

4 October 2024

Mr Aidan Storer
Assistant Secretary
Scams Taskforce
Market Conduct Division
Treasury

Via email: scampolicy@treasury.gov.au

Dear Mr Storer

Exposure Draft Scams Prevention Framework

COBA thanks Treasury for the opportunity to provide feedback on its exposure draft legislation to establish the Scams Prevention Framework (SPF).

COBA represents Australia's customer owned banks (mutual banks and credit unions). Collectively, our sector has over \$170 billion in assets, around 10 per cent of the household deposit market and around five million customers. Customer owned banking institutions account for around two-thirds of the total number of domestic Authorised Deposit-taking Institutions (ADIs).

Key points

COBA strongly supports the Government's intention to create a consistent ecosystem framework created through this legislation, including its capacity to expand to other sectors such as digital marketplaces and cryptocurrency exchanges.

COBA supports each sector having a legislated code and that pre-existing industry codes should not be accepted as a substitute. We strongly oppose any sector being designated under the SPF (i.e. subject to only general obligations) until the respective legislated codes are developed. This is due to the concerns about interpreting and operationalising broad obligations without codes in place.

COBA remains concerned with the proposed multi-regulator model. While we note the efforts to ensure consistency, there may be differing levels of scrutiny and regulatory oversight applied by sector regulators. We continue to support the ACCC being the sole SPF regulator for all sectors

COBA supports a single external dispute resolution (EDR) scheme as the simplest means to resolve consumer disputes. However, there are many questions around how this works in practice, particularly with multiple internal dispute resolution (IDR) processes and the sharing of liability with telecommunications providers and digital platforms. We look forward to continuing to work with the Government on these issues.

Suite 403, Level 4, 151 Castlereagh Street,
Sydney NSW 2000

Suite 4C, 16 National Circuit,
Barton ACT 2600

[Customerownedbanking.asn.au](https://customerownedbanking.asn.au)

COBA is concerned with the legislation's complexity and the regulatory burden that could be created, especially for smaller banks. We are particularly concerned with the various reporting obligations throughout the SPF Principles. As it stands, there is the potential to lead to a regime focused too much on reporting rather than protecting customers from scams. The complexity of these obligations evidences why the SPF code must be created before designation, as key details on how to comply with the SPF Principles will be within these codes, without which our members will lack clarity in how to meet their obligations under the SPF.

In approaching these obligations, Treasury must clearly indicate considerations around proportionality and the scale, size and complexity of the regulated entities in reasonable steps. What may be considered reasonable steps by the major banks or large multinational digital platforms is not necessarily reasonable or practicable for a small-medium sized bank.

Ultimately, the proposed SPF legislation should focus on being enabling legislation with the detail in subordinate legislation such as the designation instrument, SPF rules, reporting rules and sector codes. This approach will allow sufficient consultation on critical regime details and allow the regime to be easily adjusted to improve its effectiveness to combat both current and new scam typologies.

The scourge of scams adversely impacts many Australians and customer-owned banks are committed to this fight to protect their customers. We congratulate the Government for bringing forward these measures and believe that these provide good next steps in combatting scams that builds on the strong actions already being taken by banks through the COBA-ABA Scams-safe Accord.

COBA provides detailed commentary on key issues arising from this consultation in **Appendix A**.

We note that Treasury has sought information on expected costs and/or resourcing impacts arising from these changes. However, we are unable to do so in detail due to the highly truncated consultation being undertaken. Some broad anticipated compliance costs that are likely to arise for our members from the SPF as proposed include:

- Significantly increased reporting and compliance costs, including for the new annual certification regime.
- Costs associated with implementing system enhancements to meet new requirements.
- For IDR, there will likely need to be additional resources to support the expected increase in complaints volume. Additionally, due to the complexity of scam complaints, it is likely that these additional resources will need a different and higher skill set to manage the technical aspects.
- Training and change management costs.

We further note that this consultation coincides with consultations being conducted on significant changes to the Anti-Money Laundering and Counter-terrorism Financing (AML/CTF) regime, privacy laws, and artificial intelligence. This further highlights the importance of the Financial Services Regulatory Initiatives Grid that is currently under development and the need for improved coordination between Government departments and agencies to ensure an orderly consultation and implementation process.

We look forward to engaging with Treasury on this issue and thank you for taking our views into account. Please do not hesitate to contact Robert Thomas, Policy Manager (rthomas@coba.asn.au) if you have any questions about our submission.

Yours sincerely

A handwritten signature in blue ink, appearing to read 'Michael Lawrence', with a stylized flourish at the end.

MICHAEL LAWRENCE
Chief Executive Officer

Appendix A – COBA’s response to key issues

Key issue	COBA’s comment
Definitions	
Scam	<p>COBA believes that the definition of ‘scam’ proposed in the SPF has improved significantly over the proposal in the previous consultation, but it remains broad, and we seek the following clarifications:</p> <ul style="list-style-type: none"> • Potential overlap with ePayments Code, for example, with remote access scams these could be covered by ePayments where the scammer has gained access to the victim’s account and makes unauthorised payments. • Potential overlap with misleading and deceptive conduct in the Australian Consumer Law. • Interaction with current work underway by government on addressing financial and elder abuse.
SPF consumer	<p><i>Breadth of definition</i></p> <p>COBA is concerned that the definition is too broad in that it includes individuals who are not customers of the banks. While we understand the desire of the Government to create a broad net, we wish to highlight that this creates significant complexities for our members being able to meet their obligations under the SPF Principles. The broad definition means that our members would have to contemplate and take actions regarding people that they have no or little knowledge of, or capacity to interact with. For example, under s 58BK(2), it is difficult for banks to provide warnings to each SPF consumer who is not already a customer and on whom they have no or limited information in order to contact them. Additionally, under s 58BO potentially creates an obligation on banks to try and trace every single non-customer who has made a payment into a potential scam account held by the bank. If so, this would be administratively onerous.</p> <p><i>Application to business</i></p> <p>While COBA supports including small businesses within the definition, we are concerned with the proposed inclusion of businesses up to 100 employees as these are not currently considered to be ‘small businesses’ under the law. We believe it is more appropriate to align with the definition of ‘small business’ that is provided for in s 23 of the <i>Fair Work Act 2009</i> which provides that a small business employs fewer than 15 people. We believe that this aligns more closely with the policy intent to protect those businesses that: may lack the resources to have a comprehensive scams protection approach; is at greater risk of a single point of failure; and where a scam loss could be more debilitating to its survival. We believe that businesses with up to 100 employees have vastly more resources and are better placed to have appropriate protections in place.</p>

Key issue	COBA's comment
	<p>An additional consideration is how will our members be able to know or validate that a 'scammed' business meets the employee definition. It is not clear how our members would be able to easily discern and authenticate that a business meets the definition and is covered by the SPF.</p> <p><i>Overseas application</i> Further clarity is needed on how the SPF will operate in relation to the overseas Australian element in the definition. It is not clear on how this will work in practice and what will be required of regulated entities/sectors.</p>
Actionable scam intelligence	<p>COBA is concerned with this definition as it is very broad and, on our reading, almost captures all kinds of information in all situations. This makes it very difficult for our members to understand and to know what to do and when to do it. This is especially the case in that our members will hold intelligence on the victim rather than on the scammer which impedes their ability to meet all their obligations under the SPF. As noted elsewhere in our submission, obtaining or sharing the intelligence is further complicated in that it could breach privacy obligations.</p> <p>The sheer volume of data and information being contemplated by this definition means that what is expected from the obligations may not be reasonably achievable. This is because there will be too much information to analyse and to respond to, for example, actionable scams intelligence could include:</p> <ul style="list-style-type: none"> • Scams reported by customers. • Information identified through internal transaction monitoring. • Reporting in industry news. • Information from AFCX. • IDR/EDR complaints. <p>To assist in the drafting of this definition, the information that our members consider to be actionable intelligence that would assist them includes the following:</p> <ul style="list-style-type: none"> • BSB and account numbers of banks that funds are going to. • Phone numbers provided by scammers (if applicable). • The type of scam. • IP address if it is different from the genuine customer.
Framework	
Contributory negligence	We are concerned on the Bill's and the Explanatory Material's silence on the role of contributory negligence by the consumer. The SPF appears to assume that all liability or negligence will lie on the regulated entities/sectors, which appears to contradict the Government's public comments on the SPF.

Key issue	COBA's comment
	<p>The Government has indicated that the liability will fall on the regulated entities/sectors where it can be shown that they failed to meet their obligations and if they have met their obligations than consumers will need to wear the liability for the loss. For clarity, it may be worth including this explicitly within the Bill and consideration could be given to including a similar provision to cl 11 of the ePayments Code that provides for contributory negligence on the behalf of the consumer. A clear provision outlining the role of consumer liability will also assist consumers in that the existence of the provision can be referred to by regulated entities/sectors and AFCA in dealing with complaints under IDR/EDR.</p> <p>An additional consideration from a banking perspective is the banker's duty requires banks to follow their customer's instructions. The proposed provisions are silent on how banks can complete their due diligence obligations under the SPF where customers refuse to answer questions or provide information to the bank, whether this occurs because the customer is choosing to do so for private reasons or if they have been coached to do so by the scammer.</p>
Participants	<p>COBA supports a consistent framework model presented in the proposed SPF and its capacity to be expanded to include other sectors including digital marketplaces, crypto exchanges, insurance and super. However, we would reiterate our preference that digital marketplaces and crypto exchanges be included from the beginning of the regime. We understand that the Government is seeking to deliver benefits and protections for consumers, however, we do not see why a social media company has been included but its marketplace has not been. Especially as its marketplace is a significant source of scams.</p> <p>We also ask, regarding digital platforms, whether this is specifically targeted at social media operators or whether domain name administrators will be included? This is because website spoofing is a key conduit for scams, and it would be appropriate to create accountability for these entities as well.</p>
Multi-regulator model	<p>COBA remains concerned with the proposed multi-regulator model. We note the provisions and efforts being made in the SPF to attempt to ensure consistency in approach. However, we continue to be concerned that due to differing regulatory approaches and cultures within the proposed sector-specific regulators that there is significant risk that sectors will be subject to differing levels of scrutiny and regulatory oversight. We continue to support the ACCC being the sole regulator for the SPF.</p>
Designation of sectors and interaction with codes	<p>COBA strongly opposes the designation of any sectors under the SPF until the respective sector specific codes and their obligations have been developed. The SPF imposes very broad obligations and exposes entities to significant penalties for breaches. The designation of sectors without the accompanying detail would be complicated and not in the interest of consumers or regulated entities. The proposed option of designating sectors without codes would create uncertainty for all involved and see convoluted</p>

Key issue	COBA's comment
	<p>circumstances in the treatment of scams as some will be pre-SPF commencement, others will be post-designation but pre-code, and others will be post-designation and post-code meaning that entities will need to have different practices and responses to each. This will create complexity for AFCA and the regulators in determining what obligations apply and how they apply.</p> <p>An alternative is that some SPF Principles could come into force before others. For example, the implementation of the Governance Principle could be achievable without the code.</p>
Commencement and transition	<p>As part of commencement and transition there will need to be clarity on when Government expects to make sector designations, when codes will be developed, when the IDR/EDR regime will be developed, and when will all entities and sectors need to be compliant.</p> <p>We believe that the SPF, at the very least, should not be implemented ahead of the implementation dates agreed to under the Accord. Our members are progressing their implementation of those measures per the Accord and should not be required to implement any of these measures early under the SPF. However, for simplicity, and to ensure that our members have sufficient time to implement any additional measures under the SPF, we believe a minimum of 12 months for implementation should be provided after the Rules have been developed. We consider this to be reasonable especially as it is likely that our members will also be implementing significant changes under the AML/CTF and privacy regimes at a similar time with each consuming significant time and resources.</p>
Legislated codes	COBA supports each regulated sector having a legislated code and does not support the continuation of industry codes for some sectors while others have legislated codes. However, we are concerned that there is a risk that the code development will not be coordinated between ACCC/ACMA/ASIC to create a consistent ecosystem wide approach especially regarding dispute resolution. Due to the multi-regulator model, we believe that there is a strongly likelihood that there will be inconsistent obligations and practices adopted.
SPF Principles	
SPF Principles and codes	It is currently unclear exactly how the SPF Principles and the codes will interact and the apportionment of responsibilities between these instruments. It is currently not clear how these will operate in practice particularly if code obligations were to be deemed by regulators, AFCA, or the court as being insufficient to meet the SPF Principles obligations.
Proportionality	COBA wishes to highlight the challenges that face our members in meeting some of the obligations under the SPF Principles due to their reliance on third party providers for core systems. This can limit the ability

Key issue	COBA's comment
	<p>of the banks being able to take similar actions as larger banks as they have less control over these systems. For example, a larger bank could more easily place greater limits or controls on account transfer limits as they own their systems compared to our members that rely on a third-party provider. This highlights the important of proportionality in approaching all the obligations created under the SPF and that flexibility needs to be provided so that differing sized entities can respond in different ways. The size, scale and complexity of regulated entities must be an active consideration in both the enforcement approach adopted by regulators and in the EDR approach of AFCA.</p>
Governance	<p>In general, this appears to be largely appropriate, however, we note that there could be some challenges in the obligations proposed and we seek clarification on some of the policy rationale. COBA asks whether consideration has been given to how these obligations are intended to interact with other existing governance obligations, for example, as required by APRA and through the Financial Accountability Regime.</p> <p><i>Annual certification – s 58BE</i> The completion of the annual certification within 7 days of the start of each financial year by a senior officer could be highly challenging for our members. This is because most of our members are heavily reliant on third party providers for key services and functions. It is expected that it will be highly challenging for all our members to obtain the appropriate certifications and assurance from these providers and to then review and seek internal approval all the appropriate material within the 7 days, noting these providers are retained by multiple members. Because of these challenges we believe that a more appropriate time period would be 30 days of the start of financial year as it is unclear what the justification of this urgency for review and approval is.</p> <p><i>Record keeping – s 58BG and s 58BH</i> COBA seeks more information on the obligation under s 58BG to hold records for 6 years and what the underlying rationale is and whether this period aligns with record retention standards. It is not clear what the justification is for the specific and prescriptive obligations for records to be kept. We submit that it would be more appropriate to limit the obligation to copies of the final version of records that are approved and certified annually by the senior officer. We also believe that the keeping of each risk assessment is appropriate.</p> <p>In relation to s 58BH, we believe that 5 business days is far too short of a period to provide a response. This appears to be an arbitrary period and will be difficult to action within time if there are significant volumes of scams and requests made by regulators. In addition, it is not clear how these requests will be</p>

Key issue	COBA's comment
	<p>triaged across the three sectors. We are uncertain what the time sensitivity is for these requests and why a more appropriate period such as 15 business days or a month is not provided.</p> <p>The Government should also consider whether these prescriptive times should be able to be determined by subordinate legislation (i.e., SPF Rules) to ensure flexibility in the event the legislated time is inappropriate.</p>
Prevent	<p>We believe that the burden of most of these obligations should primarily fall onto telecommunications providers and digital platforms as our members will have very limited ability to prevent scams from reaching consumers. For example, what options are available to banks to prevent scammers using fake websites as there are very limited tools available to banks to proactively prevent these actions.</p> <p>Under the general obligations without a code in place, it is likely that expectations will be created on banks to take certain steps that are neither reasonable nor practicable. COBA submits that the wording of the obligation in s 58BJ is too broad and should be limited to circumstances where regulated entities should be reasonably aware of the scam if they have complied with Principle 3 – Detect, or where the entity has actionable scam intelligence.</p> <p>We also have concerns about the practical implementation of s 58BK relating to warnings to SPF consumers – we have concerns that this could lead to warning fatigue given the broad definition of SPF consumer while also being impractical if the expectation is to tightly target individual customers in particular classes.</p>
Detect	<p>COBA generally supports the need to uplift and increase the use of data to detect and prevent scams. However, we are concerned about the impacts and practicality of some of these obligations due to the wide definition of 'SPF consumer'. Due to non-customers of the bank being captured there are obligations to detect and identify these non-customers which is likely to be difficult without further clarification from the code.</p>
Report	<p><i>Volume of reporting – impact on banks</i></p> <p>COBA is concerned with the complexity and the potential for the creation of significant burden that these obligations would create, especially for smaller banks. Based on the proposed obligations it is not clear if the reporting will need to occur in real time or whether delays in reporting will be acceptable. Regardless of whether the reporting is in real time or not, we expect that our members will need to allocate significant resources to undertake the reporting obligations which will consume much of their time. Based on these</p>

Key issue	COBA's comment
	<p>volumes we expect it may be challenging for our members to discern the actionable scams intelligence from this data and then to take appropriate actions.</p> <p>For example, it currently takes each of our members approximately an hour to complete a suspicious matter report (SMR) to AUSTRAC. Based on this, it is likely that generating the reports under the SPF will take a similar amount of time. The reports under the SPF and the SMRs to AUSTRAC are likely to contain very similar information and the need to create these reports will see significant likely duplication and double handling of the same information. This is likely to be exacerbated further in that many of our members operate separate units for combating fraud and AML/CTF which will both be managing the same material.</p> <p><i>Volume of reporting – impact on Government</i></p> <p>It is not clear what it is intended for the regulators to do with the sheer volume of information and data being provided to them. Based on the large amount of data, including personal information, that will be held by the regulators it additionally could create a 'honey pot' of data that could be targeted for theft by hackers. We believe that based on the proposed obligations the volume of reporting required will be significant for regulated entities and will likely overwhelm the regulators. We believe that this will occur because the obligations require both:</p> <ul style="list-style-type: none"> • An initial report of a suspected scam; and • Subsequent reports of these suspected scams. <p>Considering the volume of scams occurring every month and the likely duplicate reporting by numerous entities of the same scam we believe that the volumes of reports will likely not be manageable by the regulators. But even if this data is somehow able to be managed by the regulators, we remain unclear on what it is intended for the regulators to do with this information.</p> <p>We do not believe that the obligations here are necessary or helpful to the Government and will be duplicative of existing reporting obligations that already apply to banks to AUSTRAC under AML/CTF and to APRA under CPS 234. It is not clear who will be normalising the data to ensure that it is correct and is in a usable format.</p> <p>We understand that Treasury had intended to hold workshops to work through how the end-to-end data flows would work and impact on reporting. We believe such workshops would be beneficial, however, if it is unable to do so before the Bill is introduced then we recommend that the detail on these data flows be provided for in the Rules so that an appropriate analysis can be undertaken before the obligations come into force.</p>

Key issue	COBA's comment
	<p>Without key details in the Rules or within the code we believe that it will be difficult for our members to understand how a bank would comply with this regime.</p> <p><i>Reporting by third parties</i> It is not clear what the reporting role, if any, will apply to key third party providers. Many of our members are reliant on core banking and payments service providers for the provision of key services. It is not clear what their role will be in the SPF as these entities will often have key information on the scams that could be of value. Consideration could be given in some instances whether it may be more effective if these entities can report on behalf of smaller banks.</p> <p><i>Privacy considerations</i> The Privacy Act likely will need to be reviewed and amended to ensure that financial institutions are empowered to work together and to share personal information. Privacy considerations often have proven to be a challenge to the effective collaboration and sharing of data in these kinds of circumstances. We particularly note that the obligations in s 58BS and s 58BU would likely require the sharing of key personal information of scam victims, which could be a privacy concern.</p> <p><i>Alternative proposals</i> We propose in the alternative that aggregate, quarterly data of scams be provided to the regulators, and in the case of banks, via the AFCX. The regulators should then have the powers to seek and obtain more detailed information from the regulated entities via a regulatory investigation. This will ensure that the Australian Cyber Security Centre and other regulators will be gaining access to high level and meaningful data from regulated entities that will allow for a strategic view of the ecosystem and to monitor compliance. If anomalies are found or there are issues of concern the regulators would then be able to undertake more targeted and effective investigations to identify the core problems.</p> <p>If, however, the current model is preferred then we would encourage consideration be given to minimising the amount of duplicative reporting. For example, strong consideration should be given to ensuring that only a single report needs to be completed to a single regulator that will satisfy multiple regulator regimes, including SPF, AML/CTF, and CPS 234. Consideration could also be given to allowing AFCX to make these single reports on behalf of banks.</p>
Disrupt	<p><i>Tipping off in AML/CTF</i> COBA is concerned that due to the significant overlap between activities covered by the SPF and the AML/CTF regime that conflict could arise between the tipping off provisions of the AML/CTF regime and</p>

Key issue	COBA's comment
	<p>the obligations under Principle 5 – Disrupt. We suggest that this would need to be clearly resolved under the two separate legislative regimes prior to the commencement of the SPF.</p> <p><i>Reasonable steps to disrupt scams – s 58BW</i></p> <p>We note that there likely will need to be an uplift from members to be more effective in the use of transactional data to build the system rules that will allow them to identify and examine where multiple transactions are taking place on consecutive occasions for similar amounts. Scams often occur where there are several similar transactions that occur in sequence. This will take time for members to build out the resourcing and capability to effectively disrupt scam activity.</p> <p>While COBA is supportive of the adoption of objective tests throughout the SPF Principles, we are concerned by apparent confusion within the Explanatory Materials and in Government briefings on what is reasonable and practicable. We are concerned that some of the scenarios and examples used as suggestions for what is reasonable and practicable for banks to do to disrupt scams are neither reasonable nor practicable for our members to adopt.</p> <p>For example, in response to an impersonation scam it was suggested that it would be reasonable for banks to completely cease the use of SMS until the scam is brought under control. Such a suggestion is not reasonable or practicable as our members are reliant on the use of SMS for many security measures, such as when accounts or other products are opened or for the use of one-time passwords. Similarly, our members would not consider it reasonable to take down their website due to a bank impersonation website so we would not consider appropriate to do similar for SMS.</p> <p><i>Sharing information about scams – s 58BX</i></p> <p>We believe that to comply with this obligation that banks will be risk adverse and are likely to err on the side of issuing communications to their customers warning about scams or the potential risk of scams rather than not issuing the communications. This will likely see a dilution in the effectiveness of these communications as customers will quickly experience scams awareness fatigue and will likely ignore the communications thereby rendering them ineffective. Clear direction will need to be provided to banks in the code if this is to be avoided.</p> <p>COBA also questions the appropriateness of the 24-hour response time in s 58X(3)(a) as this seems excessively tight and it is not understood why this amount of time is needed over a more reasonable period of several business days. Additionally, it is not clear if this 24-hour period is business hours or simply hours. If the latter this could be challenging for smaller COBA members that often run minimal or no staff on weekends and public holidays.</p>

Key issue	COBA's comment
Respond	<p>COBA believes that these obligations are generally appropriate, however, we believe that for the IDR to be effective there needs to be a mechanism to coordinate complaints across sectors and/or a liability apportionment model. We believe it is likely that many if not most complaints through IDR will be made through the banks rather than the telecommunications providers and digital platforms. Additionally, any liability model should not absolve individuals of their responsibilities to take reasonable precautions against scams. The default position should be that regulated entities are not responsible for SPF consumer losses unless it can be shown that they have failed in their obligations under the SPF.</p> <p>Further comments on the IDR and EDR framework are discussed below.</p>
Additional Impacts	<p>The obligations and wide definitions will likely require our members to redraft their terms and conditions to incorporate these new obligations and to allow them to take the necessary actions required. However, we note that this redraft will face limitations in that our members will need to comply with unfair contract terms obligations that could limit the responsiveness of banks to potential scams. For example, the ability to allow a bank to unilaterally close an account without notice and without engaging with the customer may breach the unfair contract terms provisions.</p>
Privacy	<p>Due to the broad definition of SPF consumer our members will need to consider the impacts of scams on those non-customers with whom they do not have a contract or any other prior relationship with. Our members will likely need to collect the personal information of non-customers which will trigger obligations under the Australian Privacy Principles. It is not clear how our members are supposed to notify non-customers that their personal information has been collected or how to gain their authority to use and hold it. As such, the contact details and other personal information of victims will need to be shared between regulated entities which has significant implications as a collection notice has not been provided to the customer. We also note that even if this information is provided, due to the amount of public concern regarding scams it is likely to be difficult to convince these consumers that they are being contacted by a legitimate entity for legitimate reasons as they have no prior relationship with that organisation.</p> <p>Additionally, the obligation may also give rise to the need for our members to collect and hold the personal information of scammers to be able to take reasonable steps to disclose with consumers so they can act in relation to a suspected scam. This in turn has privacy considerations.</p>
Dispute resolution	
Single EDR	<p>COBA supports the adoption of a single EDR scheme as the simplest means for consumers to have disputes resolved.</p>

Key issue	COBA's comment
ePayments Code	Clarity will be needed on how the ePayments Code will interact with the SPF.
AFCA approach	<p>It is unclear on how AFCA will approach the SPF. It is likely that AFCA will need to do a significant uplift to understand the operations across the sectors and the complexities involved in the scam lifecycle.</p> <p>We believe that there needs to be a clear demarcation between the responsibilities of the regulators and AFCA. This means that there will need to be clear rules, and a clear approach set by the regulators to ensure that an ecosystem approach is taken with a collective focus and does not fall into silos.</p>
Transition of non-AFCA members	The process and timeline for the transition of the telecommunications providers and digital platforms to being AFCA members will need to be clearly resolved prior to any designation of any sectors.
Time limits to make complaints	COBA seeks clarity on whether there will be time limits on whether consumer will be able to lodge scams complaints to IDR/EDR. We believe it is appropriate that there be a period that a consumer must make a complaint in order for it to be considered by the IDR/EDR, similar in principle to a 'Statute of Limitations'. This is to ensure that scams complaints cannot be unduly raised many years after the event and the ability of the entity to take any meaningful action to address the scam. We believe that consumers should have 12 months from the date of the scam to lodge a complaint about a scam to the IDR/EDR scheme.
Interaction between IDR and EDR	<p>COBA has concerns with how the IDR and EDR processes might work together in practice, particularly in relation to the determination of liability. We look forward to continuing to work with the Government on these issues. In brief, our concerns cover:</p> <ul style="list-style-type: none"> • How will the AFCA process work, including the attaching of different entities to a complaint? • How will the consumer know that they have alternative IDR schemes available, in addition to the banking IDR? • There is a strong likelihood that banks will become the default IDR meaning that our members will bear more of the costs than telecommunications providers and digital platforms. Will there be a cost sharing mechanism? • How will the three IDR schemes work with the single EDR? • A potential lack of incentive for consumers to meaningfully engage with IDR. What prevents consumers from 'shopping around' for desired outcomes or defaulting to EDR regardless of the outcome? • Due to the likelihood that many matters will escalate to EDR, how will the significant costs of having AFCA complaints going to determination be managed across the sectors? • How will the apportionment and determination of liability occur in both EDR and IDR? • What processes will be in place to ensure consistency of decision-making across IDR?

Key issue	COBA's comment
	<ul style="list-style-type: none"> • How are attached entities to an EDR complaint supposed to manage a complaint that did not proceed through their IDR and was not aware of until it was attached to the EDR complaint? • Due to the attaching of different entities to complaints, our members will likely receive or be involved in complaints from non-customers. How are they supposed to manage these when there is no prior relationship especially with other regulatory obligations such as privacy? • Our members have obligations under <i>ASIC Regulatory Guide 271 (RG271) Internal dispute resolution</i>, how are they to comply with this if telecommunications providers and digital platforms do not have similar or appropriate processes in place to respond?
Penalties and enforcement	
Penalties	<p>COBA has the following concerns with the SPF's approach to civil penalties:</p> <ul style="list-style-type: none"> • While designating provisions as being civil penalty provisions we are concerned on the lack of greater specificity on what the amount of penalties capable of being awarded for a breach are, especially as the Tier 1 and Tier 2 system allows significant discretion in the awarding of penalties. • The volumes of penalty capable of being imposed under Tier 1 and Tier 2 appear to be very excessive and inappropriate for the regime. <p>While some regulated entities included in the regime may be very large multi-national corporations, our members are not, and the risk of penalties being awarded between \$10 million to \$50 million per offence will have a significant impact on our member's businesses. We believe that greater proportionality should be added to the penalties to reflect the size difference between our smallest members and the multinational digital platforms. For some of our smaller members, a penalty in the hundreds of thousands of dollars or up to a million dollars would still be a very significant penalty. The risk of these significant penalties could also have unintended consequences regarding the required capital our members would need to hold.</p> <p>Greater clarity is also needed on whether these penalties will only be applied for systemic breaches of the SPF or could be applied for relatively minor breaches. We also seek clarity on whether the penalties could come with personal liability, as some of our members are concerned that contraventions of the SPF could see some of the remedies applied against senior officers of the entity.</p>