Australian Banking Association

SUBMISSION ON SCAMS – MANDATORY INDUSTRY CODES

31 January 2024

Australian Banking Association

Table of Contents

Australian Banking Association

Key Recommendations

The Australian Banking Association (ABA) strongly supports the Government working to 'set clear roles and responsibilities for the Government, regulators, and the private sector in combatting scams'[1]. ABA sees the proposed legislative framework for establishing mandatory industry codes is an important component of the Government's overall scams strategy.

The overarching success measure for the proposed Framework will be whether it improves scams prevention and disruption across the ecosystem of sectors and law enforcement, and creates more accessible and consistent outcomes for consumers.

The banking industry has taken proactive steps to combat scams and protect customers. Most recently, the ABA and COBA jointly announced the Scam-Safe Accord in November 2023. Under the Accord, banks will:

- deliver an $100 million industry-wide confirmation of payee solution to customers
- take action to prevent misuse of bank accounts via identity fraud
- introduce warnings and payment delays to protect customers
- invest in a major expansion of intelligence sharing across the sector, to help to prevent more scams and recover funds for customers faster
- limit payments to high-risk channels to protect customers
- implement an Anti-Scams Strategy

Principles

ABA supports Principles 1 and 2 in the Government's consultation paper, Scams – Mandatory Industry Codes (Consultation Paper):

- A whole-of-ecosystem approach to address scams ensuring 'businesses in key sectors to take a *consistently* proactive approach to stopping scams' (emphasis added); and

- The proposed 'Framework must be flexible and responsive…to future changes in the scams ecosystem'.

ABA supports Principle 3, 'The Framework will complement and leverage existing interrelated regimes, systems and initiatives' where doing so will help to achieve Principles 1 and 2.

ABA supports the proposal in Principle 3 that the legislative framework for scams should be aligned with the Government's cybersecurity strategy. There is a strong nexus between scams and cybersecurity crimes. For example, Australians' personal and financial information may be harvested via a data breach, which enables further scams and fraud. Many online and digital scams are perpetrated by offshore criminal groups, and a significant proportion of scams proceeds go to fund offshore-originated cybercrimes.

Key recommendations

ABA's overarching comment is to consider the interplay between the components of the proposed Framework and whether they can achieve policy intent through consistent implementation efforts,

[1] Page 6 of the Consultation Paper

regulatory oversight and consumer redress where there is a failure to comply with a mandatory code obligation.

ABA's key recommendations are:

- Ensure the proposed Framework establishes a robust takedown mechanism that applies to digital platforms and telcos. When a trusted party (such as a bank or the NASC) reports a scam advertisement, SMS or phone number, the recipient entity should be required to investigate promptly and take down material confirmed to be a scam.

- Ensure the proposed Framework also applies to online marketplaces (which are proposed to be excluded from the definition of 'digital platforms'), crypto platforms and payments service providers on commencement.

- Consider the merits of a single EDR mechanism for scams (which could be a new entity or an existing one) from the perspective of transparency and access for customers, ability to consider all entities that may have contributed to a scam loss, consistency of decision making and ability to respond rapidly to the changing scams environment.

- Consider the relative merits of a single regulator arrangement versus a multi-regulator arrangement as proposed in the Consultation Paper.

- Consider the overall impact to reducing scams and sequencing of additional obligations for banks proposed in the Consultation Paper, such as the introduction of a "freeze switch".

- Specific additions to the Privacy Act and AML/CTF Act reform program to enable cross-sectoral and public-private coordination on reporting and takedowns.

Policy Director contact: Rhonda Luo

Policy Director

About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

Australian Banking Association

Detailed Submission

Key features of the proposed Scams Code Framework

Proposed framework structure

ABA supports the proposed framework structure with overarching framework obligations that are consistent across sectors, and sector-specific codes. This structure:

- clearly sets out how the framework obligations align to the principles of Prevention, Detection and disruption, Response, and Reporting (to Government and other businesses);
- provides an overall level of consistency between sectors; and
- maintains capacity for sector codes to address issues, prevention and disruption actions, and other obligations in a way specific to a sector.

This structure raises questions about whether the dispute resolution and regulator arrangements supporting this Framework would help to achieve Principles 1 and 2 of this Consultation Paper.

Definitions

1. Digital platforms and online marketplaces

ABA is concerned that 'digital platforms' will not include online marketplaces, which is a key transmission mechanism for buy/sell scams (as distinct from consumer disputes about misleading or deceptive practices relating to the sale of goods or services). While the losses for each case of buy/sell scams are lower compared to, for example, investment scams, this category accounts for one of the highest number of cases reported and has significantly eroded consumer trust in online commerce. This approach would leave a significant gap in the Government's ability to act on this type of scams.

2. Definition of scam

ABA agree this definition is key, as industry requires clarity on what we are targeting and therefore measuring.

ABA does not support conflating scams and fraud as proposed. For the banking and payments industry, it is critical to delineate between the scams mandatory code and ePayments Code (which currently deals with genuine typographical errors and unauthorised transactions). Doing so will provide more clarity and certainty to customers about what protections apply, their responsibilities for, eg, keeping passcodes secure, and avenues for dispute resolution. ABA notes that phishing and remote access are included in some Australian scams data, but may be considered to be fraud in countries such as the UK.

As a drafting matter, using a definition of fraud from the Criminal Code in a civil penalty regime will require careful consideration.

3. Other definitions

ABA highlights that different regulatory and legislative regimes have inconsistent definitions of, eg, consumer and small business. ABA seeks clarification from Treasury on the proposed definitions that will be used in this Framework and relevant codes.

Australian Banking Association

Overarching framework obligations

Focus on a reporting and takedown mechanism

ABA strongly advocates for legislation and sector-specific codes to establish a robust mechanism to takedown scam content or transactions. This can be done by building on and bringing together proposed obligations on information sharing, reporting, responding to and taking down scam content, and record keeping.

A robust takedown mechanism is a critical part of reducing the number of scams affecting Australian consumers and businesses, which can help to reduce the number and size of losses to scams. This outcome can also help to make Australia a hard target for scams. An effective takedown mechanism should have a way to minimise fraudulent or malicious reports, or reports made in error.

Specifically, ABA advocates:

- for NASC to leverage existing AFCX technology (in the first instance) to provide takedown reports from trusted parties
- these reports should be actioned promptly, with SLAs in mandatory sector-specific codes or via an operational level mechanism such as an organisation's anti-scams strategies. Acknowledging entities may need to investigate each report, any requirement or SLA should provide for accountability on the timeliness of the investigation and follow up actions
- using the technology platform to provide an audit trail of investigations, outcomes and actions taken
- Treasury considering Privacy Act amendments that may be necessary to support this mechanism

Principles based obligation to ensure effectiveness of scams strategy

ABA notes having an anti-scam strategy is an initiative of the banking industry Scam-Safe Accord. To make this proposed requirement more impactful on aligning and/or lifting scam disruption capability, the legislative framework should ensure entities take an outcome-focused approach to each entity's scams strategy.

ABA agrees that entities should have the ability to consider which aspects of a scam strategy to make public, if any. ABA also asks whether a more principles-based requirement to make public information about particular issues (such as what a customer can expect from an entity when a customer reports being directly impacted by a scam) can achieve a similar outcome.

Other comments

ABA agrees with the proposed obligation to help prevent customers from engaging with scams, noting this should not detract from the principle that customers also have responsibility to pay heed to alerts and warnings, and take steps appropriate in the circumstances to protect themselves. ABA also asks for this obligation to be detailed in sector-specific codes.

Practical and implementation considerations

ABA provides the following questions for consideration.

- Consumers currently receive a large number of communications about scams from private sector organisations, government and other organisations. The proposed obligation to warn

consumers of potential scams or provide information to consumers could result in a larger numbers of consumer communications. ABA asks Treasury to consider the role that NASC can play in aligning warnings to consumers and enhancing the consistency of consumer messages from Government.

- The consultation paper proposes that businesses should have a reporting mechanism for consumers not directly impacted by a scam to report to the business. It would be useful to clarify whether this is seeking to apply to a customer that has directly been targeted by a scam (such as by receiving a scam text, or a scam message on a platform) but did not fall for the scam, or a customer that did not directly receive a scam but has seen a suspicious activity. Some types of reports can have a large number of 'false positives' and divert attention from consumers who have been directly affected and require urgent assistance.
- Also consider practical ways to streamline reporting to NASC, law enforcement and regulators to reduce duplicative reporting.

ABA highlights many of these potential duplications can be streamlined in practice by using technology platforms that create a 'single door' approach for businesses, such as the AFCX.

Sector specific codes: banking

ABA acknowledges the Government's support for the Scam-Safe Accord. Industry has identified the initiatives that, together, will have the most impact on reducing scams from the banking industry perspective. ABA and COBA members are focused on implementing the Accord initiatives over 2024-25.

In this context, ABA welcomes the opportunity to work with Treasury to contribute to the development of sector specific codes. This work can consider the relative impact and sequencing of possible obligations.

Freeze switch and making it easier for customers to report

ABA acknowledge the rationale underpinning this proposal. When a customer realises they have made a payment to a scam, it may take time for a customer to contact their bank so that their bank can contact the receiving bank to seek a return of funds.

A freeze switch can be a useful tool if a customer seeks to stop future payments and otherwise prevent potential misuse or fraudulent activity. This can be the case where a credit or debit card is lost or a card may have been skimmed, and banks already provide functionality to temporarily block a card. Where a customer has authorised a payment (including a payment to a scammer), a freeze switch does not stop or recall the payment that has been made. This is the case for a freeze switch as implemented in an overseas jurisdiction.

ABA also understands a freeze switch is implemented overseas via a range of channels. A small number of banks have provided an in-app function to lock an account, while others require customers to use telephone banking. Many banks require customers to call or visit a bank branch with identity documents in order to reverse an account freeze. Depending on technology capability, freezing an account will have impacts on the customers' day to day banking, including their ability to access funds during the freeze and the risk of missing scheduled payments.

ABA proposes considering if the objectives of this proposal can be met where banks provide other tools or channels for customers to report a scam more efficiently and/or provide a tool for customers to protect their accounts. ABA also asks Treasury to consider the prioritisation of this obligation against other Accord initiatives.

If Treasury proposes to include a stand-alone obligation to make it easier for customers to report, ABA asks Treasury to consider providing more specific minimum requirements. [ABA notes the Telecommunications complaints rules include this form of words, which is currently satisfied by telcos providing a number of channels to report a complaint, similar to existing banking channels.]

Reversing a transaction in 24 hours

The ABA-COBA Scam-Safe Accord includes an initiative for all members to join the Australian Financial Crimes Exchange and the Fraud Reporting Exchange (FRX) to help customers recover money faster. This means scams intelligence can be shared at speed between banks, helping banks prevent more scams and recover funds for customers faster.

The FRX provides a technology platform for banks to send recall requests to other banks. Its key features are:

- Near real-time reporting of fraudulent transactions between member banks
- The ability to, where possible, halt multiple fraudulent transactions taking place as part of the same scam
- Shared intelligence between banks to assist with fraud and loss prevention efforts
- A faster, more streamlined return of funds, where possible
- Secure and tracked communications between member banks within the platform with agreed timeframes, reducing the need for multiple phone calls and emails between banks.

Use of the FRX platform has significantly reduced the time to resolve most scam cases.

It is important to highlight the FRX does not require participating banks to reverse a transaction (that is, return disputed funds) within 24 hours. This is because this timeframe is unlikely to give the receiving bank sufficient time to investigate the disputed transaction(s). Reversing a transaction without an investigation creates material risk of harm to the 'receiving' customer if the 'sending' customer seeking the recall is not entitled to the money.

Instead, ABA proposes that an obligation should refer to acting promptly to investigate and notify a recipient institution rather than reversing a transaction. Consideration can be given to whether a receiving bank should be required to investigate and act on reports. Finally, as a practical matter, ABA proposes that this obligation could refer to SLAs set out in anti-scam strategies or by FRX operating requirements.

Delineation from ePayments Code

ABA reiterates the need to clearly distinguish between the proposed scams mandatory code for banks and the ePayments Code, while also ensuring there are no unintended gaps between the two instruments. These related outcomes are critical to provide clarity to both industry and consumers. This suggests that work on the scams mandatory code and ePayments Code should proceed concurrently.

Sector specific codes: other sectors

In addition to the proposed focus on reporting and takedown of confirmed scam content or transactions (above), ABA asks Treasury to consider requiring other sectors to:

- consider customer vulnerability, noting vulnerability is currently only proposed in the bank specific sector code;

- identify ways to report losses or 'missed' cases to provide transparency on effectiveness of anti-scams measures.

ABA also urges the Government to:

- urgently implement the SMS ID registry including a specific timetable for making the register mandatory; also provide a proposed timetable for expanding the registry to phone numbers;
- bring crypto platforms and payments service providers into this proposed Framework at the same time as banks, telcos and digital platforms. ABA considers that, for specific payments functions, many of the proposed obligations for banks are also relevant and applicable.

Finally, ABA agrees with Treasury's proposal for the superannuation sector to be brought into the Framework in the second phase.

Internal and external dispute resolution

Dispute resolution may be required after the customer and/or the company has taken initial steps to respond to a scam. ABA agrees a critical consideration for customers is that 'dispute resolution should operate coherently across the system […] so that consumers are not referred back and forth between businesses and different EDR schemes'[2] and receive consistent outcomes.

The Consultation Paper proposes the following dispute resolution pathway:

- A customer or user should be able to access the internal dispute resolution (IDR) process of a business subject to the mandatory code Framework, in relation to the business's response to a specific report or general activity. If the business has not met its obligations under the Framework, the business can consider customer redress [in relation to the business].
- If the matter is not resolved through a business's IDR process, a customer or user would be able to access industry specific external dispute resolution (EDR) arrangements. This would be AFCA for banks, the Telecommunications Industry Ombudsman for telecommunications providers, and a potential new ombudsman for digital platforms. The EDR arrangement can consider customer redress to the extent the business has not met its obligations under the Framework.

ABA sees potentially competing considerations in whether the proposed pathway can achieve the objective for dispute resolution to operate coherently across the system. For example, in relation to EDR, a sectoral EDR scheme will have an understanding of the entities in the sector and can consider additional matters that may relate to a scams complaint (such as financial hardship); however there will be difficulties in two or more EDR schemes working together to provide determinations in a way that reflects the role that each business (and a customer) may have played in a scam transaction. Practical considerations include speed of establishment to align with the Framework's commencement.

ABA has identified the following principles that can help to inform the design and operations of the EDR regime:

[2] Page 6 of the Consultation Paper

1. Whole of Ecosystem Application: all sectors in the scam ecosystem must be subject to an EDR mechanism. All industry participants should participate in the scheme in good faith and be incentivised to take actions to prevent and disrupt scams.
2. Accessibility: consistent with the 'no wrong door' approach, it should be clear to the consumer where to go. The process must be easy to navigate and transparent to consumers.
3. Consistency of outcomes and avoid fragmentation: fragmentation of complaints (e.g. between entities or multiple dispute resolution schemes) should be avoided and outcomes should be consistent.
4. Efficiency and effectiveness: an EDR mechanism must facilitate the quick and efficient resolution of disputes.
5. Resourcing and expertise: an EDR mechanism should be appropriately resourced. The mechanism (as a whole) should have subject matter expertise covering all relevant sectors within the ecosystem of a scam, to ensure customer disputes can be considered and assessed accordingly.

Without downplaying the challenges noted earlier, ABA believes there are benefits in having a single EDR scheme for customers to access for scams. For example:

- A 'one stop shop' for scams complaints can improve ease of access for customers.
- A single EDR scheme can provide more consistent outcomes for scam complaints, and can be better placed to consider each sector's responsibility for consumer redress where a relevant business has failed to meet a mandatory code obligation.
    - This outcome can help to incentivise parties to take action to detect, prevent and respond to scams.
- Having one EDR scheme can enhance flexibility to respond to the changing scams environment, including the relative ease of bringing additional sectors into the EDR scheme in the future.

EDR needs to be supported by robust IDR

A success measure for the framework should be whether the framework incentivises scam prevention and disruption, thus leading to a reduction in the number of scams impacting Australian consumers. IDR and EDR can play a role in this success measure if dispute resolution incentivises scam prevention and disruption actions.

A further success measure for IDR processes is how efficiently IDR can resolve customer complaints and limits the cases that need to be escalated to EDR.

ABA is further considering how IDR could work in practice to consider and resolve customer complaints that may relate to two or more companies' actions in an efficient manner. The effectiveness of IDR processes is likely to be influenced by the EDR arrangement and its outcomes.

ABA asks Treasury to also work with industry to consider how IDR can best operate to support efficient EDR arrangements and the objectives of the framework overall.

Specifically, ABA advocates for applying consistent IDR requirements for scams complaints to all sectors including timing requirements and response guidelines. This can be done by including specific obligations in sector-specific mandatory codes, where equivalent sector-specific IDR

obligations do not already exist.[3] Consideration can also be given to the feasibility of introducing mechanisms that could enable over time, businesses to coordinate with other businesses to resolve complaints at the IDR stage.

Regulatory oversight and enforcement

The consultation paper proposes a tiered, multi-regulator model for oversight and enforcement of the proposed Framework. ACCC would have responsibility for oversight and enforcement of obligations set out in legislation as well as systemic or cross-sectoral issues, and ASIC and ACMA respectively having responsibility for oversight and enforcement of sector specific obligations.

Decisions about regulatory oversight and action should be designed to give equal incentives for all sectors to take action on scams, and not create information silos. As such, ABA supports ACCC having responsibility for the governance of the proposed Framework. This responsibility should include alignment across the Framework on prevention, disruption and enforcement priorities.

The enforcement of sector-specific codes and obligations warrants further consideration. ABA agrees that sectoral regulators have a relationship and a more in-depth understanding of the companies in the relevant sector. However, this proposed arrangement could create misalignment between each regulator's regulatory culture and strategy, and the need to provide equal incentives to sectors. ABA also asks Treasury to consider mechanisms to mitigate the risk of duplicative regulatory actions and penalties as between the legislative framework and codes.

[3] Appendix A of the ePayments Code sets out dispute resolution requirements for ePayments Code subscribers that are not Australian Financial Services Licensees, and could provide a model for IDR obligations across sectors.