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

03 October 2024

Scams Taskforce
Market Conduct Division
Treasury

By email: ScamsPolicy@treasury.gov.au

RE: Scams Prevention Framework

INTRODUCTION

The Internet Association of Australia Ltd (**IAA**) thanks the Treasury for the opportunity to respond to the consultation on the proposed legislation concerning the Scams Prevention Framework (**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 anti-scam regulation that applies to the telecommunications sector. 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.

As stated in our response to the consultation held earlier this year, we again express IAA and our members recognition of the ever-increasing scam activity in Australia as a serious problem. However, we reiterate our belief that in order for legislation to be effective, it must be practicable, proportionate and measured. In particular, it is important that legislators and regulators keep in mind the disproportionate burden placed on smaller entities by legislative obligations. Thus, we also believe that simple and efficient legislation is also in the best interest of both entities who seek to comply with their obligations, as well as consumers who struggle in understanding their legal rights and the remedies available to them.

To that end, we are concerned that the proposed Framework may cause some confusion for both industry and consumers. We therefore offer our response in the sincere hope that through meaningful engagement with industry and other stakeholders, we can develop a scam prevention framework that is effective and benefits all Australians.

OUR RESPONSE

PROPOSED LEGISLATION

Does the draft legislation effectively achieve the policy objectives set out in this document?

Does the draft legislation include an appropriate level of detail, noting subordinate legislation can provide more prescriptive obligations?

Are there provisions in the draft legislation that are better suited to subordinate legislation?

Will you face any practical challenges in implementing the obligations in the draft legislation?

Although we support the policy objectives of the draft legislation, we are concerned that it is too prescriptive and will be difficult to comply with. We strongly believe that in order for legislation to be effective, it needs to practicable.

In particular, we are concerned that as the subordinate SPF Codes are yet to be drafted, it will be difficult for entities to comply with the principles-based obligations under the draft legislation. Many of the provisions provide that entities must take "reasonable steps", and without the SPF Codes specifying what is considered 'reasonable' for the purposes of the sector, such provisions are not practicable for entities to comply with. However, simultaneously, there are heavy penalties that may apply for potential non-compliance, thereby creating an unfairly onerous situation for entities.

We especially note that in respect to the telecommunication sector, regulation to combat scams activity already exists and there has been great success in reducing scam calls and SMSes. As such, to introduce a new framework with additional rules places too much burden on entities that provide telecommunications services. In previous consultations, it was suggested that the *C661:2022 Reducing Scam Calls and Scam SMS Code* (**Scam Calls and SMS Code**) would be the designated SPF Code for the telecommunications sector. We seek further clarity on this matter, and would strongly support this approach. However, we believe this would still cause difficulties for the telecommunications sector where the Scam Calls and SMS Code do not provide further rules that align with the SPF Principles, thereby causing further regulatory anxiety for entities.

Moreover, the draft legislation is too broad in capturing all entities that provide a telecommunication service. The legislation should also allow for the SPF Code to set out exceptions for when an entity may not be a "regulated entity" similar to the exceptions provided in subsection 58AD(4).

In general, there are also certain provisions in particular which are too vague or confusing, while others are too onerous. For example, section 58BF makes unclear what sort of information is required from an entity. We appreciate it does not require an entity to make publicly available, all its governance policies, procedures, metrics and targets. However, we recommend some guidance material to specify what sort of information would be required. Whereas only providing an entity 7 days following the financial year for certifying its compliance with its obligations as per proposed paragraph 58BE(1) is too short and onerous on entities. With the end of financial year period already a very busy period, including other regulatory matters that need attending to, we request that this be amended to allow entities 15 business days to make the written certification.

Furthermore, we appreciate that section 58FJ sets out that the legislation does not intend to duplicate the pecuniary penalty that may be imposed on an entity for failing to comply with an obligation that would be an infringement of both the legislation, and subordinate SPF Code. However, to avoid any confusion, we would recommend a note to be included to sections 58CC and 58GC to make this clear.

In addition, while an entity may not be fined twice under multiple civil penalty notices for the same conduct, it seems that under section 58FL, an entity may receive multiple infringement notices for

the same conduct or omission, both from the SPF General Regulator, and the SPF Sector Regulator. We believe that similar to section 58FJ, there should be a provision relating to double jeopardy when it comes to penalties payable under infringement notices.

What would be an appropriate transition period to enable you to implement these changes?

In general, given the comprehensive scale of these changes, we would request a minimum of 6 months before the legislation becomes enforceable. In addition, we would urge government to adopt the compliance enforcement approach taken by the Department of Home Affairs in enforcing reform to the Security of Critical Infrastructure Act in 2022. When the legislation was amended to introduce new sectors to the critical infrastructure framework, for the first 12 months after the legislation taking effect, the government took an educative and awareness raising approach. Importantly, government did not enforce compliance and enforcement provisions, unless in very serious or egregious circumstances involving an entity's contumelious disregard for its obligations. During this period, the Department also heavily engaged with industry to consult on the changes, including conducting sector-specific forums as part of its educative approach. We believe this has been a very helpful approach that has fostered greater trust between industry and government, and assisted entities with their compliance. We would strongly urge the Treasury to work with the SPF General Regulator and SPF Sector Regulators to engage with industry in a similar way, and only use enforcement measures in select circumstances for a 12-month period, given the framework is a similarly large body of regulation.

We also reiterate that without the SPF Codes, the SPF Principles are difficult to implement and comply with and would cause undue regulatory burden on entities as they try to take "reasonable steps" that are not defined in the overarching legislation. As such, at the least, entities should not face penalties for failure to comply with the SPF Principles until the SPF Codes come into effect.

USAGE OF PERSONAL INFORMATION

We are concerned the Scams Prevention Framework will be forcing entities to retain personal information about customers for too long a period under proposed sections 58BG and 58FZ. While we understand that 6 years may be in line with the statute of limitations for civil proceedings in various Australian jurisdictions, we do not think this is appropriate given the implications this would have for individuals' privacy concerns.

The retention of data for unnecessarily long periods is likely to mean entities will be retaining personal information about individuals, long after the individual ceases being a customer of that entity. This will also increase further risk of data breaches due to the large volume of data available, which will only in turn, increase an individual's susceptibility to be targeted for scam activity. This was evidenced following recent wide-scale data breaches where those individuals whose data was included in the breach experienced increased vulnerability to scams.

EXPECTED COMPLIANCE COSTS

Given our broad membership and our members' varying sizes and services, it is difficult for us to provide a monetary figure on the expected costs of compliance. However, we do note the disproportionate burdens that smaller entities will face in implementing these obligations. As noted above, many of IAA's members are smaller telecommunications providers. As such it is often the case that our members do not have personnel dedicated to regulatory affairs, and require

professional legal assistance to comply with these legislative requirements. Especially as the Framework and SPF Code is likely to require entities to change ancillary policies such as privacy and complaints handling policies. This creates undue burden on smaller entities who lack resources to begin with.

Hence, we request that government considers adopting a phased approach, and allow smaller entities a longer timeframe to comply with the Framework and any applicable SPF Code. The thresholds for such an approach can be set out in the SPF Rules, or each SPF Code so that such thresholds are applicable for the various sectors. For the telecommunications sector, we recommend entities with less than 20,000 services in operation be the threshold, noting this is the threshold used in other regulation affecting the sector.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the proposed Scams Prevention Framework. 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 Scams Prevention 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