29th January 2024

Submission to the Consultation Paper on

Scams Mandatory Industry Code

Introduction

Global Echoes are a group of experts from regulatory, policing and technology backgrounds that have significant experience managing the adverse outcomes of scams. We understand the details of the ecosystem at all aspects of the value chain and from the perspective of stakeholders across government, industry, and civil society.

We are pleased to provide a submission to the Government's consultation on a proposed Scams Mandatory Industry Code (Scams Code) and support the principle to initiate a framework to address the escalating impact of scams to the health and wellbeing of our economy, businesses, and communities. Scammers are exploiting the fragmented nature of the current ecosystem to combat scams – and a national coordination of organisations and systems is required to make Australian consumers and businesses less of a target.

Our Global Echoes team enable a new way for the ecosystem to function to addresses the gaps scammers exploit today and importantly empowers consumers, businesses, and communities to regain trust through shared intelligence about scam threats.

This is the "New Speed of Trust" that benefits all Australians in real time.

Our submission aims to provide the Government insights from our many decades of experience from all parts of industry, to enable the implementation of a Scam Code as soon as possible.

Executive Summary

We agree that a national scams mandatory industry code operating as an ecosystem, is critical to reduce the harms from scams and make Australia a less attractive target. We believe that to be successful in its objectives, the Scams Code will need to add the following elements

- Future sectors should include Crypto-currency and Digital Wallet providers as critical participants from the outset.

- Enabling personal identifiable information (PII) sharing for the benefit of ecosystem participants

- Enable a number of specialist providers to participate in the shared intelligence ecosystem – with consideration given to an accreditation to accelerate industry uplift and reduce the risks for Government of delays to intended outcomes.

- Ensure that the Framework design has elements for innovation in prevention and disruption – recognising the current anti-scam initiatives (e.g. website takedowns) are more responsive to known threats.

- Consumers and businesses need a simplified reporting process because today it involves significant effort of days to report to multiple agencies and organisations.

- Consider how existing datasets could be shared with intelligence providers today.

- Include incentives into the Scams Code for good industry performance that enables the objectives of the framework

Overall, we believe that opportunities exist to expand this framework across multiple industry sectors – and acting now is critical to mitigating scams. However, it is acknowledged that the shifts required for industry to adopt new workflows, share information and deploy technology - cannot be underestimated in its complexity, especially in highly regulated, cost-focused and fast-paced environments.

With the openness of the national framework to include innovation solution providers – who are motivated by the same goals to reduce the impact and harm from scams – Australia has the opportunity to be an international leader and innovator in anti-scams and the establishment of trust in the digital economy and among the consumers and businesses participating in their daily consumption of financial, telecommunication, information and other core services.

Framework (Qs 1-7)

Questions 1/5/6.

We support the proposed framework acknowledging it creates the basis for most of the necessary stakeholders to unite against scams. We recommend that the pillar relating to Banks be expanded to include payment providers and other financial services that facilitate payments. There are two key reasons for this approach:

1. This will make it clear who is responsible for their customer; and
2. payments are an intermediated businesses meaning that some banks will rely on other businesses to process payments and some payment providers are business-to-customer (B2C).

Future sectors should also include crypto-currency and digital wallet providers – who already can play a significant role in preventing and responding to scams – including the recovery of funds

It should also be clear that Telco and Digital Communications platforms includes search engines – who can play a critical role in identifying information promoting scams.

Questions 2 and 7.

The framework should recognise the role for other industry players, including civil society, who can provide anti-scam capability to the industries. This may be a critical step to introduce innovation

and reduce delays in implementing new systems and processes in the complex and highly regulated banking and telecommunications environments.

It is important to recognise these types of firms have a core offering that protects consumers and businesses. The Framework might include an accreditation of firms, like the Federal Trusted Digital Identity Framework, to manage the risks associated to this field of work and ensuring that those offering services have been vetted to do so by the Australian Government.

Example: Trusted Digital Identity Framework (TDIF) | aga

https://architecture.digital.gov.au/trusted-digital-identity-framework-tdif-0#:~:text=The%20Trusted%20Digital%20Identity%20Framework%20%28TDIF%29%20is%20an,security%2C%20transparency%2C%20trust%2C%20and%20choice%2C%20to%20achieve%20accreditation

Definitions (Q8)

We support the proposal that scams are specifically defined to help bring into effect the various aspects of the framework. The definition of scam can be aligned to fraud as per the proposal.

However, one addition to indicate the focus on scam activity is consumers and businesses (because they will be the target for personal information or financial losses) as opposed to financial institutions bearing any losses of data or funds.

Principles-based obligations (Q15, 18, 19)

The Framework proposed has a necessary and welcome focus on reporting and compliance to share intelligence. We recommend that a complete end-to-end process design will identify opportunities for prevention and ensure all opportunities for disruption and intervention are assessed, even if they are not currently leveraged today.

Anti-scam Strategy Obligations (Q21)

The implementation of anti-scam strategies will be an integral part of the framework to support consumer trust and corporate accountability. We recommend the government include measures of success as part of the reporting requirements for businesses – that reflect the overall goal of the framework. Strategies should also ensure that data captured enables reporting on the volume and the dollar value of scams.

The benefit for businesses to collect this data is that they could be incentivised by Government to report success as an offset to when perhaps things don't go well. Not only will it enhance a business's reputation reporting on how successful they have been for their customers, for those businesses who don't have that level of reporting, they may be the subject of fines similar to the cybersecurity framework.

Information sharing (Q26 - 29)

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?

We agree that information is a cornerstone of making this framework successful – timely and relevant information is key. Privacy legislation will could be adjusted to enable personal identifiable information (PII) sharing between & across sectors. In addition, for the recipient of any shared

scam intelligence information there would need to be an education campaign for both participants as well as their end consumers on how to interpret the intelligence and act on it.

Mechanisms will be required to enable a recipient business to understand, validate and decide to act on any information. Scams are also a volume-based issue so the information sharing processes should be designed so that scale and repeated issues can be shared across the ecosystem in an actionable way. This is likely to require a standard to be established so intelligence is organised, trusted, and can be educated on what to do next.

27. What safeguards and/or limitations (regulatory, technical, logistical, or administrative) should the Government consider regarding the sharing of information between businesses, the NASC or sector specific regulators?

We agree that safeguards are required to manage information sharing, however a principle of 'share-first' must remain to combat scams. We identify that the largest impediment to businesses and banks sharing intelligence until now has been the concern regarding Privacy Regulations. Sharing of intelligence across the ecosystem comes with risks. It is important that shared intelligence is distributed in a real time fashion however, this cannot come at the compromise of PII data that results in the ecosystem being a target of data breaches and even larger scale of victims.

The government could consider defining information relating to bad actors' activity as being excluded from the privacy legislation thereby ensuring that every consumer's and businesses' information is otherwise kept private and not exchanged unless under consent. However, strong controls are still required as it is acknowledged this information can include stolen or compromised identity credentials of genuine consumers and businesses.

We also recommend that sector specific entities such as the Australian Financial Crimes Exchange (AFCX) who have the benefit of being owned by the largest Australian Banks, are not the only option for that sector to be able to share intelligence and therefore should not be mandated as the sole-provider of such services. Other options will exist for more modern approaches that extends internationally and cross sector for significantly more impact and available sooner to businesses as well as small banking organisations – and connect stakeholders across the banking, telecommunications, and other digital sectors.

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

One of the biggest impediments to the implementation of a shared intelligence ecosystem is that smaller banks have legacy platform environments and very limited access to resources. This is an industry-wide constraint. The design for sharing intelligence needs to be structured in such a way that it is easy to:

- deploy to a range of businesses;
- integrate into existing workflows and operating systems;
- digitise content – as if shared intelligence requires manual and human handling, especially to decide whether to act on it or not, it will fail to have impact on reducing scams due to the time delays, providing scammers an ongoing vulnerability to exploit.

Other intelligence sharing arrangements do exist which are designed for all business sectors and are available for deployment now.

- As Global Echoes, we are a 100% Australian owned platform offering a shared intelligence service.
- This has been successfully tested within a banking context in the last 2 years and identified instances of scams, providing the opportunity to intervene before money or information is lost to bad actors.

We are also aware of other organisations (including successful deployment in Asia across the banking and communications sectors) who would be excellent providers to a shared intelligence ecosystem, and we would welcome the opportunity to share this information with Treasury.

We recommend the Government establish a Scam Intelligence Framework where providers can be accredited to provide scam intelligence services to the industries. We would welcome the opportunity to demonstrate what could be achieved and how this type of open market approach enables technology providers to partner in this field. It also ensures an accredited standard is set by which all businesses in any sector can select a technology partner to assist them to share intelligence. This accreditation is incredibly important given it will no doubt be the subject of attack and therefore may be limited to a set number of players to manage those risks as is done for the Federal Trusted Digital Identity Framework.

Example: Trusted Digital Identity Framework Trusted Digital Identity Framework (TDIF) | aga

https://architecture.digital.gov.au/trusted-digital-identity-framework-tdif-0#:~:text=The%20Trusted%20Digital%20Identity%20Framework%20%28TDIF%29%20is%20an,security%2C%20transparency%2C%20trust%2C%20and%20choice%2C%20to%20achieve%20accreditation

29. Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?

As stated previously, one of the largest impediments to sharing intelligence between parties is that scams necessarily involve sensitive personal data such as identity, address, bank accounts and customer information. The transfer of this data is not possible without taking on significant risks as a business or industry body and the whole ecosystem would become a target for information.

Another impediment is whether a standard will exist as to how “intelligence” is validated and therefore trusted by the receiving party who needs to be able to act on that intelligence.

We recommend 3 things to support the ability to share intelligence and act on it.

1. Define data relating to bad actors and their activity as being excluded from the Privacy Legislation.
2. Introduce as part of the Framework an accreditation of providers that businesses can rely on for the provision of such intelligence. An existing example of this is the Trusted Digital Identity Framework listed above.
3. Education and awareness for consumers on how to interact with financial intelligence to inform their decisions and wider financial literacy

Example: Denmark has a 71% financial literacy rate.
Denmark mandates financial literacy education from age 13 | World Economic Forum (weforum.org)

https://www.weforum.org/videos/denmark-teens-financial-literacy/

Consumer Reporting (Q30-33)

Reporting is an essential part of the framework to create trust and the opportunity for information sharing. Reporting today is focused on consumers as victims of scams reporting to multiple government entities as well as organisations to remedy their situation.

In addition to making these processes much simpler, it is important to emphasise that consumers should also be able to easily share instances they observe or are exposed to that they believe to be a scam -supporting the trust concept introduced in Q26/29 and the critical role for consumers and business as participants in the framework.

With regards to victim reporting – when a consumer or business has to report a scam event, there should be a single data collection point to cover their service provider (bank or communications provider), police and other government bodies (e.g. the Australian Cyber Security Centre). It should also be mandated that the consumers / business reporting scam events are able to receive feedback on the progress and status of their case.

Sector Specific codes (Q34-42)

The concept of sector specific codes does support the need to recognise that each sector's function and operations will require a different level of technology, standards, cooperation between entities and a different set of industry specific issues to solve related to their operations and the community's expectation of them.

Importantly, Global Echoes is confident that appropriate solutions exist which enable small businesses to be able to comply with these new standards. Small and medium businesses represent 95% of business in Australia and have been the target of man in the middle attacks and scams. It is vital that any shared intelligence scheme be able to support and protect them from significant losses that can be difficult to recover from and impact entire communities.

Enforcement / Compliance (Q43-45)

We recognise that implementation and maintenance of this framework, will increase costs to industry and government. However, there is he decreased trusts and costs to the community of continuing to operate in a fragmented system where scammers are able to exploit both businesses and the community of significant wealth is at an unacceptable level. There is strong evidence (e.g. ACMA SMS Code) that scammers will move from where the new code applies to those sectors where it does not apply. We believe the intent to make the code apply to all sectors over time is the method by which we begin to retain more of our economic wealth as a nation, businesses and communities that can be reinvested in our futures.

We recommend consideration is provided to incentives for good performance in industry. The types of incentives that could matter to any business investing to meet this Framework could include:

- tax deductions for the investments made that reach demonstratable outcomes or community benefits
- If an industry fee is applied by Government to cover some of its costs, then a reduction of that fee may apply if the business meets performance objectives e.g. have a strategy (incl external review for effectiveness), reduce customer losses, share information in timely ways, make it easy for consumers, publish timely awareness materials.
- In the same way that Education and Health facilities are rated by the Government on performance, perhaps businesses can be ranked by their level of cyber and scam efforts and outcomes for the community.