDR bodies to undertake relevant training so that they are adequately equipped to deal with scam-related matters, it may be more efficient and

all-round beneficial to expand the functions of a central body such as the ACCC or NASC to perform dispute resolution functions instead, if such functions are needed.

30. ***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?***
31. ***Does the Framework set out a clear pathway for compensation to consumers if obligations are breached by regulated businesses?***

As noted above, we do not see the need for direct dispute resolution process. Similarly, we also do not support the introduction of a direct right to compensation for consumers for breach of an obligation by a business where the consumer has been the victim of a scam. This is likely to result in vexatious claims as consumers seek to recuperate losses from the business, regardless of the entity's culpability. It is also likely to result in a sharp increase in caseload for EDR bodies that they are unlikely to be prepared for, nor do the existing EDR bodies have the adequate experience to deal with these matters.

We believe that this is an area that requires further consideration with more in-depth consultation prior to introduction alongside the rest of the Framework. In addition, should a compensation scheme be implemented, we recommend that there is an appropriate grace period between the legislation coming into effect and the compensation scheme coming into force to allow both industry as well as EDR bodies time to sufficiently implement their respective obligations under the Framework. Furthermore, compensation should also be necessary in the most egregious instances of non-compliance.

SECTOR SPECIFIC CODES

34. ***Are sector-specific obligations, in addition to the overarching obligations in the CCA, appropriate to address the rising issue of scams?***
38. ***Are the proposed approaches to developing sector-specific codes appropriate, and are there other approaches that could be considered to meet the objectives of the Framework?***

As noted above, the proposed overarching obligations are too prescriptive, and neither are they favourable. We recommend setting out broader principles of prevention, detection and disruption, response and reporting in the overarching legislation, but not necessarily requirements other than provisions that refer to the requirements set out in the sector-specific instruments. Finer details as to the requirements that fall under these principles, tailored to each sector should be contained in the sector-specific instruments. Having multiple sets of obligations contained across different legislative instruments will cause unnecessary confusion and increased regulatory burden. As aforementioned, this would also cause undue confusion and obstacles for consumers seeking redress.

37. ***Are the proposed obligations for the sector-specific codes set at the right level, sufficiently robust, and flexible?***

As it pertains to the telecommunications sector, the Consultation Paper has not outlined any proposed amendments for us to comment at this stage. Given the Telco Scam Code has been in

operation since 2022, (and the 2020 Reducing Scam Calls Code before that) we would support the ACMA in collaboration with industry undertaking a review of the effectiveness and shortcomings of the Telco Scam Code to determine what, if any amendments are required.

OVERSIGHT, ENFORCEMENT AND NON-COMPLIANCE

43. ***How would multi-regulator oversight impact different industries within the scams ecosystem? Are there any risks or additional costs for businesses associated with having multi-regulator oversight for enforcing the Framework?***
44. ***Are there other factors the Government should consider to ensure a consistent enforcement approach?***

We reiterate that multiple layers of legislation and legislative instruments cause unnecessary confusion and complexity, as they will contain different requirements, and would then also necessitate multiple regulators to oversee compliance with the distinct sets of obligation. Thus again, we note that the overarching legislation should not itself prescribe any substantive obligations. Furthermore, the multi-regulator approach would also have an adverse impact on consumers.

In addition, given the broad wording of some of the principle-based obligations, there is likely to be risk of overlap between the overarching obligations, and sector-specific obligations. For example, many of the detection and disruption based obligations are very general such as "A business must seek to detect, block and prevent scams from initiating contact with consumers". The existing obligation under the Telco Scam Code to block a phone number once a scam call is confirmed mirrors the overarching obligation. As such, in cases where an entity breaches its obligations, this would give rise to it being in contravention of multiple requirements, resulting in the involvement of multiple regulators, and also attracting multiple penalties. This seems inefficient, unfair and unnecessarily punitive.

In addition to our above comments that there is a lack of justification as to why the CCA has been identified to be the appropriate overarching legislation for the anti-scam code, we are also concerned that the penalties for non-compliance as set out in the CCA would be too great and disproportionate to the issue at hand. Notwithstanding the fact these penalties represent the maximum amounts, having a two-tiered system of potential penalties across different legislative instruments further heightens our concerns that the penalties a business could potentially face are unnecessarily large.

45. ***Should the penalties for breaches of sector-specific codes, which sit in their respective sector legislation, be equal across all sectors?***

The maximum penalties for breaches across the sector-specific instruments could be equal across the eco-system to ensure harmony. However, different requirements may be more relevant to some sectors more so than others, and have greater importance or function in assisting consumers and/or preventing or disrupting scam activity. Therefore, there may be value in certain obligations attracting higher penalties between different sectors, so long as the maximum penalty for a breach is still the same.

Furthermore, similar to our recommendation regarding consumer redress, we would request that a long grace period be introduced so that entities have time and opportunity to meaningfully

understand the Framework and implement changes in their business to comply with their obligations without incurring penalties for genuine mistakes. During this process, we would expect the relevant regulators closely work with industry to assist with compliance. Having a grace period prior to the penalties coming into effect would also mean entities are comfortable in requesting help without fear that their admission of lack of understanding could be used against them.

Moreover, in general, we are concerned that the approach to opposing scams as set out in the Consultation Paper is focusing heavily on obligations and enforcement. However, we believe that the more effective approach would be to focus on education and awareness, particularly in more vulnerable communities. Given the ever-evolving nature of scams alongside constant developments in technology and the economy, there will always likely be a gap between scam activity trends and legislation. Therefore, we strongly recommend there is a concerted focus across the entire eco-system to educate businesses and consumers on scams.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the proposed proposed Mandatory Industry Code Framework on Scams. We appreciate the work of the Treasury on this matter thus far, and recognise the importance of having a robust anti-scam framework in Australia. To that end, we sincerely look forward to working with the Treasury, regulators, industry, consumer advocates and other relevant stakeholders to ensure the development of a practical, efficient and effective anti-scam framework in Australia.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (IAA) is a member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IX-Australia is a service provided by the Internet Association of Australia to Corporate and Affiliate members. It is the longest running carrier neutral Internet Exchange in Australia. Spanning six states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.

IAA is also a licenced telecommunications carrier, and operates on a not-for-profit basis.

Yours faithfully,

Narelle Clark
Chief Executive Officer
Internet Association of Australia