



NATIONAL AUSTRALIA BANK SUBMISSION

Scams Prevention Framework – exposure
draft legislation

October 2024

Introduction

National Australia Bank (NAB) welcomes the opportunity to respond to the Department of Treasury (Treasury) consultation on the Scams Prevention Framework (SPF) – exposure draft legislation (draft legislation). This submission builds on NAB’s February 2024 submission to the initial Treasury consultation on the establishment of mandatory industry scam codes.

Scams are a global epidemic with devastating impacts on people and society. They are an increasing part of the sophistication of global organised crime working beyond laws, regulation and ethics.

NAB has strongly encouraged the adoption of an ecosystem approach to scams and looks forward to enhanced coordination of Australia’s national response under the proposed SPF. As previously stated, NAB supports the SPF approach of overarching obligations augmented with those for specific sectors.¹

NAB’s response is guided by the divisions of the draft legislation and in particular focuses on the six proposed SPF principles (governance, prevent, detect, report, disrupt and respond). As a member of the Australian Banking Association (ABA), NAB contributed to and supports the ABA’s submission.

Executive Summary

NAB supports the establishment of the SPF and our feedback is focused on how the SPF can best protect consumers from scams while being practical and workable to implement without duplicating existing practices and procedures. NAB’s feedback focuses on how the draft legislation can be enhanced or amended to achieve this outcome.

With the mandatory sector Codes still to be developed, it is critical the legislation offers clear and practical principles that regulators can apply to these sector Codes. The legislative principles should not have requirements that reach beyond the sector specific Code as foreshadowed in the draft explanatory memorandum.² In parts, the legislation feels more heavily weighted towards compliance, oversight and enforcement with the SPF’s obligations. Consideration could be given to whether this approach will achieve the desired collaboration across the ecosystem needed to better prevent scams. There may be a risk that regulated entities adopt a compliance focused approach to the SPF to avoid exposure to civil penalties as opposed to working as an ecosystem to reduce the impact of scams and organised crime on the community.

Principally, NAB urges the definition of actionable intelligence to be amended and made more specific. NAB considers the current draft too broad, creating a significant risk it will not achieve the objective of helping prevent scams. NAB suggests the definition be refined to types of information that a designated entity can use to take tangible action or provide a realistic basis for a decision to prevent a scam. Reporting under the definition could also better utilise existing reporting made to

¹ See NAB submission to Treasury Mandatory Codes Consultation, February 2024

² See 1.25 ‘In some cases, taking reasonable steps to meet one or more of the SPF principles may require a regulated entity to take steps beyond the sector specific obligations set out in an SPF code’.

the Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Australian Financial Crimes Exchanges (AFCX).

In relation to other key issues, NAB:

- Encourages some reporting timeframes to be extended and where possible aligned to comparable regulatory requirements;
- Seeks clarity on the definition of key terms such as a scam and SPF consumer;
- Urges caution on any wholesale requirement to pause or delay payments while the bank investigates a suspected scam given the volume of scams as a portion of the overall payments that NAB processes; and
- Encourages the development of documented guidance or rules for the Australian Financial Complaints Authority (AFCA) – as the proposed external dispute resolution (EDR) scheme for the three initial sectors – regarding how it should interpret and apply the SPF when assessing scam complaints.

Division 1 – Preliminary

NAB seeks further clarity on Subdivision B with respect to regulated entities and regulated services, including whether:

- The draft legislation is intended to capture scheme operators – for example, card schemes or Australian Payments Plus (AP+);
- Email service providers that fail to prevent business email compromise scams are captured; and
- Entities can be regulated under multiple sector codes.

The designation of the banking sector using the definition of an authorised deposit-taking institution (ADI) has the potential to be inconsistent with the Government’s proposed payment service provider (PSP) licensing provisions and liability models in payment services, especially payment initiation. Payment initiation frameworks such as PayTo enable non-ADI entities to connect to the infrastructure for payment initiation. The connected institution is liable for payment initiations it puts in the system. By designating the banking sector via the definition of ADI, banks would be liable for scam activity perpetrated by scammer customers of connected institutions, who hold the customer relationship with the payment initiator. The payer bank is generally obliged to act on the payment initiation of a verified payment agreement. The proposal potentially confuses payment facilitation with banking business.

NAB also suggests the inclusion of an additional consideration in section 58AE – that the Minister must consider other regulation and related laws in terms of effectiveness, regulatory burden and overlapping or conflicting obligations. For example, it is crucial the SPF does not create obligations that could expose banks to breaches of the AML/CTF Act ‘tipping off’ provisions.

Key terms

In relation to the definition of a ‘scam’, further clarity on what will be treated as a single scam event as opposed to multiple scams would also be useful. For example, in circumstances where a scam involves multiple SPF consumers, it is unclear whether this would be one scam, or a scam for every individual SPF consumer.

NAB notes the definition of ‘SPF consumer’ may expose entities to liability with respect to consumers with whom they do not have a contractual or service obligation. For example, a customer of Bank B who is not a NAB customer but who sends a payment that transits through a NAB mule account. It also includes a business with less than 100 employees. While this is a simpler definition than applied for “small business contracts”, it is different to the *Corporations Act 2001* definition, and the lack of consistency has the potential to create confusion. As a general principle, NAB encourages the use of existing small business legislative definitions with an objective over time of reducing the number of these definitions.

As currently drafted, Subdivision E may present challenges for entities that outsource elements of their scam governance, prevention or detection – for example an entity would be accountable for any action or omission of a third party who will not be captured by the legislation or codes. This could be particularly challenging for smaller institutions who may be contractually tied to service providers who will not be subject to the SPF. For example, many smaller institutions have contractual arrangements with third parties to deliver fraud and scam transaction monitoring services. In some circumstances it may be difficult for smaller banks to negotiate changes to contracted services with their provider to ensure compliance with the SPF obligations. It is recommended this be factored into an appropriate implementation or transition period for compliance with the SPF.

Division 2 – Overarching principles of the SPF

1. Governance

Clearer articulation of minimum metrics and targets would help regulated entities understand how to comply with section 58BC. It will also assist senior officers in providing annual certification about SPF governance policies. NAB acknowledges there may be details that are intended to be captured in the sector specific codes for each regulated sector, or the SPF rules.

Certification about SPF governance policies should be annual, but not set at a specific universal date such as 1 July. This recognises not all organisations have the same ‘financial year’ and would allow flexibility for organisations to follow their own financial year reporting cycles in reviewing documents. It would seem unreasonable to have a civil penalty for attesting a document at a different date if that document is otherwise regularly reviewed.

NAB supports publication of information about protecting SPF consumers from scams. However, NAB would welcome greater clarity with respect to the type of information an entity is expected to publish. As previously argued, businesses should not be required to disclose details of the

capabilities and techniques they use to prevent and detect scams, as doing so would provide significant advantages to organised criminals.³ Section 58BF should be more generalised (e.g. add 'key' measures), and 'measures' should be defined to ensure consistency across the ecosystem.

The purpose of section 58BG is unclear. Banks are constantly changing procedures in response to the operating environment, outcomes of dispute resolution proceedings, implementation of new capabilities. It would be difficult to track and retain records of all activities related to the development of these items, and the material benefit of doing so is unclear. NAB notes the suggested period of 'at least six years' is misaligned with obligations in the *Corporations Act* (seven year requirement for financial records). An alternative approach may be for the senior officer to be required to note any material changes to the entity's SPF governance policies, procedures, metrics and targets as part of their annual compliance attestation.

With respect to section 58BH, NAB suggests lengthening the current five-business-day time period for entities to comply with a request. Locating and extracting relevant data from NAB's systems, validating its accuracy, and obtaining the required clearances may not always be possible within that timeframe. The attachment of civil penalties for a failure to achieve the timeframe may create a risk that regulated entities prioritise response over ensuring the information provided is accurate. As an alternative Treasury could instead consider giving discretion on the response period to the general regulator. Alternatively, consideration could also be given to providing a longer response period aligned with other comparable regulatory requirements. For example, section 49(1B) of the AML/CTF Act mandates that any written notice (under s49) provided to a reporting entity must clearly outline the timeframe within which the requested information (for example, additional information regarding a previously submitted suspicious matter report (SMR) from another reporting entity) is to be provided. This timeframe must be no less than 14 days from the date the notice is issued, although some exclusions can apply depending on the circumstances.

2. Prevent

Clarity on the meaning of 'reasonable steps' / 'reasonableness' is required to help regulated entities understand expectations and the standards that need to be met in this subdivision (NAB understands that the sector specific codes will provide more detail). In general, identifying classes of customers that are more likely to fall victim to scams can be challenging, as vulnerability is as much circumstantial as it is demographic. Treasury could consider whether the vulnerability indicators under the Banking Code of Practice may be appropriate to help ensure consistency with existing standards.

Further specificity is needed on what would be required of an entity in making relevant resources accessible to consumers to identify scams and minimise the risk of those consumers becoming victims of scams. With respect to warnings, it may be challenging for a regulated entity to demonstrate that each SPF consumer belonging to a specific class had received a warning. Given the ambiguity in sections 58BJ and BK, NAB encourages more detail in the sector specific codes –

³ See NAB submission to Treasury Mandatory Codes Consultation, February 2024, p.11.

recognising the code provisions should have greater flexibility than primary legislation to account for the evolving scams landscape.

3. Detect

NAB recognises the need for regulated entities to take reasonable steps to detect scams as described in section 58BN. However, the provisions as drafted appear to place an impractical burden on entities to detect every scam. A bank's ability to identify consumers impacted by scams is also limited to the information available to the bank via its systems, data and processes. For example, there are four main ways banks become aware of a scam impacting their customers or accounts:

- A suspicious payment is detected by the bank's systems initiating an investigation leading to the scam being identified;
- A customer realises they have fallen victim to a scam and reports it to their bank;
- Another financial institution identifies a scam payment from their customer to a mule account at another bank (or vice versa) and reports it to the other bank; and
- A third party such as law enforcement provide information that permits a bank to identify previously unreported scam activity.

In cases where a customer is targeted by a scam but suffers no loss or falls victim to a scam but for a variety of reasons chooses not to report it, their bank may never become aware of the scam. It would be desirable if the framework could be amended to recognise that regulated entities can only detect scams where there is a reasonable expectation that it is within their capability to do so.

With respect to section 58BO, NAB suggests extending (1)(b) to 'each class of SPF consumer', given it may not be reasonable to identify each individual consumer, especially as the provision covers potential impact, not just actual impact. NAB also queries what is expected (beyond report, disrupt, and investigate) in relation to these consumers, once they are identified. It may not be possible to contact all SPF consumers, particularly if they do not have a direct customer relationship with the entity or choose to ignore the bank's approach.

4. Report

As noted in NAB's response above, the definition of actionable intelligence is too general. In its current form, there is a significant risk it will not achieve the objective of helping prevent scams. For example, under the current definition, information that customers of a telecommunications company are receiving scam calls from 'an overseas source with a UK accent' would likely create reasonable grounds to suspect a scam is happening, but the information is not 'actionable' in a way that a designated entity could take any practical action in response to it.

NAB recommends narrowing and specifying the types of information that constitute actionable scams intelligence. Specifically, amending section 58AI to focus on what makes information 'actionable'. Actionable intelligence could instead be types of information that a designated entity

can use to take tangible action or provide a realistic basis for a decision. This could be to prevent a scam or otherwise used by the entity to detect, disrupt, investigate and identify scam activity, including intelligence related to criminal actors, and mule profiles/accounts. For example, a telecommunications provider blocking calls from a known scam phone number or a bank blocking payments to a known scam recipient account.

NAB also suggests changes in relation to the requirements on reporting information to SPF regulators. This could include the content of reports, frequency of reporting, and manner in which reports are provided. NAB queries whether the expectation is that entities will forward reports of every scam event reported to them to the regulator – in NAB’s case, this would be thousands of events per year. Across the three sectors to be captured by the SPF the volume of information would be significant and may become self-propagating as designated entities will need to respond to actionable intelligence received, thus generating more reporting.

The draft legislation appears to envisage the SPF regulator as being at the centre of the scams intelligence cycle with responsibilities for receiving and disseminating reports. Such a model will require significant new investment by Government and designated entities in technology and human capital to manage the volume of information exchange that will eventuate. The benefit of this approach is unclear as it largely duplicates existing, proven and mature capabilities such as the AFCX which could be leveraged and expanded to meet SPF requirements.

Banks already report scam events to AUSTRAC via Suspicious Matter Reports, and to the AFCX via data catalogues. NAB encourages Treasury to consider how these existing sources of data might be used, rather than creating an entirely new reporting stream. An alternative could be to give the regulator broad powers to require entities to provide specified types of information to them, rather than being prescriptive about the provision of actionable intelligence to the regulator. Such an approach would empower Government to designate an institution or capability, for example the AFCX Anti-Scams Intelligence Loop, as the conduit for SPF intelligence exchange. It would also allow the regulator to better define the types of intelligence it requires and to refine those definitions over time. This would permit Government and regulators to adapt swiftly and flexibly to changes in the operational environment, the emergence of new technology capabilities and/or new reporting or information needs.

Seeking to align the ‘actionable intelligence’ definition with other comparable regulatory requirements should also be considered. For example, AUSTRAC recently provided guidance to banks and other industries with specific examples of ‘suspicious activity indicators’ associated with scams and fraud, among other criminal activities.⁴ Greater alignment with this definition would help achieve more consistency in regulatory requirements relating to scams.

It is also unclear how sharing information with the regulator under subsection 52BS(3) and 58BU of the exposure draft will interact with existing legislative obligations under section 123 of the *AML/CTF Act* (tipping off). Banks will require specific assurance that the information sharing envisaged is permitted, including that they may lawfully share information related to an ongoing fraud investigation.

⁴ See [Indicators of suspicious activity for the banking sector | AUSTRAC](#)

NAB notes that on receipt of actionable information designated entities must take reasonable steps, within a reasonable time, to identify each SPF consumer who is or could be impacted by the actionable scam intelligence. Entities must also communicate with “each SPF consumer ... who is or could be impacted by the suspected scam”. These provisions will create obligations that will not be practical for banks to comply with. For example, given an SPF consumer may not have a formal customer relationship with an entity it essentially creates an obligation on the entity to communicate with all Australians (whether living in Australia or living outside Australia given the unclear extra-territorial provisions).

Other areas where clarification would be useful include:

- The level of certainty required for an entity to report actionable intelligence to the regulator (there are some inconsistencies in section 58BS(3) which may impact the information entities believe they have to provide).
- How information will be stored and retained by the regulator (given the need for security of the types of information requested), and whether the information would be subject to freedom of information (FOI) requests or personal information access requests.
- If a customer is the source of the actionable intelligence and does not want the bank to disclose information about the scam.
- If an entity is in a joint operation with a law enforcement agency and for operational security reasons is unable to disclose the information.
- How privacy considerations will be managed.
- How demographical information could be de-identified if the scam victim is identified (s58BS(2) Note 2).
- The purpose for which the regulator is collecting personal information (noting it cannot share this information under section 58BU).

Given that SPF entities only have to ‘suspect’ scam activity, there is also a high potential for incorrect (or even malicious) information to be inadvertently provided to the SPF regulator. As has been experienced with AML/CTF requirements, ‘defensive SMR filing’ has been a frustration for regulators and law enforcement who have argued that a very small percentage of SMRs filed contain actionable intelligence. Reporting by regulated entities is often driven by a compliance culture where it is safer to report information regardless of its probative value to avoid any risk of exposure to criminal or civil penalties.

The legislation should also ensure that only necessary personal information is collected by the SPF regulator, especially where it is collected without the consent of a person engaged or attempted to be engaged in the scam, who is identifiable in the report. There is the potential by describing a scam, additional personal information or sensitive information will be disclosed (e.g. sexual preference in a romance scam). An alternative could be to restrict collection of personal information about alleged victims to complaints to EDR schemes about the SPF entity’s conduct. Legislation should also cover personal information retention periods and potential deletion of personal information after a period of time, given the nature of the information.

5. Disrupt

In general, further clarity is requested on how these provisions interact with AML/CTF Act tipping off provisions including whether regulated entities can share information with each other when disrupting scams.

On the obligation to take reasonable steps to disrupt scams, the suggestion that ‘it may be appropriate to pause or delay payments while the bank investigates the suspected scam’ could have a disproportionate impact on legitimate payments. For context, scam payments comprise a small proportion of the overall volume of payments processed by NAB and other banks. Placing banks in a position where they must disrupt all payments of a certain type in response to an emerging scam typology seems a disproportionate requirement. This could have adverse consequences across the Australian economy due to the blocking of a large number of legitimate payments. To prevent this, the requirement could instead be for banks to act proportionately and in a timely manner to implement effective responses when scam trends or threats emerge. For example, over the last 12 months NAB’s real time payment alerts have resulted in \$171 million in potential scam payments being abandoned by customers. These alerts are carefully targeted to avoid warning fatigue with about one per cent of NAB’s digital payments triggering an alert.

Consideration should also be given to the level of responsibility expected of consumers to minimise the risk of scams. For example, where a bank has provided a customer with a warning (such as a real time payment alert or telephone warning) that they may be caught in a scam, and the customer ignores the warning and makes the payment, the bank should not be liable for any loss that occurs. NAB encourages the legislation to include basic obligations for SPF consumers who are a critical component of the scams ecosystem and should be required to conduct their financial affairs to a reasonable standard of prudence and due diligence. NAB also seeks to understand if the threshold for ‘sufficient’ information would be assessed at an individual or general level. NAB has a duty to act on customer instructions (the customer mandate) but if compliance with the SPF requires NAB on occasion to disregard this mandate, it would be useful to have legislative protection against a claim customers could make arising from not acting on their instructions.

With respect to sharing information about scams, the form of disclosure and types of information to be disclosed to SPF consumers will be crucial. Further clarity is required on whether this obligation would be met by an entity posting regular updates on its website. For example, that NAB has observed an increase in a particular type of scam, how they typically present, the red flags to be aware of, what consumers can do to protect themselves, and what they must do if they think they’ve fallen victim to the scam.

NAB welcomes the 28-day safe harbour period. However, the provision assumes banks will have sufficient information available to them to form a suspicion an event is a scam and enable a report to be made within the 28 days. This is often not the case as scams can occur over a long period of time (for example romance and investment scams) and investigation periods can be lengthy due to limited access to information, uncooperative parties and sophisticated methodologies used by the criminals. It may take longer than 28 days for an entity to realise an activity is not a scam, but the actions taken to that point would have still been taken in good faith. NAB notes that the safe harbour

provisions only apply while a scam is being investigated and ceases once the regulated entity confirms the activity or event is a scam. This is impractical as the period after a scam is confirmed is crucial as this is when banks need to move swiftly to disrupt the activity, for example blocking payments and freezing recipient accounts. NAB recommends the safe harbour provisions be amended and extended to include actions taken after a scam is confirmed.

If these provisions are enacted, they will in large part duplicate information already available via AFCX and AUSTRAC. It is also unclear who will have access to the information, whether it will be subject to FOI requests, and whether the regulator might publish reports using this information. NAB also queries the need for section 58BX(5)(c), which imposes obligations on an entity relating to activities that the entity does not think is a scam.

Similar to 58BO, NAB seeks to understand how it is envisaged an entity will communicate with a SPF consumer that it does not have a direct customer relationship with. Further clarity is also sought on the reporting requirements outlined in section 58BR versus section 58BX. Based on the differing requirements presented in the draft legislation, NAB's interpretation is that reporting requirements in 58BR are separate and distinct from those in 58BX.

With respect to 1.173 in the explanatory memorandum, 'confirmation of payee' (CoP) will prevent loss only when the customer uses the CoP response to decide to not take an action to proceed (for example, a name mismatch results in the customer ceasing). CoP will not intervene in the payment process, rather it will provide the customer with information regarding the intended recipient account to support the payment decision. Customers will be able to disregard the information offered by CoP and proceed to make a payment. NAB seeks guidance on whether presenting a customer with the CoP result would satisfy the Disrupt principle in Subdivision F (58BV to 58BZ) even if the customer proceeds with a payment that is later discovered to be a scam. NAB suggests that in the Code or any consideration of liability, that liability on reporting entities could be diminished if SPF consumers do not act with prudence or diligence (such as by ignoring scam warnings or alerts).

Similarly, in 1.174 on taking reasonable steps to disrupt scam activity includes introducing "holds to payments to enable the regulated entity to contact the consumer and provide them with information that the account they are making a payment to has been identified as associated with scam activity." Further clarity would be welcome on how this would provision would interact with AML/CTF tipping off provisions.

6. Respond

NAB believes that any code obligations with respect to internal dispute resolution (IDR) should be aligned with obligations in the Australian Securities and Investment Commission's (ASIC) Regulatory Guide 271.

The proposed framework contains no provision for apportioning scam loss liability across sectors or across regulated entities within a sector. To achieve the best outcomes for SPF consumers the framework should include a mechanism for joining additional involved parties at the IDR stage of a

scam complaint. For example, if a NAB customer falls victim to an investment scam advertised on a digital platform and as a result sent a payment from their NAB account to a mule account at Bank B, there should be a mechanism for NAB to join the digital platform and Bank B to the IDR process. In the absence of such a mechanism the volume of matters moving to EDR will increase significantly requiring proportionate additional investment in the EDR authority and delaying outcomes for SPF consumers.

Further guidance is also sought on how multi-party complaints will be considered at EDR, including principles or guidance on liability apportionment across designated sectors for a single complaint.

Division 3 – Sector-specific codes for the SPF

This division should include detail on sector consultation and minimum times before a Code can take effect. NAB considers that 28-days be the standard consultation period required by the regulator for the Code to be established or then amended. A provision for a shorter period, such as five business days, could be stipulated for rare occasions where the regulator outlines that more urgent changes are required.

Division 4 – External dispute resolution for the SPF

NAB notes it is unclear whether guidance will be provided to how EDR schemes will approach complaints. For example, will the focus of AFCA in considering a complaint be confined to whether there has been a breach of the SPF principles / SPF Code, or could AFCA still determine that a bank is liable to compensate a scam victim based on other principles even if there is no breach of an SPF obligation.

To ensure that AFCA's determinations are consistent between complaints and aligned to the intent of the exposure draft, NAB recommends AFCA, and any other future EDR scheme, be subject to clearly articulated rules regarding how they should interpret and apply the SPF when assessing scam complaints. AFCA's current approach includes the application of a 'fairness' construct to scam complaints that can lead to inconsistent outcomes for similar cases. While AFCA is not currently bound by precedent, NAB would encourage a clear set of rules to be established so outcomes can be predicted with greater confidence. A clear set of rules and possibly publishing novel or key determinations (anonymised) would likely make the EDR process more efficient and effective. This could be supported by AFCA publishing guidance on how it will determine scam complaints within the confines of these rules as it has done for other topics (such as responsible lending). Such an approach would encourage and support faster decision making at the IDR stage, reducing the volume of matters proceeding to EDR and contribute to better SPF consumer outcomes. Facilitating faster IDR and EDR outcomes in relation to scams is critical, as consumers who have lost money may find themselves in financial difficulty while waiting for complaint processes to be completed.

Division 5 – Regulating the SPF

NAB notes regulators can share information or documents in their possession with other regulators. NAB encourages further detail be stipulated on whether this is limited to information received from regulated entities under the SPF, or if it is envisaged the information could have been received

outside the SPF, but still relevant (NAB would suggest it should be limited to the former). Clarity on whether these documents are subject to FOI requests would also be welcome.

Division 6 – Enforcing the SPF

The draft legislation does not expressly provide for how liability might be apportioned in the event multiple regulated entities are ‘involved’ in the same contravention. This should be addressed in the legislation or the SPF rules.

Conclusion

Thank you for the opportunity to provide comments on the draft legislation. NAB would be happy to discuss any aspect of this submission with Treasury.