



Commonwealth
Bank

Scams Prevention Framework – exposure draft legislation

Response to consultation

4 October 2024

Contents

1.	Executive summary	3
2.	Scams Prevention Framework (SPF)	4
2.1	Liability, compensation and apportionment	4
2.2	Civil penalties	7
2.3	Definition of a scam	9
2.4	Actionable scam intelligence	10
2.5	Other matters	13



1. Executive summary

The Commonwealth Bank of Australia (CBA) welcomes the opportunity to respond to Treasury's consultation on the *Scams Prevention Framework – exposure draft legislation*, released in September 2024.

CBA supports the overall intent and design of the Scams Prevention Framework (SPF), which will establish an ecosystem approach to tackling scams by setting responsibilities for designated sectors through overarching principles-based obligations under the *Competition and Consumer Act 2010* (Act) and supplemented by mandatory sector-specific codes.

The proposed legislation will significantly strengthen Australia's defences against scams and increase protections for consumers across the scams ecosystem. We welcome the Government's holistic approach to combatting scams through prevention, detection, disruption and response, as well as reporting and governance obligations. We also support the requirement for a single external dispute resolution (EDR) mechanism which will provide a consumer with a clear pathway for compensation where one or more regulated entities has failed to meet its relevant obligations.

To help ensure the SPF achieves its intended objectives, we have identified a number of important areas which in our view require attention. In particular, we note the Government's stated intent *'to provide victims with a clear pathway for redress where the entity has done the wrong thing'* and *'create end to end accountability across the initial designated sectors when a scam victim makes a complaint'*.

To achieve this, we consider clear liability rules and a mechanism to attribute liability between different regulated entities are essential. These should be outlined in regulation or rules by the Minister to provide a clear legal basis for ensuring all regulated entities in the scam ecosystem are incentivised to act and are accountable for compensation where they breach their obligations. CBA's view is that liability to contribute to compensation should be determined in accordance with legal liability rules and an apportionment mechanism; in contrast, the overarching principles should be reserved for regulators to assess for contraventions and take enforcement action. This is a threshold question for the efficacy of the SPF and fundamental for timely, efficient, and consistent compensation outcomes for scam victims. The absence of such measures materially undermines the prospects of the SPF achieving its stated intent.

We also identify aspects of the SPF requiring clarification or design improvement, including:

- authorising AFCA as a special purpose compensation complaint body to investigate compensation claims as a 'one stop shop', rather than through an IDR/EDR construct;
- broadening and clarifying the definition of a scam to ensure that common scams, such as remote access and phishing scams, are captured;
- ensuring that actionable scam intelligence is used effectively and efficiently across the ecosystem, including reporting provided to regulators, and businesses sharing with each other through the established Anti-Scam Intelligence Loop;
- clarifying the civil penalty regime to ensure that civil penalties are proportionate and apply to systemic issues, not individual or 'one off' failures; and
- ensuring alignment with payments reforms through concurrent review of the ePayments Code and designation of services by Payment Service Providers (PSPs) instead of 'banking business'. It is also important to ensure a whole-of-government approach to addressing scams and fraud is taken, including harmonisation between the SPF and the AML/CTF regime.



At CBA, we remain focused on protecting and supporting customers by improving early detection and prevention of scams. Over the past year, we have invested \$800 million to protect our customers by combating cyber and financial crime along with fraud and scams. Our customer scam losses decreased more than 50 per cent in FY24, following the delivery of initiatives such as NameCheck to help prevent scam and mistaken payments, customer verification measures such as CallerCheck and CustomerCheck, introduction of friction in certain payments to cryptocurrency exchanges, as well as other collaborative initiatives with telcos to identify and prevent scam calls to customers, and social media companies to help reduce the volume of scam content hosted on these platforms.

Our priority is to further reduce customer scam losses and volumes and we believe the introduction of the SPF will help incentivise all parties in the scams ecosystem to take action against scams and better protect consumers.

We provide further detail below on our key concerns and other areas we have identified for improvement, and we would welcome an opportunity to discuss the matters raised in our submission.

2. Scams Prevention Framework (SPF)

We support the Government's proposed approach to introduce overarching principles and require regulated entities to implement these through governance arrangements and by taking steps to prevent, detect, report, disrupt and respond to scams. These overarching principles are best placed to incentivise regulated entities to improve their anti-scam processes and controls at a systemic or macro level in a similar way to the general financial services licensing obligations under the Corporations Act (for example, the obligation on an AFSL holder to act "efficiently, honestly and fairly" in s.912A(1)(a)). In contrast, specific liability rules are best placed to determine compensation at an individual consumer level. Consistent with this framing, we outline key proposals that we believe will help the SPF to meet its objectives in the following sections.

Given the significance of the Government's reforms, we recommend a review of the SPF occur 12 months post implementation to consider whether it is operating as intended and the objectives are being achieved.

2.1 Liability, compensation and apportionment

The overarching principles outlined in the Exposure Draft will be important in incentivising action and driving consistency across designated entities under the SPF; however, we consider they are not fit-for-purpose to determine whether compensation should be payable in the case of an individual consumer.

As noted earlier, we believe clear legal liability rules and a mechanism to attribute liability between different regulated entities is an essential element of an effective SPF. This will ensure the SPF delivers the Government's intention of a clear pathway for consumers to seek redress (where an entity has failed to meet its obligations) and incentivise designated entities to be accountable and take action to prevent, detect, respond to and disrupt scams.

Without specific rules, there is significant uncertainty in how liability would be determined for individual cases. The overarching SPF principles are not, in our view, a helpful guide to determining individual consumer loss compensation. They generally do not address the question of causative relevance for specific customer cases and do not lend themselves to establishing consistent compensation outcomes.

In addition, reliance on the overarching principles to determine individual consumer loss compensation will require assessment of the internal policies and procedures implemented by regulated entities to comply



with those overarching principles. Such processes and procedures are commercially sensitive documents, which must be protected. Any reference to an organisation's policies or procedures in public documents, such as AFCA determinations, would risk providing scammers with information that could be exploited in future scams.

For these reasons, we propose that the primary law or a subsequent instrument should supplement the overarching principles with specific liability rules. These would operate at an individual customer level to determine a regulated entity's obligation to contribute to compensation payable to a consumer.

While the overarching obligations focus on reasonable business conduct to detect and disrupt scams at a systemic level, the liability rules should focus on the allocation of liability to compensate an individual consumer who has suffered a loss. The SPF general regulator (i.e. ACCC) could consider conduct by a regulated entity giving rise to compensation outcomes when assessing compliance with the overarching principles, but our view is that compliance with the overarching principles should not be a matter considered by AFCA in determining liability to compensate a consumer. Determining non-compliance with the overarching principles is a complex, sensitive matter that should only be dealt with by regulators or a court.

Specific liability rules

Specific liability rules would have the benefit of making the compensation framework more efficient and consistent for consumers, regulated entities and AFCA. Without specific liability rules, there is a high likelihood of disparate outcomes for consumers even though the scam complaint may have the same or similar underlying factors. A consequence of this inconsistency will likely be dissatisfaction amongst consumers, which in turn risks a loss of confidence by consumers in the operation and benefits of the SPF.

Specific liability rules which can be readily assessed would not only provide clarity for consumers but also for regulated entities, on which they will be able to base significant investment decisions in technological scam prevention capability. Such rules would also support a more efficient and consistent approach to compensation determinations, by providing case managers with specific guidance to consider individual cases and avoiding them having to make difficult compensation determinations based on an assessment of compliance with overarching obligations.

Apportionment of liability

We note the draft SPF does not contain a mechanism for attributing liability between different regulated entities and the consumer. This is a key issue that needs to be resolved for consumers to access a clear and efficient pathway for compensation and if all regulated entities across designated sectors are to be held accountable for scam prevention and losses.

Establishing in regulations or rules a mechanism to apportion compensation would lead to faster and more consistent compensation outcomes for scam victims and assist to avoid excessive reliance on discretion and subjectivity.

Dispute resolution – IDR and EDR design flaw

We welcome the intention to appoint a single EDR mechanism for designated sectors under the SPF and we support the requirement for all regulated entities to implement IDR systems for complaints related to scam prevention and protection processes. In the case of a bank, this means that we want our customers to contact us so that we can secure their accounts, change their passwords, notify other parties per our intelligence sharing obligations, and attempt recovery of funds from the recipient account.

Although we acknowledge that IDR/EDR models work well in many scenarios, we do not consider that an IDR/EDR model is a suitable process for assessment of compensation for consumers as contribution may



be required from multiple regulated entities in relation to a single complaint. An IDR/EDR model functions well when a complainant can readily identify the organisation that they believe is responsible for an act or omission that gave rise to the complaint. The model does not function well when there is uncertainty concerning the entity or entities which may be responsible for the act or omission.

The most common scams exploit vulnerabilities across industries with multiple parties having the opportunity to implement measures to better protect consumers against loss. As a result, there will always be multiple parties who may conceivably be responsible for an act or omission that gives rise to a complaint, including a financial firm, a telecommunications provider, and a digital platform. Neither a complainant nor any of these providers will know which party may be at fault until an investigation is conducted based on information made available by all of these parties.

It would be quite onerous to expect a consumer to be able to discern whether, and to what extent, regulated entities that may have played a role in a particular scam event, had failed to meet relevant obligations, and therefore determine whose IDR processes should be engaged. Accordingly, the IDR/EDR model is likely to result in uncertainty, confusion and frustration amongst consumers. Further, if the entities are equally uncertain it will result in the complainant potentially shuffling from one entity to another as they seek to resolve this uncertainty. At the IDR stage, in the absence of any effective multi-party information exchange mechanism, a complaint could only be considered on narrow grounds based on limited information available to the relevant entity. Such outcomes are likely to be shown to be error prone when reviewed at EDR with the benefit of all relevant information. However, by that stage, one or more suboptimal IDR processes would have already been engaged.

Another shortcoming is that decisions at IDR for each regulated entity would need to be tracked and notified to other regulated entities in order to prevent under or over compensation and to mitigate the risk of abuse of the scheme, including by scammers. This would be complex. It is also likely that different IDR processes would make inconsistent decisions in relation to the same claim, raising the risk that a consumer will be confused and dissatisfied.

Overall, this design flaw would lead to inefficient outcomes and increased total system costs for all parties in terms of time and money and would cause avoidable stress to complainants.

Special purpose compensation complaint body

In order to better achieve the legislative intent and ensure a positive consumer experience, we suggest that the compensation framework be established as a separate process where applications are made to a special purpose compensation complaint body. This body would investigate matters as a 'one stop shop', rather than through an IDR/EDR construct. We support AFCA performing this role, although considering the distinct nature of the new model, we believe that new terms of reference and operating rules will be required as part of the authorisation conditions for AFCA.

A special purpose compensation complaint body would be more effective because it would have visibility and jurisdiction across the broader scam ecosystem, unlike any IDR process, and would be more conducive to a better consumer experience. This will ensure that all regulated entities are required to compensate customers where they breach their obligations and will incentivise investment in better procedures across the ecosystem to reduce the risk of customers losing money to a scam. Regulated entities could be required to assist consumers to make a claim for compensation by helping them navigate the compensation claims process. This would assist with both the customer experience and efficiency of the compensation mechanism.

A special purpose compensation complaint body would also avoid unintended consequences of utilising an existing IDR/EDR framework. For example, under Rule A5.1 of AFCA's Complaint Resolution Scheme Rules (if they were not substituted as we have recommended above), when AFCA receives a complaint,



AFCA will notify the relevant firm in writing of the complaint. This referral process would amplify the inefficiencies mentioned above. The complaint could only be reviewed by the firm it was referred to based on limited information, leading to fragmented outcomes for consumers as the case would invariably find its way back to AFCA for further review. Referring the complaint to all possible firms would compound the issue further. It will generally not be possible to identify the entity or entities that were responsible until the investigation is conducted. This is the nub of the issue. To overcome this and create a more efficient and effective outcome for consumers and AFCA, it would be more efficient for AFCA to conduct a review in the first instance.

AFCA will face challenges in determining liability across the regulated entities, which will likely be compounded at least initially by the volume of complaints, and clear liability rules (as described above) will be crucial in assisting AFCA to make determinations in an efficient and consistent manner.

As the single compensation complaint body, AFCA's resourcing will be critical. AFCA must be appropriately funded and resourced to ensure it is able to develop and maintain the requisite expertise to make rules-based determinations across different regulated sectors. This will include an investment in technical expertise across the designated sectors. We acknowledge that regulated entities will need to assist with funding the administration of the scheme and suggest that the design of the funding model be linked to compensation outcomes under the liability rules to incentivise all regulated entities to improve their processes for protecting consumers against scam losses.

2.2 Civil penalties

In the Exposure Draft, we support the objective reflected in the Preamble to Division 2, Subdivision A, which indicates that the SPF principles are intended to operate at an overarching policy and governance level: *"These principles require each regulated entity to: (a) have appropriate governance arrangements; and (b) have appropriate strategies for preventing, detecting, reporting, disrupting and responding to scams"*.

The SPF recognises that even with significant improvements in scam prevention across the ecosystem, it will not be possible to eliminate all scam activity. Civil penalties should be commensurate with the seriousness of the breach and in our view should only apply to systemic failures at the policy, strategy or governance level, with consideration given to whether the entity had taken reasonable steps in all the circumstances.

On the current drafting of the Exposure Draft, there is some inconsistency between the notion that the SPF regulator's role is to regulate and enforce compliance with these systemic failures, having at its disposal remedies that include seeking civil penalties, and the fact that many of these obligations operate at a very granular level. Many of the proposed civil penalties could operate in circumstances where there was a very limited failure (including for one SPF consumer) because they rely on the defined terms "scam" and "actionable scam intelligence".

By way of example, the following subsections provide that a regulated entity will contravene a civil penalty provision if it fails to take reasonable steps to:

- prevent another person from committing "a scam" (s.58BJ(1));
- provide warnings to "each SPF consumer" who is identified as having a higher risk of being targeted by a scam (s.58BK(2));
- detect "a scam" relating to its regulated services (s.58BN(1));
- identify "each SPF consumer" who is or could be impacted by a suspected scam where the entity has "actionable scam intelligence" about "a suspected scam" within a reasonable time (s.58BO(1));
- disrupt "a scam or suspected scam" relating to "actionable scam intelligence" and prevent loss or harm arising from such "a scam or suspected scam" (s.58BW(1));



- disclose to SPF consumers sufficient information to enable them to act in relation to “actionable scam intelligence” about “a suspected scam” (s.58BX(1)).

The disproportionate effect of applying civil penalties at an individual customer incident level is multiplied by the fact that more than one of these provisions may apply in any situation where an individual customer falls victim to a scam. Where there are objectively reasonable grounds to suspect a specific scam has occurred or is in the process of occurring and a regulated entity fails to detect it, there are a myriad of civil penalty provisions that are breached (relating to preventing, detecting, reporting and disrupting). We consider this to be disproportionately harsh given that it will never be possible to stop all scams.

We suggest that the civil penalty provisions be reframed as obligations to take reasonable steps to perform the relevant activities at a systemic level. As outlined above, we suggest these overarching obligations would be complemented by specific liability rules, the breach of which would trigger an obligation to contribute to compensation for an individual consumer.

The current drafting of other civil penalty provisions appears to establish obligations that are unclear and onerous. For example:

- a regulated entity will contravene if they fail to implement policies and procedures (s.58BC(1)(b)). There is no materiality threshold for this obligation;
- taking reasonable steps to prevent scams and warn higher risk customers requires more than acting on actionable scam intelligence (s.58BK(2)). There are likely to be different interpretations of “higher risk” customers. In addition, given the granular nature of the definition of actionable scam intelligence and the fact that SPF codes will prescribe more specific obligations, it is difficult to conceive of further steps that would be reasonable, or indeed, possible.

We suggest that the civil penalty provisions are reviewed to make sure they are reasonable and proportionate to the regulated entity’s conduct.

We note that the current drafting could also lead to unintended consequences. For example, the civil penalties which currently apply to obligations to disrupt a “scam” or “suspected scam” (Principle 5) are likely to encourage banks to adopt a conservative approach that will significantly impede the flow of payments and create significant disruptions to businesses and consumers. We note that the UK Treasury is proposing amendments to the Payment Services Regulations (PSRs 2017) in conjunction with mandatory reimbursement rules to allow Payment Service Providers (PSPs) to delay the execution of an outbound payment transaction by up to four business days.¹ In order to comply with Principle 5, a bank may need to block all payments to a merchant following a single confirmed scam report from a customer of that merchant instead of first detecting trends or patterns to categorise a merchant as high risk. Payment delays and longer payment processing times may also lead to unintended consequences for Australian businesses.

The ability to make and receive real-time payments 24 hours a day, every day of the year is a strategic objective of the RBA.² The RBA expects financial institutions to deliver more fast payment capabilities to consumers and businesses through the NPP. Real-time payments improve overall market efficiencies in the economy by allowing institutions to make funds available in recipients’ accounts immediately without settlement or credit risk. We note the RBA’s Payment System Board statement “... *that while restrictions on*

¹ https://assets.publishing.service.gov.uk/media/65eed7233649a26deded630f/Policy_note.pdf

² <https://www.rba.gov.au/payments-and-infrastructure/payments-system-regulation/past-regulatory-reviews/strategic-review-of-innovation-in-the-payments-system/conclusions/>



*individual payments – such as blocks, delays and limits – can help to reduce scam losses, consideration should be given to the relative risk of payments and any impact on end users, other participants and the payments ecosystem”.*³ Clarification to ensure that civil penalties apply at a systemic level would allow banks to employ more targeted interventions to high-risk transactions using ‘intelligent friction’ as part of their processes for complying with the overarching obligations to prevent and disrupt scams, rather than introducing them more indiscriminately in a reactionary manner.

2.3 Definition of a scam

CBA supports the inclusion of a scam definition in primary law and the intent to define scams in a way that ensures it remains suitable for evolving and future scams activity. We also note in the draft Explanatory Memorandum that certain activity/conduct could be carved out through the Rules where the definition is considered to operate too broadly. A clear and workable definition of a scam is crucial to establish an effective SPF, particularly in clarifying the protections offered to consumers as well as the responsibilities of entities and the overall regulatory perimeter of the SPF.

Broaden the definition to ensure all scams are captured

As currently drafted, we consider the definition of a scam in s.58AG may not capture some common scams, such as remote access and phishing scams, and would welcome further clarity.

In deceiving consumers, scammers impersonate a range of organisations and people. Their deception is not limited to representations related to the regulated service or impersonation of a regulated entity, and the means used to deceive consumers are constantly evolving. For example, in the case of phishing, a consumer may click on a link from a search result, which is not paid advertising but nevertheless part of a scam. In some remote access scams, scammers may impersonate a well known trusted organisation and represent that there is an issue with their account or device. The scammer then persuades the consumer to download a remote access tool and, in some cases, it is the scammer who then makes transactions (as well as, or instead of the consumer).

To mitigate this, we propose:

- broadening the impersonation point in s.58AG(2)(b) to cover impersonating any third party; and
- broadening the actions taken in s.58AG(2)(c) to include actions by the scammer, for example:

(2) The attempt involves deception if the attempt:

- (c) *is an attempt to deceive the SPF consumer into facilitating an action **by the SPF consumer or by the [scammer]** using the regulated service; or*

As there is currently no definition of “scammer”, one would either need to be inserted or an alternative reference included here e.g. “person or persons involved in the attempt”.

Carve-outs outlined in Rules

We support the intention to use the Rules to carve out other types of fraud that do not involve any action from the consumer (such as credit card fraud), cybercrime, misleading and deceptive conduct and actions taken under threat of violence.

³ <https://www.rba.gov.au/media-releases/2024/mr-24-10.html>



We suggest that in doing this, for:

- fraud – attempts involving parties who are known to each other be excluded from the definition of scam;
- misleading and deceptive conduct – deception involving the exchange of goods and/or services be specifically excluded;
- threat-based fraud – in addition to excluding attempts involving threats of violence, the rules should also exclude other serious threats, for example reporting to government authorities (such as police and immigration), blackmail, or extortion etc. We support the Government’s Privacy reforms and other measures that address these harmful acts.

The draft Explanatory Memorandum indicates that the Rules will be used to carve out misleading and deceptive conduct within the meaning of the *Competition and Consumer Act*. It would be helpful if clarification could be provided on what type of activity is intended to be excluded from scope as a result of this rule and whether a similar carve out will be provided for misleading and deceptive conduct within the meaning of the *ASIC Act*, *National Consumer Credit Protection Act* or *Corporations Act*.

We recognise the difficulty of drafting a definition which is sufficiently broad and flexible to cover current and future scams, but which does not extend to a range of other fraudulent and deceptive conduct that is more appropriately covered by other laws. To provide greater clarity on the scope of the SPF, we suggest that to supplement the definition and ‘carve outs’, a list of scams that are within the scope of the definition and a list of activity which is not within the scope of the definition be specified in regulation by the Minister. By specifying this in regulations, the intended coverage of the SPF can be amended as the scams environment and threat evolves and be subject to industry consultation.

Align Scam Prevention Framework and ePayments Code

We believe there should be a clear delineation between the SPF and the ePayments Code to prevent duplication and overlap that will create confusion and uncertainty for customers. Minimal amendments could be made to the ePayments Code to remove scams from scope in time for the SPF to come into effect, and prior to the comprehensive review planned in 2025–26 as part of the payments reforms.

This will ensure the SPF and ePayments Code work in a complementary way as the ePayments Code will continue to cover mistaken and unauthorised payments for which it was designed, and the SPF will cover losses due to scams that involve a wider range of sectors.

2.4 Actionable scam intelligence

At CBA, we view the sharing of verified scams intelligence by entities across the ecosystem as a significant reform to protect customers from scams and to disrupt scammers quickly. Leveraging the collective knowledge of consumers, entities, and government to detect a scam and prevent it from being used by scammers, through timely information sharing and action, is crucial. However, we have concerns about how regulated entities will be able to implement the obligations related to actionable scam intelligence. Consideration should also be given to how intelligence sharing can be leveraged by other parties, such as the Australian Signals Directorate (ASD), Australian Cyber Security Centre (ACSC), as well as AUSTRAC and avoid duplication where possible.

Definition of actionable scam intelligence

The current definition of actionable scam intelligence, as outlined in s.58AI, is broad. As indicated in Note 1, any individual interaction with a consumer may give rise to a range of information which could be actionable scam intelligence, e.g. a URL, email address, phone number, social media profile, bank account,



information about the suspected scammer and information, including complaints, provided by SPF consumers.

We agree that gathering and reporting much of this information will help minimise the harm from scams. However, we suggest that the definition of actionable scam intelligence should be amended by:

- removing the requirement for the regulated service to be a regulated service of *the* entity and replacing it with a requirement for the actionable scam intelligence to be in relation to a regulated service of *any* regulated entity. For instance, sometimes a consumer may report to their bank that they received a scam text message from a particular phone number. Requiring the bank to report that phone number (if it is provided by a consumer), i.e. via the Anti-Scam Intelligence Loop, will assist other regulated entities to take action to block it. It should be clear however that the obligations only relate to actionable scam intelligence that a regulated entity has (which will include information provided by consumers, other regulated entities (e.g. through the Anti-Scam Intelligence Loop) or regulators. There should be no obligation to otherwise seek it out;
- removing the reference to “digital wallets” from the information listed in Note 1 to s.58AI and replacing it with “device”. When a scammer adds a consumer’s card to a digital wallet (e.g. ApplePay) on the scammer’s device, the digital wallet is not information which can be identified or reported and acted on. The relevant information is the device the scammer used to set up the digital wallet;
- removing the references to information about the suspected scammer and information, including complaints provided by the consumer. Generic ‘free form’ information such as this is not capable of being reported and actioned by other entities in an automated, efficient manner. Neither is it likely to be useful for preventing, detecting or disrupting scams. It will result in a significantly increased compliance burden for no discernible benefit. In contrast, specific data types such as URLs, email addresses, phone numbers, devices, social media profiles and bank accounts can be quickly reported and actioned to prevent further activity.

We note there are numerous obligations that rely on the concept of actionable scam intelligence and it would be helpful to provide clarity on how they are intended to operate given the broad nature of the definition. For instance:

- The Disrupt section (Subdivision F – SPF principle 5) includes a requirement to report actionable scams intelligence to the SPF general regulator, the ACCC (s.58BX(2)). We note that the volume of actionable scam intelligence reported will be enormous. We believe the reporting will need to be automated to allow uploading to a live portal, similar to the way the Anti-Scam Intelligence Loop currently works. However, to do this the intelligence will need to be limited to defined fields, such as “phone number” or “bank account”. It will not be practical to report “information about the suspected scammer” and “information, including complaints, provided by consumers”, and there may be privacy implications of doing so;
- The Report section (Subdivision E – SPF principle 4) also includes a requirement to report actionable scams intelligence (s.58BR(1)) and suggests that regulated entities will need to investigate and report in detail on individual (customer level) actionable scam intelligence about “a suspected scam”. In practice, this will not be possible given the volume of actionable scam intelligence captured under the current definition. It would be helpful if this requirement were amended to refer to a broader scam modus operandi, rather than “actionable scam intelligence” about “a scam”.



Ensuring information sharing is timely and actionable

We support information-sharing obligations under the SPF, including within the sector-specific codes. Regulated entities should be required to share data across sectors and meet requirements to act on the intelligence in a timely way.

Scams data shared among scams ecosystem entities will need to be transmitted using technology that is highly secure but also efficient and flexible to create confidence in the system. The Anti-Scam Intelligence Loop, which is part of the Australian Financial Crimes Exchange (AFCX), enables entities to share verified information with other participants and then to consume that data in near real-time. It is flexible to provide smaller entities with the ability to secure lower-cost technologies to participate and also to take advantage of emerging technologies over time.

Leveraging both the AFCX and NASC would enable all consumer scam data to be reported, thus enabling a more effective understanding of the number and type of scams that are occurring in Australia. This would provide a robust and credible data set that could be published by the NASC to help understand trends over time as well as helping inform the Government and regulators of any need to adjust the SPF so that it can work more effectively.

While recognising the role of reporting to regulators, we suggest that placing regulators in the middle of the reporting regime (as proposed in the Exposure Draft) will slow down data transfer and regulated entities' ability to act on data to protect consumers from scams. We understand the need for regulators to access timely and high-quality information, but we believe this can be achieved through the NASC and AFCX designing relevant reporting sets as an output of the Anti-Scam Intelligence Loop.

This is an approach employed in the cyber security space where it is recognised that entities need channels and platforms that facilitate real-time actionable data sharing as separate from regulatory information sharing, which tends to be too slow. The SPF could look to various public-private information sharing mechanisms that exist with a cyber security focus as a model for promoting real-time information sharing, such as ASD's Cyber Threat Intelligence Sharing (CTIS) service⁴, which is a two-way sharing platform that enables government and industry partners to receive and share information about malicious cyber activity at machine speed.

To ensure intelligence is being acted on by regulated entities in a timely way, a specific rule requiring action within a specified timeframe with a response back to the Anti-Scam Intelligence Loop confirming the action taken, could be used as part of specific liability rules referred to above.

The AFCX platform could also be used to automatically report failures to meet timeframes, with reports shared with the regulators under the SPF, streamlining the reporting requirements of entities and supporting regulators in their monitoring and enforcement role. It is important to leverage existing infrastructure and avoid duplication between public and private initiatives, such as the AFCX and the NASC.

Ensuring alignment with existing obligations

To be effective, industry initiatives to combat scam activity will necessarily depend upon consumer education and the sharing of scam intelligence with regulators, other regulated entities and consumers. This may include sharing some personal information and communicating information related to possible financial crime, and some of these communications will need to be made electronically in order to reach

⁴ <https://www.cyber.gov.au/about-us/view-all-content/news-and-media/join-the-cyber-threat-intelligence-sharing-service-through-sentinel>



consumers in a timely way. There may be circumstances when these activities conflict with other laws and therefore some other changes to legislation, including the *Privacy Act 1988 (Cth)*, the *Anti-Money Laundering and Counter-Terrorism Financing Act (2006) (Cth)*, and the *Spam Act 2003 (Cth)*, will need to be made to facilitate the sharing of information required under the SPF.

Essentially, exceptions under these laws would be required so that the SPF could require efficient information sharing between regulated entities, the NASC, AFCX and regulators such that:

- consumers may be informed about general scam education as well as specific scam indicators so that the consumer may take action to minimise their risk of harm or loss; and
- other businesses, the NASC, AFCX and relevant regulators may be informed about suspected or identified scam activity, without breaching privacy collection and disclosure principles, spam prohibitions, tipping-off prohibitions in the AML/CTF Act and implied contractual or equitable duties of secrecy which might otherwise apply.

A "reasonable use" exception could be included in the SPF so that contraventions of existing laws or other laws which may be relied upon as an impediment to disclosure, are not triggered where there is a "reasonable use". For example, a "reasonable use" exception would permit the sharing of suspicious matter information to prevent a scam being perpetrated even in instances where such sharing may otherwise be prohibited under the tipping-off prohibition in the AML/CTF Act. Further, we suggest that the SPF recognises the equivalent obligations under the AML/CTF Act to avoid duplication, for instance in relation to overlapping governance, procedures and reporting requirements.

To support efforts to combat scams, we consider that consumer education will play an important role in building knowledge about scam types, developing skills for identifying a scam as well as understanding how to protect oneself or one's business (such as through the use of multifactor authentication). Clarity on the role of government, regulators, the NASC, industry bodies and entities would be useful, particularly where it may overlap with cyber security strategies and messages.

2.5 Other matters

Future designation

We support the Minister's stated intention that insurance, superannuation and cryptocurrency will be designated in the second wave, whilst noting the urgency of regulating cryptocurrency due to its frequent use in the dissemination of the proceeds of crime. We encourage the Minister to also designate PSPs.

The Explanatory Memorandum states that the SPF is being introduced as part of a broader effort to modernise Australia's laws for the digital age. These reforms include modernisation of the payments system with payments licensing, a Common Access Regime, and the Consumer Data Right that will inevitably lead to greater participation in the payments ecosystem by non-banks.

Although we recognise the term "banking business" may be necessary to provide certainty when designating the sector, it is important to note that only a subset of "banking business" – payments and transaction accounts – relates to scams. These services are increasingly being made available by non-bank PSPs, leaving a gap in the SPF that can be exploited by scammers.

In Explanatory Memorandum 1.41, the statement that "*The Minister may exclude from that designation providers of purchased payment facilities; the SPF code obligations may not be appropriately targeted at this type of business because this service does not operate like a traditional banking business*" runs counter to Treasury's payments licensing reforms, which will impose the same obligations on purchased payment facilities (as "stored value facilities") regardless of whether the payments function is performed by an Authorised Deposit-taking Institution (ADI).



For example, PayTo allows customers to set up “payment agreements” with businesses or merchants that enables third parties to request a payment initiation message to be sent to the customer’s bank to process payments from the customer’s account, according to the terms the customer agreed to. The PayTo service provider that handles merchant onboarding and customer agreements has opportunities to identify high-risk transactions and prevent, detect and disrupt scams. The customer’s bank has limited ability to hold or decline a payment due to the NPP PayTo service level agreement, which is a prerequisite to participation in the scheme.

Excluding PSPs, other than banks, from being obliged to take steps to reduce scams and protect consumers, will create a weak link in the ecosystem at the outset, ultimately impacting consumers. The UK Reimbursement Rules apply to PSPs that are direct or indirect participants in Faster Payments as APP fraud performance data from the UK Payment System Regulator shows that smaller non-bank PSPs represent a disproportionately high level of fraud received.⁵ Australia’s fast payment system, the NPP, also allows PSPs to connect directly and indirectly to enable transactions, limiting banks’ ability to manage risks. We are already seeing higher risk of scams on PayTo transactions originating from certain PayTo service providers as scammers seek to exploit these vulnerabilities.

In many cases the obligations of banks and PSPs in relation to scams will be similar. For example, implementing processes to limit payments to high-risk payment channels; implementing increased warnings and payment delays; and having in place methods or processes to identify and share information with other entities and to act quickly on information that identifies an account or transaction is likely to be, or is, a scam.

Definition of SPF consumer

The definition of SPF consumer in s.58AH would benefit from greater clarification, as in its current form obligations under the SPF would have a broad application that we expect was not intended. For example, detection obligations under s.58BO(1)(b) require a regulated entity to “take reasonable steps within a reasonable time to identify each SPF consumer of that service who is or could be impacted by the suspected scam”. In effect, this would mean a regulated entity would be required to identify all Australians and Australian businesses with less than 100 employees given the definition of SPF consumer.

The definition of SPF consumer extends to businesses with less than 100 employees with a principal place of business in Australia. This may inadvertently catch entities which are part of large, sophisticated business operations. To address this, we suggest that there be an exception for:

- related entities of businesses with 100 or more employees even if the entity itself has less than 100 employees. An example of this is a special purpose vehicle subsidiary of a multinational regulated entity; and
- regulated entities and their associates.

We note that proposed amendments to the UK Payment System Regulations to allow payment delays of up to four days in the case of suspected fraud includes a provision allowing small, medium, and large businesses, which may have numerous obligations to make timely payments to suppliers, to opt out of the provisions with the mutual agreement of their payment service provider.⁶ Given the potential for disruption to some businesses by payment holds, we consider a similar opt-out provision should be considered under the SPF. This would be appropriate for sophisticated businesses with low numbers of employees that seek to move large sums without friction and have their own internal risk management and controls. There

⁵ <https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/>

⁶ https://assets.publishing.service.gov.uk/media/65eed7233649a26deded630f/Policy_note.pdf at 4.4.



should also be consideration of the appropriateness of including PSPs, that tend to be smaller and may fall under the proposed definition of 'consumer' but have core responsibilities to ensure safety and security when moving customer funds. Designation of PSPs as a regulated sector under the SPF would alleviate this concern.

AFCA authorisation conditions

Section 58DC(1) enables the rules to prescribe certain requirements for an EDR scheme. This rule making power is limited to a newly established EDR scheme. It seems less clear that this is possible with an existing scheme like AFCA, but conditions can be applied to authorisation (s.58DB(2)). We suggest that either this provision be extended to existing schemes (or clarification provided that s.58DB(2) can be used) to establish new terms of reference, requiring compensation to be determined strictly in accordance with specified liability rules. As set out above, we believe that new terms of reference and operating rules will be required as part of the authorisation conditions for AFCA. We do not consider that AFCA's existing jurisdiction and operating rules will be fit for purpose given the different role that AFCA will be playing as a "one stop shop" compensation complaint body.

Examples of sector specific codes

The Explanatory Memorandum provides some examples of sector-specific codes. The Banking Code example includes references to "transactions that appear out of character" and "verify payee details before transferring funds". We suggest these references be removed and replaced with the commitments outlined in the ABA Scam Safe Accord.

Referral of settled complaints

Section 58DD allows the EDR scheme to refer settled complaints to a regulator. This is likely to have the effect of discouraging regulated entities to resolve complaints at IDR, even where they are not at fault, in order to assist the customer. Settlement of claims being considered by the EDR scheme should be able to occur on a confidential basis without disclosing the terms of the settlement to the regulator. Alternatively, if this provision remains, the grounds for forming the view that settlement requires investigation should be clearly stipulated.

Action for damages

Section 58BZ allows a person who has suffered loss as a result of a contravention of a civil penalty provision to bring an action for damages. We question whether IDR/EDR rights should cover the field for victim compensation. Or is this provision intended to give regulated entities the right to recover compensation paid to consumers from other regulated entities? If so, we suggest that this be clarified.

