



Australian Banking
Association



Scams Prevention Framework – Exposure Draft Legislation

Submission of the Australian Banking Association

4 October 2024

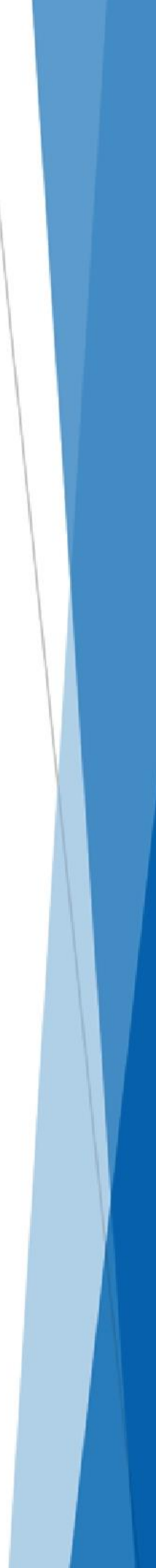


Table of Contents

1.0	Overview	2
1.1	Introductory comments	2
1.2	Themes of the submission	2
1.3	About the ABA	3
2.0	Key Recommendations	4
3.0	Detailed discussion	6
3.1	Key recommendations	6
3.1.1	Clarify the interaction between the Industry Codes and SPF Principles	6
3.1.2	Establish liability rules and clarify apportionment in IDR and EDR	10
3.1.3	Ensure data-sharing arrangements are appropriately prioritised to maximise impact	13
3.1.4	Clarify key definitions to ensure the regime operates as intended	15
3.2	Additional recommendations	18
3.2.1	Approval of Codes	18
3.2.2	Extra-territorial scope	19
3.2.3	Action for damages and potential class action risk	20
3.2.4	Interaction with other regulatory obligations	20
3.2.5	Safe harbour	22
3.2.6	Receiving Bank obligations	23

1.0 Overview

1.1 Introductory comments

The Australian Banking Association (**ABA**) welcomes the opportunity to provide a submission to the Treasury's consultation *Scam Prevention Framework – Exposure Draft Legislation (the exposure draft)*.

The ABA welcomes the exposure draft and supports key elements of the proposed framework, including the whole-of-ecosystem approach to combatting scams, sector-specific mandatory scams codes (**Industry Code** or **Codes**), and the stated intention to establish a single external dispute resolution (**EDR**) scheme for scams.

To effectively combat scams and their growing sophistication, it is essential to address the entire scam ecosystem by ensuring that financial institutions, telecommunications providers, digital platforms, and government agencies all play an active role in providing a coordinated defence against scammers. Preventing scams will require coordinated efforts to stop scams at the source before they reach consumers. By clearly defining responsibilities and fostering collaboration, this approach strengthens preventative measures and can help to reduce the overall impact of scams on the community.

The approach outlined in the exposure draft will build on proactive measures being taken by the banking industry against scams. The Scam-Safe Accord represents the banking industry's commitment to protecting customers from scams across the entire sector.¹ Through this industry-wide collaboration, banks are adding greater friction to payments, enhancing detection systems and sharing intelligence to help protect customers.

1.2 Themes of the submission

A key theme of this submission is the need to strike the right balance between compliance and effectiveness and ensuring that measures are clear and appropriately tailored to each industry. The proposed legislation introduces substantial new compliance obligations. However, in some cases, there is no assurance that these requirements would effectively reduce scams. In addition, the breadth of certain terms and compliance requirements may create uncertainty that could hinder large-scale investment aimed at preventing and detecting scams.

We understand that the Australian Government has sought to craft principles-based legislation that is broadly applicable across the entire ecosystem, each sector of which contains vastly different issues. In our view, this could be better accomplished by greater use of the Codes, which should be targeted for each sector. The primary legislation would remain principles-based as an enabling framework, with more detail on application to specific sectors contained in regulatory instruments and complemented by clear liability rules and an apportionment mechanism established by the Minister.

¹ <https://www.ausbanking.org.au/scam-safe-accord/>



Australian Banking
Association

1.3 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.

Policy Director Contact:

Chris Taylor (Chief of Policy) chris.taylor@ausbanking.org.au

Merric Foley (Policy Director) merric.foley@ausbanking.org.au

2.0 Key Recommendations

This submission provides several recommended amendments to the exposure draft that would further strengthen the proposed framework. Notwithstanding our broader comments outlined in the body of this submission, we wish to highlight four key recommendations:

1. Clarify the interaction of the Codes and Scam Prevention Framework (SPF) Principles.

- The exposure draft be amended to clarify that the SPF Principles function as obligations for Code development, rather than as obligations directly imposed on regulated entities (**REs**).
- As the Principles are overarching obligations within the *Competition and Consumer Act 2010 (CCA)*, the exposure draft be amended to provide that only systemic breaches of the Act are considered, and civil penalties would apply in relation to systemic breaches (rather than individual breaches).

2. Establish liability rules and clarify apportionment in internal and external dispute resolution.

- The exposure draft be amended to:
 - i. Provide a Ministerial power to establish clear liability rules and a mechanism for apportionment in regulations, which applies at both internal dispute resolution (**IDR**) and external dispute resolution (**EDR**), including rules for joining parties. This will be crucial in ensuring consistent outcomes for consumers and providing REs with clarity on their obligations.
 - ii. Require the Minister to establish rules directing how the single EDR mechanism should deal with scams referred to it both as a matter of process (how it will bring other parties in to a complaint) and as a matter of substance (to confirm that when it is making its determinations as to whether an RE should compensate a SPF consumer, it will focus on whether there has been a breach of a liability rule, rather than considering a wider range of factors under its fairness jurisdiction).
 - iii. Clarify that the Australian Financial Complaint's Authority (**AFCA**) fairness jurisdiction does not apply to scams disputes referred to it. This clarity will help to provide consistent outcomes for consumers and ensure that regulated entities are clear on the measures they need to implement to protect consumers.

3. Ensure data-sharing arrangements are appropriately prioritised to maximise impact

- The exposure draft be amended to remove prescription regarding the provision of actionable scam intelligence to the SPF general regulator, but instead give the Minister broad powers to set out specified types of information to be shared and whether this information is to be provided to the regulator or a third party. This would allow the Minister to designate the types of information to be shared, potentially through real-time reporting from an institution such as the Australian Financial Crimes Exchange (**AFCX**) and to refine those arrangements over time. This will help to encourage timeliness of information-sharing and, importantly action taken in relation to reported information, as well as minimising duplication by leveraging existing information-sharing mechanisms.



4. Clarify key definitions to ensure the regime operates as intended

- The exposure draft be amended to more closely align with the policy intent, and to remove unintended breadth, including:
 - i. **SPF consumer:** Remove the text “or may be” and “or purportedly provided”, and instead explicitly deal with any categories of scam (eg. impersonation or phishing scams) that those provisions are intended to capture. Likewise, consider the application of the text “indirectly” providing a service.
 - ii. **Small business:** Align the small business test with the provisions in the unfair contract terms (**UCT**) provisions with the exception that the limbs be cumulative (that is, that both the headcount and turnover limb be applied).

3.0 Detailed discussion

3.1 Key recommendations

3.1.1 Clarify the interaction between the Industry Codes and SPF Principles

The exposure draft envisages that the SPF Principles will apply in full to designated sectors (and their REs), and that SPF Principles 1, 2, 3, 5 and 6 may be further developed in the Codes.² Therefore, the exposure draft currently envisages that obligations imposed by the sector-specific SPF codes (**the Codes**) and the SPF Principles will apply concurrently and that Codes will not address SPF Principle 4.³ Further, the exposure draft intends that compliance with Code obligations will not automatically entail compliance with the SPF Principles.⁴

The ABA understands that the intention of the SPF Framework is to create broad-based obligations for REs to flexibly and proactively respond to the evolving scams environment and newly emerging scams typologies that may not necessarily be captured by the more prescriptive Codes.

Our concern is that the SPF Principles are broad and make repeated reference to criteria of “reasonableness”,⁵ which is not defined. In practice, the SPF Principles would function as additional obligations that are determined by a complaint authority or a court. This poses several issues:

- There is no certainty that determinations of reasonableness will be effective, appropriate or proportionate to combatting scams.⁶
- REs may be entirely compliant with Code obligations but still face the prospect of being found to have breached the broader SPF Principles.
- As the SPF Principles are contained in primary legislation, amending them (for example, to respond to the evolving scams environment) will require new legislation.
- An environment in which reasonableness is determined on a case-by-case basis will not provide sufficient certainty on which to base long-term investment decisions in anti-scams capability. The industry-led Scam-Safe Accord provides a strong example where clearly defined obligations have underpinned substantial ongoing investment in anti-scams measures across the banking sector. Industry actions were possible because of the certainty provided by collaborative discussion and agreement on the key priorities for combatting scams.

² Per section 58CC(1)(b).

³ Instead, Principle 4 will be elaborated in a separate notifiable instrument. We make further comments regarding reporting requirements in the body of this submission. See **3.1.3 Ensure data-sharing arrangements are appropriately prioritised to maximise impact**, page 13

⁴ Draft Explanatory Memorandum, paragraph 1.214

⁵ For example, 58BJ, 58GN and 58BW refer to “reasonable steps” to prevent, detect and disrupt scams, while 58BK and 58BO refer to “reasonable steps” to identify SPF consumers.

⁶ As the regime intends to cover entities of all sizes and resourcing capabilities, it is particularly important to ensure that anti-scams measures are targeted towards the most effective interventions.

Below, we outlined three options that we view could resolve the above concern:

1. Amend the exposure draft to re-formulate the SPF Principles as normative principles that inform the development of the Codes but do not themselves impose separate obligations.
2. Amend the exposure draft so that compliance with an Industry Code is taken to be compliance with the relevant SPF Principle.
3. Amend the civil penalty provisions so that they apply only for systemic and/or egregious breaches of relevant Code or SPF Principle, but not for breaches in individual cases.

Should the Treasury adopt Approach 1 or 2, we further recommend that Approach 3 be adopted as a complementary set of measures.

Approach 1: Re-formulate the SPF Principles as normative principles

Under this proposed approach, the SPF Principles would be re-formulated as normative principles for Code development (aligned to prevention, detection, disruption, etc.), rather than as obligations imposed on REs. Each Code would need to align with the SPF Principles, but the SPF Principles themselves would not form a separate set of obligations directly applicable to REs.

In other words, the CCA would set the overarching SPF Principles. The Codes would be specific to each industry and align with the SPF Principles. The Codes would be supplemented by liability rules (including a mechanism to apportion liability), established in regulation by the Minister, to provide consistency and legally enforceable rules across each sector. Civil penalty provisions would apply for systemic and/or egregious breaches of the relevant Code.

The Codes would be drafted to provide sufficient flexibility to account for the evolving scams landscape and ensure appropriate action is being taken by each sector. To meet the Government's expectations of flexibility, the Codes could themselves incorporate and define broader concepts of reasonableness. Being in subordinate rather than primary legislation, these would be easier to evolve. An additional requirement for regular reviews would have the advantage of providing a platform for whole-of-industry collaboration in identifying common concerns.

Approach 2: Compliance with the Code taken to mean compliance with the SPF Principles

Under this proposed approach, the primary legislation would state that RE compliance with a Code is taken to mean compliance with the relevant aspect of the Principle to which the Code relates.

For example, if an SPF Principle states that an RE must take 'reasonable steps', the Code sets out ten steps that need to be taken and the RE complies with them, then the requirement in the Principle is met. The RE may choose to take additional action over and above the Code requirements but they will be taken to have met the Principle if they meet the requirements in the Code.

The primary legislation should also clarify, for the avoidance of doubt, that a breach of an obligation under a Code does not automatically mean that an SPF Principle has been breached and require a causal link between the loss and the relevant SPF Principle.

Taking the same example above: if an RE failed to take one out of the listed ten steps but instead undertook five other steps which the RE considers, assessed objectively, mean that

the same or a better outcome was achieved, the failure to take the one step would not mean that the Principle had been breached.

Approach 3: Operation of civil penalties at the systemic level

Many of the SPF Principles rely on the definition of “scam” and “actionable scam intelligence” that are drafted at the individual scam and individual customer level. As a result, civil penalties could potentially apply in relation to each individual consumer and individual instance they are impacted by a scam.

For example, the SPF Principles provide that an RE will contravene a civil penalty provision if it fails to take reasonable steps to prevent another person committing a scam,⁷ detect a scam relating to its regulated services,⁸ or disrupt a scam or suspected scam relating to actionable scam intelligence and prevent loss or harm arising from such a scam or suspected scam.⁹

Further, for each individual instance of a scam, multiple penalties may apply for each SPF Principle. Cumulatively, this could lead to significant civil penalties. Given the severity of the civil penalties proposed, we consider that a better approach would be to:

- Retain civil penalties only for egregious or systemic Code breaches, and
- Include a non-exhaustive list of matters that should be considered in determining the pecuniary penalty, for example the nature and extent of any loss or damage suffered because of the contravention. Section 1317G(6) of the *Corporations Act* could be drawn upon in drafting this list.

Recommendations

Note: Below, the ABA has provided two sets of recommendations for consideration. The first set involve amendments to individual SPF Principles to cover the issues raised above. However, noting Government’s intention to proceed with Parliamentary introduction this calendar year, we have also proposed an alternative approach which we believe would involve fewer amendments but which would ensure that the SPF Principles operate only at a systemic level, and that civil penalties only apply to systemic failures.

Amendments to the SPF Principles:

- **Approach 1:** The exposure draft be amended so that the SPF Principles do not constitute obligations in their own right but as normative principles informing Code development. The Codes should implement the obligations set out in the SPF Principles and compliance with the relevant industry Codes should be taken to be compliance with the Principles. One way this could be effected is to redraft each of Principles 1 to 6 so that they are not framed as direct obligations that are currently “a regulated entity contravenes this subsection if the

⁷ Section 58BJ(1)

⁸ Section 58BN(1)

⁹ Section 58BW(1)



entity...” but rather are framed as enabling obligations such as “The SPF Code must set out obligations on regulated entities to...”

- **Approach 2:** The exposure draft be amended so that (i) compliance with a Code is compliance with the aspect of the related Principle and (ii) non-compliance with a Code is not an automatic breach of a Principle. One way in which this could be effected is:

- (i) taking the civil penalty provision in section 58BJ as an example, to include a new section or sub-section to the effect:

“If a SPF code for a regulated sector includes sector-specific details about what are reasonable steps for the purposes of subsection 58BJ(1), and a regulated entity in that sector complies with those reasonable steps, that regulated entity cannot be found to have contravened subsection 58BJ(1).”

Equivalent language would be included for the other civil penalty provisions in Division 2. Or a more general statement to the effect above could be included in section 58CC(1); and

- (ii) again taking the civil penalty provision in section 58BJ as an example, to include a new section or sub-section to the effect:

“If a SPF code for a regulated sector includes sector-specific details about what are reasonable steps for the purposes of subsection 58BJ(1), the Court will have regard to those details in the SPF code when assessing whether there has been a contravention of subsection 58BJ(1), however the fact that the regulated entity has not undertaken all those reasonable steps does not require a conclusion that subsection 58BJ(1) has been contravened.”

Equivalent language would be included for the other civil penalty provisions in Division 2. Alternatively, a more general statement to the effect above could be included in section 58CC(1).

Amendments to ensure the SPF Principles operate at a systemic level:

- **Approach 3:** The exposure draft be amended so that only egregious or systemic breaches attract civil penalties. One way in which this could be achieved is through the introduction into Division 6, Subdivision C, of a provision in similar terms to s 1317G(1) of the *Corporations Act 2001* (Cth) (and adopted in a range of other legislation).¹⁰ For example, that provision could state that:

A Court may order a person to pay to the Commonwealth a pecuniary penalty in relation to the contravention of a civil penalty provision of an SPF principle, or a civil penalty provision of an SPF code, if the contravention of the civil penalty provision:

- *is serious; or*

¹⁰ For example, s 196(4) of the *Superannuation Industry (Supervision) Act 1993* (Cth).

- *materially prejudices the interests of a significant number of SPF consumers.*

- The exposure draft be amended to include a non-exhaustive list of matters that should be considered in determining the pecuniary penalty, for example the nature and extent of any loss or damage suffered because of the contravention. Section 1317G(6) of the *Corporations Act* could be drawn upon in drafting this list.

3.1.2 Establish liability rules and clarify apportionment in IDR and EDR

The ABA supports the single-body EDR model envisaged in the exposure draft, noting that the challenges of taking on this whole-of-ecosystem role will require the single body to be appropriately resourced and skilled. As noted in our earlier submissions, it will help ensure that consumers know where to direct their complaint if they are unhappy with an IDR outcome. It will lead to quicker and more predictable outcomes that will benefit consumers, hold all ecosystem participants to consistent standards, and enhance the regime's economy-wide impact.

We note the significant complexity of IDR arrangements, and we consider that amendments are required to ensure both IDR and EDR function effectively.

Liability rules and a mechanism for liability apportionment is required

Notwithstanding the practical operational implications associated with IDR, the proposed framework contains no mechanism for apportioning liability across sectors or across REs within the same industry segment and it contains no express power to join an external party at IDR stage. The lack of these mechanisms will severely hamper the ability of an IDR process to adjudicate and allocate liability across all REs that have contributed to or caused the scam loss.¹¹ This will significantly impact the effectiveness of IDR and likely result in more cases being referred to EDR.

Example: a customer initiates an IDR process with their bank regarding a scam loss. On examination, the bank identifies that the scam originated from a digital platform that, as reported via intelligence to the Anti-Scam Intel Loop, may not have taken appropriate actions in line with their Code requirements to disrupt the activity that led to the scam. As the bank has no ability to join a third party to the dispute, the customer may only receive an offer for only a proportion of their entitled compensation.

In that instance, the bank would be in a position of resolving the case internally and may either:

- i. If the bank identifies that it has failed to comply with its relevant Code requirements:
 - a. Pay 100% of the scam loss irrespective of the liability of other REs; or
 - b. Offer the customer only the portion of the compensation that it estimates is attributable to its own actions and referring the customer to the digital platform or EDR for the remainder.

¹¹ Similar concerns exist with respect to other matters regarding liability apportionment, including evaluation of contributory SPF consumer liability, use of RE branding by fraudsters, and so on.

- ii. If the bank identifies that it has complied with its relevant Code requirements (or that there is no causal nexus between the scam loss and any non-compliant Code requirements), decline to pay any scam loss and referring the customer to the digital platform or EDR.

We view that all outcomes are sub-optimal:

- Outcome (i)(a) would undermine Australia's whole-of-ecosystem approach as it would effectively exempt other sectors from liability.
- Outcome (i)(b) would likely result in substantially more cases being escalated to EDR and longer wait times for customer outcomes as the customer may go through the other RE's IDR and not receive the remaining compensation (or may choose to go straight to EDR after their initial IDR experience), meaning that the complaint is escalated to AFCA who then needs to assess the evidence to assess how the two REs did not meet their relevant Code requirements, the relative weighting of those requirements, the likely extent to which they contributed to the loss, etc.
- Outcome (ii) would mean even longer wait times for outcomes as customers go between IDR processes and substantially more cases being escalated to EDR.

Clear liability rules and a mechanism for liability apportionment established by the Minister in regulations (discussed further below) would enable REs to apply the liability apportionment as part of the IDR process (noting that, in some cases, a bank may not have the evidence to assess whether a digital platform has complied with its Code obligations). Importantly, while a customer would need to seek the actual compensation from other RE(s), the proportion of liability of the other RE(s) would be better understood from the initial IDR process. Importantly, clear liability rules would also drive incentives across the whole ecosystem to prevent scams from reaching Australians.

Further, the Australian banking sector is comparatively more advanced in developing dispute resolution procedures than the other industries intended to be subject to the regime. Australian banks have already implemented *RG 271 Internal Dispute Resolution* and *RG 267 Oversight of the Australian Financial Complaints Authority*. This high bar may not be replicated by other industries, meaning that a large proportion of SPF consumers are likely to first raise a complaint with their bank as this is where they may first realise they have lost money.¹² Notwithstanding this observation, all REs should be required to have IDR processes that provide consumers with a choice of how to contact them, such as by phone or online.

Therefore, the ABA views that the Minister should be provided powers to establish via regulation clear liability rules, the ability to join REs to an IDR and a mechanism for apportionment. This would ensure the approach to liability is consistent across the framework and regulated entities (rather than individually applied through different Industry Codes) and has the force of law to ensure compliance.

¹² This highlights the need for simultaneous publication of all Industry Codes, which is discussed below under section **3.2.1 Approval of Codes**, page 18.

Application of rules at EDR

We understand the Government expects that AFCA will, through decisions over time, build up a body of practice regarding liability apportionment that can be imported back into RE's IDR practice.¹³ While this may occur, this will take a significant amount of time during which both customers and industry will lack certainty. The absence of an agreed approach will likely mean disputes over liability apportionment and will not provide the certainty needed for consistent outcomes for consumers, efficient operation of the single EDR mechanism, or requisite investment by REs.

Further, there is no guarantee that the EDR cases that eventually come to constitute the body of practice will be representative. They may represent edge cases, and are likely to be inconsistent, making them unsuitable for supporting broad-based IDR decision-making.

In addition, the exposure draft does not contain any requirements in relation to redress for the SPF consumer. Instead, it makes REs liable for civil penalties to the extent that they have failed to comply with their obligations at the individual scam and customer level. AFCA's current "fairness" consideration is not fully aligned to this policy position. Under its current approach, AFCA considers the broader circumstances of a complaint meaning that it may focus on compensating consumers if it will result in what AFCA considers to be a fair outcome to the consumer. In its determinations to date, AFCA has applied its approach of fairness, on occasion in contradiction to legal and common law requirements or precedents. That fairness approach may be appropriate in the context of a broader consumer complaint system but is ill-suited to the SPF where the policy intent is to require regulated entities to take specific actions to combat scammers.

Finally, we note several potential conflicts with other consumer laws.¹⁴ The draft legislation will require AFCA to use evaluative judgment to determine whether the steps a sector took over another alternative step was more or less reasonable or proportionate. Rules of the type recommended above would support AFCA in this process.

Recommendations

- The exposure draft be amended to provide the Minister with the power to impose a whole-of-ecosystem liability rules and a liability apportionment mechanism at both IDR and EDR. One way this could be achieved is by including a rule-making power that outlines principles including a new sub-section within section 58GE to the effect:

"The SPF rules must contain rules, to be applied by a regulated entity's internal dispute resolution mechanism and by a SPF EDR scheme, as to the process to be followed and how liability to a SPF consumer is to be apportioned in circumstances where regulated entities in different regulated sectors have each failed to comply with their obligations under an applicable SPF code."

¹³ Per discussion at Treasury Scams Prevention Framework Consultation and Information Session, 18 September.

¹⁴ These are elaborated in greater detail under the section 3.2.4 **Interaction with other regulatory obligations** of this submission, page 19-20. In particular, see the examples of the Banking Code of Practice and Unfair Contract Terms.

- To ensure that AFCA's determinations are consistent for all customers and aligned to the intent of the exposure draft, AFCA should be given clear liability rules directing how it deals with scam complaints referred to it. The rules would address:
 - **process matters** – how AFCA should join parties to a complaint, and how AFCA should assess compliance with Principle/Code requirements, and
 - **matters of substance** – legal liability rules that AFCA is required to consider when determining whether compensation should be paid. AFCA should only have regard to these rules, not any Principles/Code requirements (which should only be the subject of review by a regulator or court) and not any general fairness mandate. Compliance with overarching Principles operating at a systemic level is complex and not suited to determining compensation in individual cases. In addition, information relating to an RE's scam procedures for preventing, detecting and disrupting scams is highly sensitive and needs to be kept strictly confidential. If it is provided to AFCA or made public through determinations, there is a high risk that references to it in complaints or determinations will enable scammers to exploit that information in future scams.

3.1.3 Ensure data-sharing arrangements are appropriately prioritised to maximise impact

The ABA supports the policy intention of the data-sharing proposals, but views that further amendment of the exposure draft is needed to give them effect. Below, we highlight two areas for consideration – the definition of actionable scams intelligence, and the intention to place the regulator at the centre of information gathering and dissemination of scams intelligence.

Definition of “actionable scam intelligence”

The ABA notes the following concerns:

- The definition of “actionable scam intelligence” contains overly broad references that will lead to a substantial increase in compliance burden rather than the creation of more decision-useable information.
- The definition deals with when scam intelligence arises, but not when it becomes actionable. For intelligence to be actionable, it must be able to serve as the basis of a decision by a RE to act on a scam. The definition in the exposure draft does not create such a nexus.
- The exposure draft would require an RE, on receipt of actionable information, to take “reasonable steps” within a “reasonable time” to identify each SPF consumer who is or could be impacted by actionable scam intelligence and to communicate with “each SPF consumer ... who is or could be impacted by the suspected scam”. Given that an SPF consumer need not have a formal customer relationship with the RE,¹⁵ this would effectively create an obligation on the RE to communicate with all Australians (whether living in Australia or living

¹⁵ Section 58AH(2)

outside Australia given the unclear extra-territorial provisions) and all Australian businesses with less than 100 employees.

- The requirement that actionable scam intelligence relate to a regulated service of the entity may be narrowly construed and mean that, for example, an RE would fail to pass on intelligence it has received that does not directly concern it (for example, a digital platform may not pass on intelligence regarding a phone number). As discussed in our Recommendations below, we view that the Minister should have broad powers to define the types of reporting under actionable intelligence and view that this power could be used to support effective whole-of-ecosystem reporting.

Data-sharing

The exposure draft envisages that the SPF general regulator will be at the centre of the data-sharing arrangements.

In practice, we anticipate that this role will see the SPF general regulator receive an enormous volume of reports from a range of entities across all sectors. Effectively, the regulator would be taking on a role akin to AUSTRAC but with respect to actionable scam intelligence rather than suspicious matter reports. Indeed, it is likely that the SPF general regulator's role would be broader than AUSTRAC, given its proposed wider remit with respect to assessing and disseminating scams intelligence. It is unclear whether the regulator would be able to effectively deal with reporting data at this volume.

Taken as a whole, the ABA does not view that the approach proposed in the exposure draft would be effective use of resources in combatting scams. It would require the Government to fund a substantial uplift in regulator capacity, would require REs to build new APIs and fund new reporting teams, and potentially create delays as this new capacity is stood up. Given the lack of nexus between the current definition of actionable scam intelligence and decision-useful information, the likely outcome would be the creation of a significant new regulatory obligation for all REs with no corresponding impact on scams.

Finally, this would duplicate existing private-sector mechanisms such as the AFCX. This existing mechanism, which is being utilised by many banks, telcos, social media companies and government agencies, could be leveraged to report to regulators and other entities, rather than placing a regulator at the centre of receiving and disseminating intelligence. The AFCX would have the capability to provide tailored reporting to regulators.

Recommendations

- The exposure draft be amended to further refine the definition of actionable scam intelligence so that it constitutes intelligence that is able to serve as the basis of a decision made by a RE to act on a scam. One way this could be achieved is by amending the definition of actionable scam intelligence in section 58AI to read:

"A regulated entity ~~identifies, or has,~~ actionable scam intelligence if (and when):



(a) *there are reasonable grounds for the entity to suspect that a communication, transaction or other activity on, or relating to, a regulated service of anthe entity is a scam; and*

(b) *the intelligence is ~~needs to be~~ reasonably able to serve as the basis for the regulated entity to decide to act on the suspected scam.”*

- The legislation should not be prescriptive about the provision of actionable scam intelligence to the regulator, but instead give the Minister broad powers to require specified types of information to be provided to the regulator or a third party and set the type of actionable scam intelligence that needs to be published to SPF consumers. This would allow the Minister to designate an institution, such as the AFCX and its Anti-Scams Intelligence Loop, and it would also allow the Government to define the types of intelligence it wished to receive and to refine those definitions over time. One way this could be achieved is by:
 - removing the references to “SPF regulator” in section 58BR and subsection 58BS(4);
 - including in subsection 58BS(2) a new sub-paragraph to the effect:

“the body or bodies to which such a report is to be issued;”
 - including a new section within Subdivision E to the effect:

“If, under subsection 58BS(2), a body other than a SPF regulator is designated as a body to which reports under section 58BR are to be given (Reporting Recipient), the SPF general regulator may require the Reporting Recipient to share with a SPF regulator any information that it has received under section 58BR.”
 - removing the notes appearing under subsection 58BS(2)(a).

3.1.4 Clarify key definitions to ensure the regime operates as intended

Key definitions within the exposure draft could be better calibrated towards the intended policy outcome. At present, some key definitions contained within the exposure draft are broadly drafted such that they will impose overly onerous obligations on REs.

Definition of SPF consumer

The definition of SPF consumer is overly broad. Taken on its face, every Australian would theoretically be an SPF consumer of each RE. This would have significant flow-on consequences throughout the legislation. For example, section 58BX would impose a requirement to “disclose to SPF consumers of the regulated service sufficient information to enable those consumers to act in relation to the suspected scam”. This would require the RE to disclose that information to every Australian.

The ABA understands that Treasury’s intention is to capture the full range of potential scam scenarios across multiple sectors within the single definition. We view that a better approach would be to more

narrowly define “SPF consumer” and deal with non-captured cases (for example, impersonation scams) as separate categories in their own right.

Definition of small business

The ABA notes the difficulty and ambiguity of applying the current definition of SPF consumer, which extends to all enterprises with less than 100 employees, and a principal place of business in Australia. We note practical challenges of applying this headcount test, as banks can never independently verify employee numbers. Further, without a turnover limb to the test, a company with a small headcount but high profit or turnover in the millions of dollars would fall under the test.

This introduces yet another definition of small business into Australia’s regulatory framework. The CCA already contains a definition of small business for the purpose of the unfair terms regime which could be used. Similarly, ASIC provided a ‘no action’ letter to the institutional market in connection with the UCT regime giving effect to the policy position that these consumer type protections do not need to be extended to the institutional market. Additionally, the ePayments Code does not apply to business customers

The definition of small business appears to be based on the equivalent definition under the UCT requirements. For practical purposes, we view that the small business test contained in the exposure draft be aligned with the UCT provisions, with the exception that the limbs be cumulative (that is, that both the headcount and turnover limb be applied).

Definition of higher risk SPF consumers

The exposure introduces but does not define the concept of “higher risk” SPF consumers. We view that additional definition of a “higher risk” customer is needed to create certainty for consumers and industry and suggest that the Industry Codes themselves are the best place to define this. A clear definition of what is meant by “higher risk” will be important in being able to support these consumers on a consistent basis. Consideration should be given to how these consumers would be identified, particularly as circumstances may change over time.

Definition of a scam

The current definition of a scam may not capture some scams (e.g. where the scammer makes transactions or impersonates an entity who are not REs). In addition, it may capture a broad range of fraud and misleading and deceptive conduct that we understand are not intended to be, and should not be, captured.

In addition to amending the definition to capture transactions performed by the scammer and activity where they impersonate others, we recommend that a list be included in the Rules setting out which scam activity is covered or not covered by the SPF (e.g. fraud where the parties are known to each other, Ponzi schemes, misleading and deceptive conduct involving goods and services, blackmail, extortion etc). The Minister establishing this list in the Rules would provide greater clarity and enable the list to evolve over time, as the scam environment changes and with industry consultation.



Recommendations

- The exposure draft be amended to more closely align with the policy intent, including:
 - In section 58AH(1), remove the text “or may be” and “or purportedly provided” from the definition of SPF consumer, and instead explicitly deal with any categories of scam (eg. impersonation scams) that those provisions are intended to capture.
 - In section 58AH(1), align the small business test with the provisions in the unfair contract terms (**UCT**) provisions (with the exception that the limbs apply cumulatively), or explicitly exclude entities that are classified as wholesale clients for the purposes of the *Corporations Act*.
 - In section 58AH(2)(a), consider the need for application of the text “indirectly” providing a service.
 - In section 58AH, include a new subsection (5) which provides that Codes can more clearly define “higher risk” SPF consumers.
 - Amend the definition to capture transactions performed by the scammer (ie. remote access scams) and activity where they impersonate others (ie. phishing scams).
 - Provide the Minister with powers to establish and clarify in Rules the scam types to be included and excluded from the SPF.

3.2 Additional recommendations

3.2.1 Approval of Codes

The exposure draft would permit the Minister to delegate their authority to make a Code for a regulated sector to another Minister, the Australian Competition and Consumer Commission (**ACCC**) or an SPF sector regulator.¹⁶ While the ABA has no in-principle concern with delegated development of Codes, delegating Code-making responsibilities to different regulators or Ministers without an overall coordination mechanism raises two related risks:

- There is no guarantee that Industry Codes developed for different sectors will apply consistently high levels of consumer protection. While acknowledging that different sectors will require Codes tailored to their specific circumstances, an overall high bar should be maintained.
- There is no guarantee that Codes developed for different sectors will be published and made effective on the same dates, meaning that Codes could apply at different dates, with corresponding impacts to consumer outcomes.

As outlined above,¹⁷ the banking sector is comparatively mature in its approach to dispute resolution, when considered against other areas of the economy, and operates in a more tightly regulated environment with serious and material consequences provided for in legislation – particularly when compared to other sectors such as digital platforms.

Further, we note that Australia currently lacks an equivalent to the Singapore *Online Harms Act*. There is a risk that the absence of such laws will mean that, unless Codes are introduced simultaneously, locally domiciled REs may bear a greater proportion of the liability for losses until these regimes are enacted.

We view that all Codes should be designed consistently, accord with the SPF Principles and include robust, measurable and outcomes-based obligations for all sectors.

Further, reflective of the whole-of-ecosystem approach to combatting scams, the ABA considers that all sector Codes should be published and take effect simultaneously. Should the Codes not be published simultaneously, there is a risk that banks will bear a greater proportion of the liability for losses, while other entities in the first phase will lack incentive to add new controls to mitigate scam activity. This will negatively impact the overall effectiveness of the regime.

Considering the above, the ABA views that final approval powers should be retained by the Minister with primary responsibility. This will ensure greater alignment in the content and timing of Industry Code development.

¹⁶ 58CD

¹⁷ See section 3.1.2, page 11



Recommendations

- The exposure draft be amended to ensure that all sector Codes are reviewed by the ACCC and approved by the Minister. One way this could be achieved is by adding the following text at the end of section 58CD:

“provided that only the Minister has the power to approve a code and a code does not apply to a regulated sector until the Minister has approved it.”
- Industry Code development be sequenced to ensure that all Codes become simultaneously effective, all Codes hold sectors to similarly high standards, and to meet the Government's intent of an ecosystem approach to combatting scams.

3.2.2 Extra-territorial scope

There are practical questions of foreign companies submitting to the jurisdiction of AFCA. We view that foreign companies subject to the regime should be required to nominate a locally domiciled entity for service and to cover liability.

Separately, while Section 58AJ provides that the exposure draft applies to acts, omissions, matters and things outside Australia, the exposure draft does not propose to amend the extra-territoriality provisions in section 5 of the *Competition and Consumer Act* (which limits the operation of the extended jurisdiction to bodies corporate incorporated in or carrying on business in Australia) to apply to the SPF provisions.

While the exposure draft provides that “regulated sectors” are to be designated with respect to the “Australian economy”, the intended extent of this restriction is unclear and may be capable of having extensive extraterritorial application.¹⁸ Depending on how the “regulated sector” instruments are drafted, there may be uncertainty about whether REs can include entities outside Australia who provide services to Australians (whether or not the services are provided in Australia) and whether scams will include scams perpetrated on Australians whether or not the scammer or the victim are acting within Australia.

Recommendations

- The exposure draft be amended to require foreign REs to nominate a locally domiciled entity for service and to cover liability.
- The extra-territorial scope of the CCA apply without additional extension by the proposed legislation. This could be achieved by deleting subsection 58AJ(2).

¹⁸ See the High Court decision in *Karpik v Carnival Plc*

3.2.3 Action for damages and potential class action risk

Section 58FZ of the exposure draft allows SPF consumers (including small businesses) to directly commence proceedings for damages against an RE for breach of an SPF Principle or Code within a period of six years since the cause of action, which could include class actions.

The principal intention of the regime is to encourage preventative actions on a whole-of-ecosystem basis. Further, the exposure draft already contemplates whole-of-ecosystem EDR and includes substantial pecuniary civil penalties. Our view, therefore, is that the right to bring individual causes of action of REs is unnecessary.

Recommendations

- s58FZ be removed.

3.2.4 Interaction with other regulatory obligations

The ABA notes that the regulatory obligations proposed to be created by the exposure draft legislation would interact with other regulatory obligations. A non-exhaustive list includes:

- *Spam Act*. The exposure draft would create new obligations for an RE to communicate with SPF consumers which may not align with the requirements of the *Spam Act*. We suggest that an exception be provided that allows electronic communication with customers for the purpose of complying with the SPF. In effect, a consumer would not be able to opt-out of such communications.
- *Anti-Money Laundering/Counter-Terrorist Financing Act (AML/CTF Act)*. There is a need for a whole-of-government approach to money laundering and other serious crimes, to ensure a consistent approach to investigate and combat scams, fraudulent activity and money laundering. The current approach will see duplication of obligations, particularly in relation to reporting across the AML/CTF regime. ABA notes the following:
 - Sharing information with the regulator or other REs under subsection 52BS(3) and 58BU of the exposure draft may contravene section 123 of the *AML/CTF Act* (**tipping off provisions**). We request a carve-out to provide that this information sharing is authorised by law and that REs can lawfully share information that may also be part of an ongoing fraud investigation.
 - Subdivision E of the exposure draft includes reporting requirements on suspected scams and scams that have occurred. The fraud definition contained in the *Anti-Money Laundering and Counter-Terrorism Rules Instrument 2007 (No. 1)* overlaps with the definitions for scams, and therefore with existing AUSTRAC reporting. This would create duplicative reporting obligations to different regulators. We recommend that Treasury consider utilising the regulator information sharing provisions to ensure that if a case is reported to one regulator, it does not need to be shared to another regulator.
- *UCT*. REs may need to amend their contracts to enable them to take action to protect their customers in certain circumstances. There is a risk that these actions will be argued to be in

breach of the UCT rules unless the terms are taken to be required or expressly permitted by law.

- *ePayments Code.* To ensure all scams are captured and regulated under the SPF, a concurrent review of the relevant definitions of the ePayments Code should occur. This would ensure a clear delineation between scams and mistaken/unauthorised payments, which is required to provide consistent protections for consumers impacted by scams and provide clarity to REs on the obligations that apply. Without amendment there is a risk of duplication and overlap for REs and confusion for consumers. The ePayments Code should continue to apply to mistaken and unauthorised payments as it was intended. Whereas all scam payments (authorised and unauthorised) should only be regulated under the SPF. These changes should be made at the same time as the SPF comes into effect. A more comprehensive review of the ePayments Code is planned by Treasury for 2025-26 to extend obligations to relevant payments service providers (PSPs). At that stage designation of PSPs should also be considered under the SPF.
- *Privacy Act.* REs will potentially be required to provide the SPF regulator with personal information of persons engaged (or attempted to be engaged) in scams where those individuals have not consented to that information being collected. Additionally, even though the exposure draft only calls out the alleged/potential victim's identity as personal information (s5B(3)(b)), in providing such information about the scam, personal information would likely be disclosed (including sensitive information). For example, if the scam targeted a certain group, then racial or ethnic origin would be disclosed. Romance scams may require the disclosure of sexual orientation or practices. There is a question of balancing the public interest of collecting this information against the private interest of individuals who may prefer that the SPF regulator not collect this information about them.
- *CCA.* The exposure draft flags that the SPF rules will seek to exclude from being a scam activity conduct that triggers other consumer protections including such as 'misleading and deceptive conduct'.¹⁹ However, it may not be clear to a SPF consumer whether the conduct or behaviour they have encountered is deception but is not misleading (so is a scam) or is deceptive and is misleading (so is not a scam). It would be helpful to have clarity on what is intended by this exclusion and whether other misleading and deceptive provisions such as those contained in the *ASIC Act*, *Corporations Act* and *National Consumer Credit Protection Act* would be similarly excluded. As noted earlier, we recommend that in addition to amending the definition to capture transactions performed by the scammer and activity where they impersonate others, that a list be included in the Rules which sets out the scam activity that is covered and other activity that is not covered. This will provide greater clarity for consumers in relation to their protections and for REs in relation to their obligations.

The ABA understands that several of the above are currently undergoing their own reform processes, with amending legislation either under consideration or before Parliament. The ABA strongly views that the exposure draft should deal with questions of overlap or interaction with other legislative provisions to the extent possible, to ensure that it functions as a self-contained regime.

¹⁹ Per draft Explanatory Memorandum, paragraph 1.78 & 1.80.

As a practical matter, attempting to address these issues in separate legislative processes raises the risk that they will be left unresolved by the time the SPF commences. This may result in the unintended consequence of creating an environment in which other legislative obligations impact Australia's scams response.

As the ePayments Code sits outside Parliamentary processes, minor amendments could be progressed to ensure alignment with the SPF in time for implementation. A more comprehensive review of the ePayments Code could then be progressed in line with the *Strategic Plan for the Australian Payment System* roadmap.

Recommendations

- As a practical suggestion, the ABA views that these identified overlaps would best be dealt with in the SPF exposure draft itself, rather than other Parliamentary processes. This would allow the exposure draft to be dealt with as a self-contained regime. One way this could be achieved is by:
 - Including a new section in Division 2 Subdivision C to the effect:
“If the provision of a law would otherwise prevent the regulated entity from contacting SPF consumers, the provisions of this Subdivision prevail.”
 - Including new sections in Division 2 Subdivisions E and F to the effect:
“If the provisions of a law would otherwise prohibit the disclosure of information as required by this Subdivision, the provisions of this Subdivision prevail.”
 - Including a new section (3) in Section 58BZ along the lines of:
“(3) If a regulated entity is taking the steps contemplated by this section, these will be deemed to be reasonably necessary to protect their legitimate interests under all applicable laws.”

3.2.5 Safe harbour

The ABA welcomes the provision of safe harbour protections in the exposure draft.²⁰ As drafted, the safe harbour would protect the RE from liability in a civil action or civil proceeding for taking action to disrupt an activity that is the subject of actionable scam intelligence, so long as certain preconditions are met (for example, acting in good faith and in a manner reasonably proportionate to the suspected scam).

While welcoming the inclusion of these provisions, we note the following limitations:

- The safe harbour protections would apply only during the period of investigation and would cease once the RE identifies that the activity is a scam. However, it is period **after** the RE

²⁰ 58BZ

verifies the scam in which safe harbour protections are most needed as this is the period in which the RE may need to act quickly to disrupt the activity.

- The safe harbour protections would require an RE to for a definitive view on whether or not something is a scam, which may not be possible or practicable in all instances.
- The requirement that disruptive actions be “reasonable and proportionate” in order to qualify for safe harbour protections may not provide sufficient certainty for REs seeking to rely on them. For example, the discharge of a disruptive obligation on the basis of a compelling false positive may result in settlement failure for a customer. We suggest that the Industry Codes could elaborate on these provisions in more detail.

Recommendations

- The safe harbour provisions in 58BZ be amended to extend to include actions after the identification of the scam activity that are reasonable and in good faith.
- The Industry Codes provide further elaboration on the requirement for “reasonable and proportionate” actions.

3.2.6 Receiving Bank obligations

The ABA notes that the Government’s intention is that obligations will apply to receiving banks.²¹ The ABA views that the scope of receiving bank obligations be limited to accounts with a retail focus only and not extend to institutional and wholesale clients. Further, the Codes should include details of the controls required to prevent the opening of mule accounts as well as expectations for the RE to identify and take necessary action when mule accounts are identified.

The ABA agrees it is reasonable to place “high bar” obligations on the account opening Customer Due Diligence processes of REs; however, challenges arise when accounts are opened by individuals with genuine identify documents which belong to the account holder and the account holder allows the account to be used for financial crime purposes (knowingly or unwittingly), which is more often the case. Harsher individual penalties are needed to disincentivise this activity.

There is a risk that holding the Receiving Bank liable for scam losses amplifies the potential for “friendly fraud”²² or creates the risk that REs will begin to refuse to open or maintain accounts for higher-risk segments of the population, creating an ‘underbanked’ or ‘debanked’ challenge in Australia. For instances of genuine identification, it is unreasonable for an RE to be liable unless the RE did not follow the monitoring requirements defined by the regulator.

²¹ See: Q&A session of the Assistant Treasurer’s Press Club Address on Fraud and Scams, and the example given in para 1.85 (Meaning of SPF consumer) of the draft explanatory memorandum.

²² Friendly fraud, also known as chargeback fraud, occurs when an individual purchases a good via a card payment and then requests a chargeback with the issuing bank.



Recommendations

- Obligations on the Receiving Bank, including expectations of detective account monitoring, are clearly outlined in the Industry Codes.
- If the concept of Receiving Bank is defined, then the scope should be limited to accounts with a retail focus and should not extend to institutional and wholesale clients.
- In parallel to the development and publication of the Codes, further uplift is required to the relevant Criminal Codes to impose harsher penalties on individuals who allow access to or sell their bank accounts for the purposes of financial crime. An uplift in criminal charges and a strong shift towards individual liability is required to disincentivise money mule activity in relation to receiving scam proceeds.

- ENDS -