2 February 2024

Mr James Kelly
First Assistant Secretary
Scams Taskforce
Market Conduct and Digital Division
Treasury

Via portal: treasury.gov.au

Dear Mr Kelly

Scams – Mandatory Industry Codes Consultation

COBA appreciates the opportunity to contribute to Treasury's consultation on the introduction of new mandatory industry codes relating to scam activity.

COBA is the industry association for Australia's customer owned banks (mutual banks, credit unions and building societies). Collectively, our sector has over $170 billion in assets and 5 million customers. Customer owned banking institutions account for around two thirds of the total number of domestic Authorised Deposit-taking Institutions (ADIs) and deliver competition and market leading levels of customer satisfaction in the retail banking market.

Banks' proactive action fighting scams to protect their customers

In November 2023, COBA and the Australian Banking Association (ABA) jointly announced the Scams-Safe Accord that will deliver key improvements to safety and customer experience in combating scams.

COBA appreciates the work that Treasury and other agencies have put into developing this framework to date. Recent years have seen a rapid evolution in how and how often consumers are targeted by scammers. This is a challenge across sectors, and we strongly support the Government's intention to take a whole-of-ecosystem approach. This is the only way to effectively tackle this challenge and ensure that the ecosystem participants (that is, consumers and industry) each do their fair share to make Australia a 'harder target for scam activity'. The banking industry's commitment in combatting this scourge can be seen in the joint COBA-ABA Scam-Safe Accord. This Accord commits our members to take the following actions:

- Banks will deliver an industry-wide confirmation of payee solution to customers.
- Banks will take action to prevent misuse of bank accounts via identity fraud.
- Banks will introduce warnings and payment delays to protect customers.
- Banks will invest in a major expansion of intelligence sharing across the sector.
- Banks will limit payments to high-risk channels to protect customers.
- Banks will implement an Anti-Scams Strategy.

While banks can and should take action to fight scams, it is critical that this ambition is matched across the whole ecosystem.

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

Suite 4C, 16 National Circuit,
Barton ACT 2600

Customerownedbanking.asn.au

Customer Owned Banking Association Limited ABN 98 137 780 897

Key points

COBA supports a consistent ecosystem approach to addressing scams. This includes an end-to-end approach dealing with all elements of the scam lifecycle. This approach requires uniform code models and whole of sector regulatory bodies to support fairness and consistency. Ultimately, we believe that this will make Australia a harder target for criminal activity by scammers compared to more fractured and misaligned models.

COBA supports a clear definition of scams that properly distinguishes between a scam and a fraud.

COBA supports a consistent code framework across all regulated industries. All regulated sectors should have the same type of code model. We do not believe it is appropriate to 'mix and match' models across sectors. In the proposed model, telcos are proposed to have an industry-reviewed code while others have legislated codes. A singular approach will ensure consistency across industries, and the addition of new activities as required.

COBA supports a sole regulator for scams across all sectors, rather than the proposed multi-regulator model. We suggest that the ACCC should function as this regulator to ensure there is consistency in enforcement and regulation. This is consistent with the ecosystem model set out in the paper.

The overarching obligations will need to be revisited to ensure that the framework is clear on its overall intent, while more detail can be provided in the specific obligations.

COBA supports in principle the specific banking obligations; however, we note concerns about the 'kill switch' proposal which may be overly complex and costly relative to the benefit to customers of smaller banks, particularly against the backdrop of significant technology investment to meet both the Scams-Safe Accord and the proposed industry code.

COBA supports a single external dispute resolution (EDR) provider model rather than a multi-EDR model. From a consumer perspective, this will be a much more seamless experience, and avoids a consumer needing to lodge complaints with multiple entities. It will also lead to fairer outcomes as decision-makers will be able to examine the conduct of all parties in the ecosystem, rather than just a single entity. Any compensation provided by EDR should acknowledge a broader notion of fairness between ecosystem participants.

Overall comment on the Framework

We welcome the Government's intent to take a 'whole of ecosystem' approach, however, we are concerned that the framework may fall short in this aspect. COBA supports an approach that targets all aspects of the scams lifecycle. Incentivising all parties in the scams lifecycle to take actions to stop scams will provide the greatest level of protection for consumers and businesses from scams.

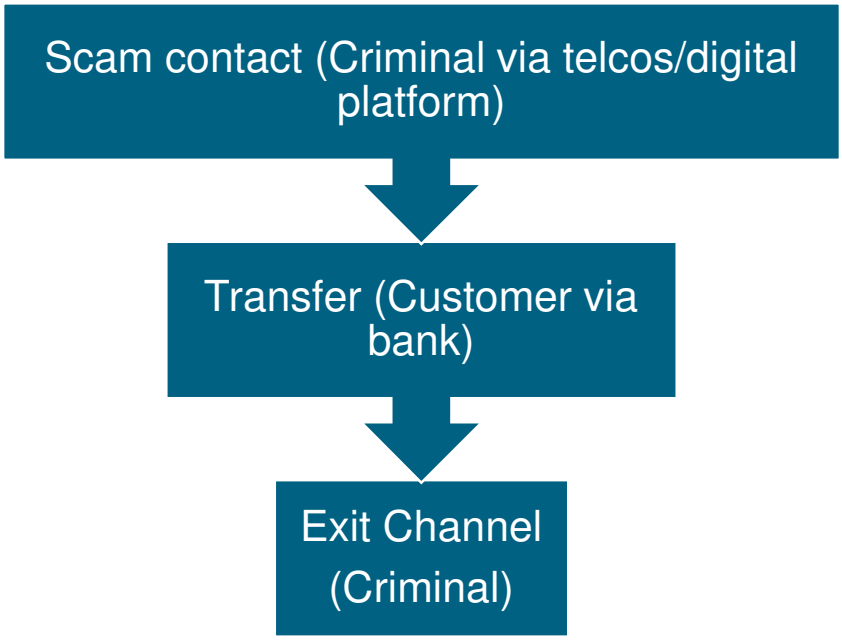
A 'successful' scam from a scammer's perspective typically involves several stages:

1. The scammer communicates with potential victims, often through the transmission of a text message or email, or through a fake online advertisement.
2. The consumer responds to the scammer's message or advertisement and asks their bank to make a payment to a third party. The bank actions the customer's payment request.[1]
3. The scammer takes possession of the customer's funds through exit channels.

[1] We note that in some cases, the scam is done via cash which can further reduce the bank's ability to detect and stop the transaction.

The scams lifecycle is like a funnel – all stages offer the opportunity for intervention to detect and prevent the scam. If scam activity is targeted at each stage, the number of ultimately successful scams will be reduced overall and at each subsequent stage.

This approach only works when all industries are similarly incentivised. If there is not consistent ambition across the whole ecosystem then the next stage in the lifecycle bears additional burden to prevent scams, and ultimately this puts more consumers at risk. We also consider there are efficiency and costs benefits in acting earlier to stop the scam in the lifecycle as the relative effort can be more efficient than further down in the chain (that is, the difference between stopping or warning of a scam contact, versus a conversation a bank needs to have with a socially engineered consumer who is determined to make a payment to a scammer).



Scammers contacting the consumer

In the ideal world, consumers would not receive scams calls, scams ads or scam texts in the first place. While this is not possible, more must be done at the 'front end' by those who have the scope to do so. This includes targeting scammers by law enforcement and relevant sectors taking actions to prevent consumers from receiving the scam contact. These activities narrow the pipeline and make it easier for subsequent stages in the lifecycle (that is, consumers, banks and exit channels) to protect themselves and their customers.

COBA believes that the framework and other Government law-enforcement actions announced to date makes a good start on addressing these 'front end' issues. However, more could be done within the framework so that those sectors with more capacity to prevent consumers receiving scams, like the telecommunications industry and the digital platforms, are obliged to take stronger action to prevent consumers receiving the scam in the first place.

While it may not be practical or possible to block all scams 'off the bat', once identified and reported swift action needs to be taken as soon as possible to 'takedown' reported scams to minimise the number of consumers that could potentially be impacted by the reported scams.

In line with our views to strengthen the 'front end, we believe the framework does not fully capture all the sectors that can make a meaningful difference in preventing consumers receiving scams and would benefit from including online marketplaces in the framework as part of phase 1. Online marketplaces are a major source of scams where consumers are offered or advertised the sale of non-

existent goods or services. While the inclusion of digital platforms will help assist in targeting scam advertising it only addresses part of the problem if online marketplaces are not included. Failing to include online marketplaces from the beginning will likely mean that scammers will shift from digital platforms to the marketplaces as a softer target.

Transacting via a bank

At this point, the customer has either handed over their personal credentials, allowed remote access to their device(s), or has authorised a transaction to a scammer. In many cases, the scammer has already convinced the customer to make the transaction and it can be too late for the banks to take actions to prevent the authorisation of the funds transfer and banks are now playing 'catch-up'.

For the framework to be successful it needs to address all stages of the scam lifecycle and not be solely focused on only one stage. Banks are, at best, the third 'gate' in the scams lifecycle if you consider the first 'gate' being the scam contact and the second 'gate' being the consumer. Each gate is an opportunity to stop the scam. We would be concerned if any framework becomes over reliant on the bank's role to prevent scams and to be liable for scam losses.

A major challenge for banks in managing scams is the customer's persistence with proceeding with the payment even when warned about the high likelihood that they are subject to a scam.
The framework's focus on trying to slow things down and gives customers more time to consider, while appropriate, will do little to prevent the loss of funds if the customer proceeds with the transfer despite advice against doing so. This focus, however, does not consider that banks are subject to the banker's mandate and that they must follow the customer's instructions in good faith (with regard to intent) even when the bank suspects that the customer is a victim of a scam. At this point, there is now a perceived shift to banks needing to move beyond just executing a customer's instructions to making subjective and probabilistic judgements on the quality of a customer's instructions, despite the customer wanting to make this payment and this money being the customer's money. Exercising these kinds of judgments creates the risk of legitimate transactions by customers being blocked by banks which exposes the bank to potential financial liability and/or reputational damage where customers suffer loss due to the blocked payment.

The framework also does not appear to have considered its impacts on the banker mandate if more liability for scam losses is shifted on to banks. The stricter liability framework creates incentives on banks to not follow customer instructions if banks are unsure about the transaction, thereby putting the bank in breach of the mandate and potentially causing loss by the customer. The effect of this is that customers will be losing full control over their own money which will have impacts that range far beyond scam related payments. Distinguishing between scams payments and non-scams payments is not a black or white exercise. However, because of the obligations imposed on them, banks will need to make probabilistic judgement calls to protect their customers and themselves from being victims of scams (that is, via compensation payments). This will have the likely impact that customers could be prevented from, or delayed, in making lawful and legitimate payments because of various red flags (false positives) in the name of protecting consumers from themselves. In some cases, banks may restrict services to protect customers from scams. We suggest that there is clear consumer communication by Government that these measures and inconveniences exist to protect them.

Scammer moving into possession of the customer's funds.

COBA is concerned that the framework appears to do very little towards the end of lifecycle when the funds leave the banks (that is, currently the last participant in the proposed scams code framework). Accountability needs to be set for those participants who enable scammers to access the customer's funds, for example, cryptocurrency exchanges, money remittance businesses, gambling platforms, and other payment systems (for example, PayPal). There are very little banks can do to retrieve scammed customer funds if they have exited the banking system. Making it harder for scammers to access these funds hardens Australia as a target as it reduces the incentives for scammers to operate in Australia. A more proactive approach would require these exchanges to be included as phase 1 sectors of the framework instead of it being added at a later point. This would ensure greater

consumer protection and reduce the likelihood of consumers who are victims not being able to recover the lost funds.

The role of the consumer

We note that this consultation focuses purely on industry codes and obligations on industry. Consumers play a key role in collective efforts to combat scams, and it is important the framework protects customers, while also ensuring it does not remove incentives for customers to protect themselves.

As outlined above, taking a full ecosystem approach also involves providing support for consumers to detect the red flags that can indicate scam activity.

Elements of this include governments and businesses:

- trying to avoid legitimate communications that include scam 'red flags',
- providing guidance and advice to consumers about common scam types and indicators,
- warning customers about specific scams during periods of heightened scam activity, and
- ensuring there are ways for customers to contact the agency or organisation to verify whether a message or advertisement is a scam.

Given the consumer's role as a 'gate' in the scam lifecycle, there needs to be clear incentives for consumers to take reasonable steps to protect themselves from scams. A key factor in scams (versus, for example, a fraud) is the role of the customer, as it involves an act of the customer to provide consent or divulge information that allows the acquisition of the funds by the scammer. We address this further below under 'Definition of a scam'.

Overall, we believe that more work is needed on key aspects of the proposed scams code framework. We have provided detailed response to the questions asked by Treasury in its Consultation Paper in **Appendix A**. We have also provided detailed comments on the both the proposed overarching obligations at **Appendix B** and to the proposed specific obligations for banks at **Appendix C**.

We will now provide a high-level overview on key issues of the framework below, covering:

- Definition of a scam.
- Design of the framework.
- Obligations under the framework.
- External resolution of scam disputes.

Ensuring a clear definition of scam that does not conflate with fraud

COBA supports defining a scam; however, the definition proposed needs to be made clearer. The proposed definition fails to properly distinguish between a 'scam' and a 'fraud'. The proposed definition fails to recognise a key difference between a scam and fraud being that a scam includes an intentional act by a customer to make a payment or to divulge information due to the dishonest invitation, request, notification or offer.

A scam necessarily involves the intentional act or consent from the customer in order to facilitate the financial benefit to the scammer, whereas a fraud does not. An examination of the offence of fraud will see that it provides: a person who by deception or dishonestly obtains the property belonging to another, or obtains any financial advantage or causes any financial disadvantage is guilty of an offence.[2] This means an offence that is a fraud is caused regardless of the victim's involvement, awareness or consent, however, for a scam to be effective it must include the involvement of the customer in providing consent or disclosing information even if that has happened with a deception by the scammer that facilitates the acquisition.

[2] See, e.g., *Crimes Act 1900* (NSW), s 192E; *Crimes Act 1958* (Vic), s 82.

COBA supports the intention of Treasury, as noted in the Consultation Paper, to exclude unauthorised fraud and consumer disputes.

Simplifying the framework design and application

COBA is concerned with the proposed framework as it is highly confusing and overly complex. The confusion in the model can be highlighted by discussing the proposed legislative model and the proposed regulator model which do below.

Proposed legislative model

COBA supports adopting a legislatively simple model, with one primary Act that empowers the codes and does not rely on a complicated legislative system to empower the sector codes. A simpler legislative model will make it easier to comply with and will make it easier to add future industries into the regime.

We believe that the proposal to use the *Competition and Consumer Act 2010* (Cth) (CCA) as the primary law seems appropriate for establishing the regime, creating an enforcement regime, and to outline the overarching obligations. However, the inclusion of additional Acts, like the *Telecommunications Act 1997* (Cth) and other ASIC and ACMA administrated Acts, to create the sector specific codes and standards will add needless complexity and has the potential to limit consistency of approach across industry and regulators. Having multiple Acts having to be amended and needing to communicate with each other will add complexity to the framework.

The Consultation Paper is unclear on what form the sector-specific codes will be in or how they will be created for the banks and the digital platforms. Our view is that all codes should be made as subordinate legislation as it will make it easier to update the codes to be reflective of changes in approaches and practices of scammers while also ensuring that it is binding on regulated sectors. However, it would be simpler if these instruments were all made under the same primary law, like the CCA, rather than being empowered under disparate Acts as is currently proposed. Legislative simplicity and ease should be key goals in the development of the framework as it will make it easier for the regulated sectors to comply.

Another concerning element with the legislative model will be the split Ministerial accountabilities due to the multiple laws and regulators involved. When there are shared or split responsibilities between Ministers it can create uncertainty in the regime due to the competing priorities of the Ministers. This would likely affect the ability of the regime to be able to develop quickly, flexibly, and consistently to changes in the scam environment. Having a single primary Act with all the codes made under this Act with a single responsible Minister will create more certainty and encourage consistency in regulatory approach.

To support consistency, COBA's view is that all industry sectors should be subject to the same code development processes and forms. This will ensure the same level of ambition and application in all codes and make it more consistent. This will become especially critical when it comes to regulator enforcement, dispute resolution and expanding the framework to new sectors. At present, it appears that the telecommunications sector will be subject to a different process to the digital platform and banking sectors which is of concern to COBA.

Multi-regulator model

COBA supports the adoption of a single regulator model to enforce the scams code framework and sees that the ACCC is the most appropriate agency to be appointed to this role.

The Consultation Paper has proposed a multi-regulator model made up of the ACCC, ASIC, and ACMA to administer and enforce the regime. The Paper provides minimal detail on how this would work in practice with vague references to Memoranda of Understanding and to a general expectation that they should 'work closely together'. We are highly concerned with this proposed model and wish to indicate our strong opposition to it.

The key principles in developing a regulator model should be:

- Take a whole of ecosystem approach.
- Consistency in regulator approach to regulated sectors.
- Efficiency and effectiveness of compliance activities.
- Accessibility for consumers.
- Minimising complexity for consumers and regulated sectors.

We do not believe that the proposed multi-regulator model meets these principles, and we are concerned that there is a high chance of failure with the proposed model. Our concerns can be summarised as follows:

- The framework will be complex and administratively difficult to administer as each regulator has their own individual obligations and mandates that may conflict with each other and the broader scams code framework.
- There is a strong likelihood of inconsistent application of the codes and the law – made especially so per our comments above regarding the complexities of the legislative regime.
- There could be siloing and shifting of responsibilities (so called 'buck passing') between the regulators.
- Likely to create accessibility issues for consumers not knowing who the appropriate regulator is and creates risks that certain regulators and sectors will experience more compliance activity if viewed as more likely to gain a favourable outcome from a specific regulator over the others.
- A high likelihood of inconsistency and confusion in messaging by the regulators communicating different things to different sectors.
- It is unclear how this model will be expanded to include other sectors – will other regulators be brought into the regime will the existing regulators take responsibility?
- The inclusion of multiple regulators means that there will be a sharing of responsibility between multiple Ministers that will make it harder for Parliament and the public to know and to hold the appropriate Minister responsible for the administration of the scheme.

COBA's strong preference is for there to be a single regulator. The most appropriate of the three regulators to serve this role would be the ACCC. The other regulators could have input into the development of the codes and other aspects of the regime, but the clear enforcement role should lie with the ACCC.

Of the three regulators, the ACCC and ASIC both currently regulate all three sectors while ACMA is a specialised communications and media regulator, which indicates it should be either the ACCC or ASIC that has primary responsibility. However, our view is that scams should be seen as a consumer issue and due to the framework being empowered by the CCA the appropriate regulator should be the ACCC.

If the multi-regulator model is pursued, which COBA strongly opposes, then strong consideration should be given to effectively manage these issues with very clear delineation of responsibility and protocols in how the relationships between the regulators are to be managed and how investigations and enforcement actions will be conducted. The joint regulator model of the Financial Accountability Regime between ASIC and APRA could provide some guidance, however, as the regime has not yet commenced, we are unable to comment on its effectiveness as a model.

Clarifying the obligations under the framework

While COBA considers the proposed overarching obligations and the specific obligations as an appropriate place to start to cover existing scam typologies, further work is needed on these obligations. Flexibility will be needed in the method to developing obligations in order to respond to the changes of approach by scammers.

Given that consumers also play a key role in collective efforts to combat scams, it is important to ensure that there are adequate incentives for customers to protect themselves, alongside the incentives for regulated sectors to protect customers.

COBA believes that the overarching obligations will need to be revisited to ensure that the framework is clear on its overall intent, while more detail is needed in the specific obligations.

COBA also expresses its concern around the proposal in the specific obligations for banks to develop a so-called 'freeze' or 'kill switch'. This will be an overly complex and costly for smaller banks to deliver relative to the benefit provided to consumers. We address our concerns in more depth in **Appendix C**.

Our full comments on the overarching obligations can be found at **Appendix B** and on the specific obligations proposed for banks can be found at **Appendix C**.

Addressing external dispute resolution of scam disputes

COBA supports establishing a single EDR to manage scams-related complaints. We are concerned that the multi-EDR model proposed will have many of the same flaws as the multi-regulator model. These flaws include:

- Complexity and poor consumer outcomes.
- Siloing.
- Inconsistency between the sectors in both the awarding of determinations and the application of code provisions.
- Lack of clarity in how future industries would be incorporated into the regime.

COBA does not currently have a preferred means of delivering this single EDR be it by establishing a new scams ombudsman or empowering an existing body. COBA notes that an existing body may need to be adapted to take on this role when it comes to existing mandate, decision factors and operations. We welcome working with Treasury and the other agencies further to determine the most appropriate body.

We look forward to engaging with the 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

MICHAEL LAWRENCE
Chief Executive Officer

Appendix A – COBA response to consultation questions

Question #	Question	Comment
Proposed Framework		
1	Does the Framework appropriately address the harm of scams, considering the initial designated sectors and the proposed obligations outlined later in this paper?	If various issues are fixed, the framework could potentially address the harms of scams via an ecosystem approach targeting all parts of the scam. We are concerned that the framework is unclear due to: • Lack of clarity in the definition of the scam (addressed at Q10) • Clearly outlining what is the problem attempting to be solved, and • How the framework proposed will resolve this problem (addressed throughout our responses to the questions).
2	Is the structure of the Framework workable – can it be implemented in an efficient manner? Are there other options for how a Framework could be structured that would provide a more efficient outcome?	COBA considers the framework to be excessively complex which will make it harder to implement and apply the framework. For the reasons below we believe that the framework should be kept legislatively simple, with one primary Act which empowers the codes and is enforced by a single regulator (addressed more in Question 3). The framework, if not developed on a technology and process neutral basis and has the potential to create disproportionate costs for the customer owned banking sector relative to the benefit given our smaller customer bases. If particular technologies are mandated than this reduces the flexibility of our sector to meet the intent in cost-effective and efficient manner. Smaller banks, such as customer-owned banks, are also reliant on third parties to implement technology changes. This factor combined with the smaller scale of our members may need longer implementation timeframes.
3	Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?	***Legislative model*** We believe that the proposal to use the *Competition and Consumer Act 2010* (CCA) as the primary law seems appropriate for establishing the regime, creating an enforcement regime and to outline the overarching obligations. However, the inclusion of additional Acts, like the *Telecommunications Act 1997* and other ASIC and ACMA administrated Acts, in order to create the sector specific codes and standards will add needless complexity and has the potential to limit consistency of approach across industry and regulators. Having multiple Acts having to be amended and needing to communicate with each other will add complexity to the regime The Consultation Paper is unclear on what form the sector-specific codes will be in or how they will be created for the banks and the digital platforms. Our view is that all codes should be

		made as subordinate legislation as it will make it easier to update the codes to be reflective of changes in approaches and practices of scammers while also ensuring that it is binding on regulated sectors. However, it would be simpler if these instruments were all made under the same primary law, like the CCA, rather than being empowered under disparate Acts as is currently proposed. Legislative simplicity and ease should be key goals in the development of the framework as it will make it easier for the regulated sectors to comply. Another concerning element with the legislative model will be the split Ministerial accountabilities due to the multiple laws and regulators involved. When there are shared or split responsibilities between Ministers it can create uncertainty in the regime due to the competing priorities of the Ministers. This would likely affect the ability of the regime to be able to develop quickly, flexibly, and consistently to changes in the scam environment. Having a single primary Act with all the codes made under this Act with a single responsible Minister will create more certainty and encourage consistency in regulatory approach. To support consistency, COBA's view is that all industry sectors should be subject to the same code development processes and forms. This will ensure the same level of ambition and application in all codes and make it easier. This will become especially critical when it comes to regulator enforcement, dispute resolution and expanding the framework to new sectors. At present, it appears that the telco sector will be subject to a different process to the digital platform and banking sectors which is of concern to COBA. ***Multiple regulators*** Our preference is for a single regulator model, the ACCC being the most appropriate. We are highly concerned that a multi-regulator system is highly likely to cause confusion, unequal application of obligations and see an imbalance in the application of the provisions. Due to the overlapping/conflicting obligations, mandates, and practices between the regulators there will be siloing and a strong likelihood of 'buck passing', especially on complex matters. The involvement of multiple regulators will likely result in miscommunications and create accessibility issues for customers knowing which the correct regulator is to manage an issue. We nominate the ACCC because the scams issue is primarily a consumer issue rather than a corporations, financial services, or media and communications issue. As such, the CCA is the most appropriate location for the legislative regime to lie and for the ACCC, as the competition and consumer regulator, to be the main enforcer of this regime especially as it already regulates all three sectors. The ACCC is also best placed to take an ecosystem view.

		If the multi-regulator model is kept, which we strongly recommend against, then consideration must be given to ensuring that there are clearly delineated responsibilities on how issues will be managed. The Government could look to models such as the joint-regulator model of the Financial Accountability Regime between APRA and ASIC, which has seen the two agencies sign a Joint Administration Agreement that has been made public. It was also suggested at the Banking Industry Roundtable that it could also be modelled on the joint model to consumer regulation model between the ACCC and the state and territory regulators. COBA is unable to comment on the details of the consumer regulator model, and it is still too early to comment on the effectiveness of the FAR model as the regime has not yet commenced. However, we would highlight that in each of these cases there are strong commonalities between the varying agencies that is lacking in the proposed scams regulatory model. With FAR, APRA and ASIC are the twin peaks of financial services regulation and as such there is already significant cooperation between these agencies. Similarly, with the consumer law model there would have been strong pre-existing cooperation between the ACCC and its state/territory counterparts, and they would have shared similar mandates and approaches. However, the three regulators currently proposed for regulating scams (with the option for more to be added later) are disparate and do not necessarily have a history of strong co-operation or pursuits of similar mandates. As such, we think that it will likely be much more difficult to achieve the same level of cooperation.
4	Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors	See comments to Questions 2-3. COBA has significant concerns about there being consistent obligations and consistent application of these obligations across the sectors. We consider there to be a higher risk of uneven application and enforcement. There is also a higher likelihood of miscommunications, siloing and 'buck passing' between regulators as more regulators and sectors become part of the framework. A single regulator with responsibility for the whole framework will ensure consistency across the board.
5	Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?	This is difficult to answer without knowing the final model, what sectors will be regulated, which regulators will be involved, and the non-inclusion of key parts of the scam lifecycle, including cryptocurrency exchanges. Flexibility will be important including the ability to seamlessly

		incorporate new sectors. However, we have doubts that the complex legal and multi-regulator approach proposed will make this easily achievable.
6	What future sectors should be designated and brought under the Framework?	COBA believes that payment providers and intermediaries, crypto exchanges and online marketplaces should be included in phase 1 of the framework along with banks, telcos and digital platforms. This is consistent with the work of the NASC that takes an ecosystem approach. The following sectors should be considered for future expansions: • Superannuation funds. • Job seeker platforms. • Utility providers. • Critical infrastructure, such as health providers that can be used by scammers to gather sensitive personal or health information. • Government – the Commonwealth should make itself bound by these provisions.
7	What impacts should the Government consider in deciding a final structure of the Framework?	The Government should consider the following: • Ensure that there is consistency and commonality in how each sector is regulated. • Ensure that there is fairness in how the codes are developed and with equal ambition (e.g., telcos having an industry code while banks and digital platforms are subject to legislated codes) and also to not provide advantage to particular parts within a sector (e.g., skewing measures in favour of larger banks over smaller). • Provide flexibility so entities can comply with measures in different ways that are appropriate to their business and business model. • The costs of implementation by industry and provide sufficient time for implementation, especially if big changes are required. • Acknowledge that sectors know their customers and know what the best way is to respond in each situation. The creation of moral hazard risks if the framework removes incentives for consumers to take a common-sense approach to potential scams, for example by failing to carefully consider a investment scheme offering unrealistically high returns (i.e. that are 'too good to be true').
Definitions		
8	Is maintaining alignment between the definition of 'scam' and 'fraud' appropriate, and are there any	An unintended consequence of alignment could be the conflating of frauds and scams, which we address more in Question 10 on the definition of a 'scam'.

	unintended consequences of this approach that the Government should consider?	Fraud is already a criminal offence, however, what is being proposed in the framework could see banks treating frauds connected to scams differently to other type of frauds that are not captured within the proposed definition. We think that there needs to be more clarity on behalf of the framework on what it is trying to achieve. Is the framework trying to combat scams, or fraud, or both? Ideally, the framework should be aimed at looking at the whole ecosystem of the scam and not just at how the authorised payment is treated by the bank. The framework should be focused on preventing customers being targeted and receiving the scam in the first place.
9	Does a 'dishonest invitation, request, notification, or offer' appropriately cover the types of conduct that scammers engage in?	Yes, this is the conduct that scammers are engaged in, but note that this is closely aligned with the 'obtain a benefit by deception' that occurs in a fraud. The definition should make clear that it does not include the following issues: • Cybercrimes that may use hacking, data breaches, identity theft that do not involve the deception of a consumer into 'authorising' a transaction. • Consumer disputes about misleading and deceptive practices relating to sale of goods and services, other than where a seller profile or website is not legitimate.
10	Does the proposed definition of a scam appropriately capture the scope of harms that should be regulated under the Framework?	We support defining a scam; however, we do not think that the definition proposed is appropriate or correct. The definition proposed is confusing and conflates the terms of 'scam' and 'fraud'. A critical difference between a scam and a fraud is that scams involve customer consent whereas a fraud does not. For example, an investment scam is the consensual transfer of funds into an 'investment' by a customer. The difficulty for the bank is in trying to identify that the transfer is a scam and preventing the customer from proceeding with the transfer. A fraud committed against the customer will be unknown to the customer, for example, where a customer's card information is skimmed. Another example to highlight the difference where both a scam and a fraud occurs as separate acts is in a remote access scam. This is where the customer is scammed to divulge credentials (or two factor codes) which is then followed by the fraud where a funds transfer occurs without the customer's knowledge. The purpose of the framework is to prevent the customer providing the authorisation for the funds to be removed. However, this is difficult to deal with for banks because the banker's

		mandate requires the bank to comply with the instructions of the customer in good faith. This conflicts with the desire of the bank to stop scam payments. It is critical that when considering ecosystem actors, that banks are right at the end of the process and can have limited ability to prevent or stop the transfer given ultimately this is the customer's money. The best area for addressing this issue is to either stop the scam generation (i.e., go after the scammers) or prevent customers receiving the scam (i.e., through the telcos, digital platforms and others) before the customer seeks to authorise a transfer of funds with the bank. Another factor to consider is where customers are acting negligently or recklessly (subject to a reasonable person test) or knowingly participating in the scam, such as a money mule.
11	What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?	See our response to Question 10.
12	Will the proposed definitions for designated sectors result in any unintended consequences for businesses that could not, or should not, be required to meet the obligations set out within the Framework and sector-specific codes?	It will depend on the final detail of the framework. The framework should be set up to allow for new sectors to be added easily as the regime evolves and expands. See commentary on the banker's mandate in Question 10. The framework could compromise the duty of the bank to act on customer instructions in good faith. The framework places pressure on banks to not follow customer instructions thereby breaching the mandate and seeing customers losing control over their money.
13	Should the definitions of sectors captured by the Framework be set out in the primary law or in the industry-specific codes?	To maintain consistency across the codes, the definitions should all be in the primary law unless there is a term that is code specific and does not impact the other codes. In this case a definition may appropriately be included in the code.
14	What impacts should the Government consider in deciding the definitions of digital communications platform or ADI?	ADI is a pre-existing and well-established term that is defined in law. Its usage here is appropriate. However, we note that there are different types of ADI business models. For example, some ADIs provide payment services rather than conduct retail banking.

Principles-based obligations		
15	Are there additional overarching obligations the Government should consider for the Framework?	The proposed obligations are sufficiently extensive, however, the non-inclusion of key parts of the scam lifecycle (i.e., cryptocurrency exchanges) means that the overarching obligations will need to be revisited when they are brought into the framework.
16	Are the obligations set at the right level and are there areas that would benefit from greater specificity e.g., required timeframes for taking a specific action or length of time for scam-related record-keeping?	The overarching obligations should be more high-level and general. However, we do have comments about the obligations that are outlined in **Appendix B**. As a general position, entities will have different approaches that will need to be considered. Any timeframes that are specified must be reasonable and we address in more detail in Question 39. Record keeping for banks is already provided under other legal requirements and there is no need for this to be specified any further in this code.
17	Do the overarching obligations affect or interact with existing businesses objectives or mandates around efficient and safe provision of services to consumers?	The code would broadly align with member objectives to protect their customers and the funds of the bank. However, the changes will likely introduce more friction in payments that will affect services to customers.
18	Are there opportunities to minimise the burden of any reporting obligations on businesses, such as by ensuring the same information can be shared once with multiple entities?	Reporting obligations to third parties (e.g., the scams code regulators, AUSTRAC, the Privacy Commissioner) when there are breaches or other triggers should be satisfied by the same report that is generated by the entity and these parties should not require tailored or bespoke reports on the same incident. This is another reason for having only one regulator responsible as multiple regulators will significantly increase the risk of burdensome reporting. Prescribing a single centralised body, such as AFCX, for reporting to that then in turn notifies the other agencies could assist. Additionally, banks are already required to submit detailed scam victim data via Suspicious Matter Reports to AUSTRAC in its capacity as Australia's Financial Intelligence Unit. There should not be any duplication of this reporting in other mechanisms to other regulators, which should seek to retrieve this information directly from AUSTRAC rather than duplicate existing processes. If this data collection was duplicated it would place additional burdens on smaller banks.

19	What changes could businesses be expected to make to meet these obligations, and what would be the estimated regulatory cost associated with these changes?	It is difficult to quantify an estimate, but these changes are likely to incur significant cost and require sufficient lead times to pay for updated technology. A non-exhaustive list of the likely changes required by our members includes: • cost of technology, • risk and operational resourcing, • training, • consumer education and awareness, • investment in board and executive awareness of responsibilities, • reporting, • initial consultancy costs, • compliance, • business decisions and process definitions, and • for members that have recently undertaken mergers or are planning mergers, then there will need to be an assessment of their current versus future state in relation to the merger in addition to any third-party costs that will be passed on. COBA expects the highest costs to be related to technology changes that involve multi-channels and customer-facing developments such as confirmation of payee as well as 'kill switches'.
Anti-scams obligations		
20	What additional resources would be required for establishing and maintaining an anti-scam strategy?	The likely areas of additional resourcing for our members include: • Dedicated fraud risk resources. • Daily operational resources to perform additional processing tasks. • Operational resources for intelligence and analytics. • Technology. • Third party relationship management and procurement. • Training. We note that the market already has a shortfall of suitably trained and skilled staff. The additional resource requirements on regulated entities will likely exacerbate this issue.
21	Are there any other processes or reporting requirements the Government should consider?	The adoption of more mandatory processes and reporting diverts entities resources away from more important activities, such as focusing on reducing the impacts of scams on customers and the community. Our members have finite resources, and we would not be supportive of more processes or reporting if this is not the most cost-effective use of these limited resources,

		especially when noting the resource shortfalls for appropriately trained and skilled staff outlined in our Question 20 response.
22	Are there parts of a business's anti-scam strategy that should be made public, for example, commitments to consumers that provides consumers an understanding of their rights?	Any requirement on businesses to disclose their anti-scam strategies publicly must be approach with great caution. This is because the details in the strategy will facilitate scammer knowledge of the entity's procedures, which is especially problematic for banks. Our view is that anti-scams strategies should not be mandatorily disclosed. Regulated entities should have discretion on what they make available to customer for without doing so will run the risk of anti-scams strategies being watered down or lacking detail. It is likely that our members will create material for their customers that will outline consumer rights and provide some high-level information to provide customers with reassurance that the bank takes the matter seriously. This sort of information would not divulge sensitive information around the prevention, detection and response to scams.
23	How often should businesses be required to review their anti-scam strategies and should this be legislated?	COBA's preference would for this to not be legislated so as to provide regulated entities flexibility in how they approach these reviews. However, if it is to be legislated then an annual review should be sufficient or unless an occurrence occurs that indicates weaknesses in the strategy. Perhaps this should be more of a minimum number of reviews rather than a mandate as scams rapidly evolve and entities will likely be reviewing the strategy regularly as matters change.
24	Are there any reasons why the anti-scams strategy should not be signed off by the highest level of governance within a business? If not, what level would be appropriate?	Board or senior management should be sufficient. Flexibility should be provided to allow individual entities discretion on select the most appropriate for their business.
25	What level of review and engagement should regulators undertake to support businesses in creating a compliant anti-scam strategy?	The regulators could prepare guidance material that Is like the ASIC Regulatory Guides. These should be developed in consultation with industry and could include voluntary design templates for each sector and guidance on what information is considered acceptable to the regulators.
Information sharing requirements		
26	What resources would be required for establishing and maintaining additional information sharing arrangements with	Duplication of information sharing arrangements is not desirable. The sharing of information requires secure protocols and storage that is compliant with cybersecurity and privacy laws. AFCX is currently certified to share information securely and should be utilised. We note that

	other businesses, the NASC and sector-specific regulators under the Framework?	our members directly joining AFCX will take significant technological resources and dedicated daily operational resources in order to review data and to contribute data. COBA wants to ensure that our members can focus resources on addressing scams rather than potentially bureaucratic reporting processes.
27	What safeguards and/or limitations (regulatory, technical, logistical or administrative) should the Government consider regarding the sharing of information between businesses, the NASC or sector-specific regulators?	The AFCX is already utilised to share information and the Government should avoid obligating entities to duplicate the sharing of information with multiple entities. Regulators and NASC should receive their information from the AFCX rather than require entities to report separately.
28	What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?	AFCX and AUSTRAC.
29	Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?	There needs to be trust in the validity of the intelligence received as acting on unsubstantiated intelligence may place entities into legal predicaments or conflicts with customers. Consideration should be given to providing protection from existing laws where there has been the sharing of personal and confidential information even if the activity turns out to not be a scam. Privacy and other legal protections are very important; however, these can cause significant hurdles as seen during the Optus data breach and the inability of companies to legally share personal information even though it was in the customer's interest to do so.

Consumer reports, complaints handling and dispute resolution		
30	What are the limitations or gaps that need to be considered in leveraging existing IDR requirements and EDR schemes for the purposes of this Framework?	COBA supports the establishment of a single EDR for managing scams. This could either be in the form of a new EDR that solely manages scam complaints or by allocating one of the existing EDRs responsibility to receive and manage complaints. We would welcome working with the Government further on this issue. The multi-EDR approach implied in the Paper has similar problems as the multi-regulator approach. There will be confusion, inefficiencies, and 'buck passing' between the EDRs. It is highly likely to result in inconsistent decision-making and poor customer experience. For example, if one EDR scheme tended to rule more favourably to consumers and in the awarding of compensation over the other EDR, this would cause this EDR to be favoured by consumers over the other and see more complaints received. There will need to be a means of apportioning any awards of compensation across the sectors as appropriate and for the inclusion of when the customer is not entitled to partial or full compensation.
31	If the remit for existing EDR schemes is expanded for complaints in relation to this Framework: a. what criteria should be considered in relation to apportioning responsibility across businesses in different sectors? b. how should the different EDR schemes operate to ensure consumers are not referred back and forth? c. what impacts would this have on your business or sector?	If a multi-EDR model is adopted, which we strongly oppose, we would suggest that the following issues be considered: • Clearly managing how disputes are allocated between the schemes. • Disputes should not receive multiple hearings between EDRs, i.e. a complaint should be made once and considered once by a single EDR. • The EDR needs to consider the whole ecosystem including the roles of each of the sectors and the consumer in the dispute. • The awarding of any compensation must be done in a manner that is apportioned in accordance with the role played by all parties. • There should not be an assumption by the EDRs that the regulated sectors are automatically fully or partially responsible for the loss regardless of the actions that they took to prevent the loss. • A clear list of responsibilities and obligations for consumers to meet in order to claim. • Clear provision of how liability is to be allocated with a focus on determining where did the failure occur, i.e., was the successful scam due to the actions of the telco/digital platform, the bank, the consumer, or multiple parties?
32	Should the Government consider establishing compensation caps for EDR mechanisms across different sectors regulated by the Framework?	We would support the caps being equal across the sectors to ensure fairness in compensation and prevent instances where lower compensation caps in a particular sector leads to another sector unfairly bearing compensation costs.

	Should these be equal across all sectors and how should they be set?	
33	Does the Framework set out a clear pathway for compensation to consumers if obligations are breached by regulated businesses?	We are concerned with the absence of a consumer role in the ecosystem and the assumption that the regulated entities should bear the costs in instances of customer negligence or recklessness. The framework does not clearly provide for how liability will be shared between sectors, when there is a genuine breach on their part, and the allocation of liability to the customer (in full or in part) due to their own behaviour. A failure to provide incentives for customers to take steps protect themselves from scams will create moral hazard and runs counters to the objective to harden Australia as a scams target.
Sector-specific codes		
34	Are sector-specific obligations, in addition to the overarching obligations in the CCA, appropriate to address the rising issue of scams?	Generally, the obligations are reasonable start in addressing current scam typologies. However, due to how rapidly scam methods change and develop, the obligations it will likely need to be regularly reviewed and updated. For more detailed comments on the overarching obligations see **Appendix B** and for detailed comments on the banking sector specific obligations see **Appendix C**.
35	Are there additional obligations the Government should consider regarding the individual sector codes?	For the digital platforms, telcos and for future codes we think that it would be appropriate for there to be equivalents to the vulnerable customer sub-provision as currently provided for in the bank sector code. Stronger provisioning could be provided for digital platforms to act to not host or pay per view scam ads. It is not appropriate for platforms to allow false and misleading advertising on their platforms. Additionally, there could be requirements imposed that social media platforms should adopt a similar approach to scams as they do with actioning and removing child abuse and terrorist related material.
36	Do the obligations considered for each sector reflect appropriate consistency across the scams ecosystem?	This depends on the governance arrangements that will be set up between the regulators plus the inclusion of future sectors and regulators. We are concerned that without a single regulator model and similar instruments being applied to each sector that there will be minimal consistency in the codes and their application.
37	Are the proposed obligations for the sector-specific codes set at the right level, sufficiently robust, and flexible?	No. Much more precision and clarity are needed in the banking sector code provisions given their expected enforcement by ASIC as well as application via the chosen EDR scheme. The provisions as currently provided are too high level. Banks need specific details on the

		circumstances when intervention by a bank is triggered. While the trigger must be specific, there must be flexibility in how banks respond to recognise each bank's size, complexity, and preferred means of response. For more specific detail and our concerns on each individual obligation see our commentary in **Appendix C**.
38	Are the proposed approaches to developing sector-specific codes appropriate, and are there other approaches that could be considered to meet the objectives of the Framework?	COBA would need more information before being able to fully comment. The Paper provides limited information on how this will occur.
39	Should any of the proposed sector-specific obligations specify a timeframe for a business to take action, and if so, what timeframe would be appropriate?	The timeframe for the trace and recover provision in the banking sector obligations is inappropriate for the reasons we provide in **Appendix C**. Additional timeframes could be suitable for other obligations, as we would prefer these obligations be clear to our members rather than having to work through the uncertainty of precedent setting through EDR or the courts. We would prefer the timeframes to be included in the code and not in the primary law as it will make it easier to update as practices in the industry changes. COBA is willing to work with the Government on determining appropriate timeframes.
40	What changes could businesses be expected to make to meet the sector-specific code obligations, and what would be the estimated cost associated with these changes?	This is difficult to answer due to the lack of specific detail on what our members will be expected to do and the costs to implement these. These costs are likely to be significant and exponential, especially if technology requirements are mandated. Some costs may be known where the technology exists (e.g. FRX), some are not known but could be estimated (additional staffing costs) and some costs are unknown ('kill switch' and payee verification).
41	What are the relative costs and benefits of other available options, pathways or mechanisms, such as co-regulation, to set out additional mandatory sector-specific obligations?	No comment.

42	Are there additional areas the Government should consider in ensuring appropriate interaction between the bank-specific scams code and the ePayments Code?	This will depend on the final definition of 'scam'. If fraud continues to be intertwined with scam, then the ePayments Code has specific provisions around liability. In which case, due consideration should be given to removing all liability from ePayments Code and have this shifted into the scams code.
Oversight, enforcement, and non-compliance		
43	How would multi-regulator oversight impact different industries within the scams ecosystem? Are there any risks or additional costs for businesses associated with having multi-regulator oversight for enforcing the Framework?	COBA's preference is for a single regulator and a multi-regulator approach should be avoided unless there are strong and compelling legal and constitutional reasons to do so. See response to Question 3 for more detail.
44	Are there other factors the Government should consider to ensure a consistent enforcement approach?	COBA's preference is for a single regulator and a multi-regulator approach should be avoided unless there are strong and compelling legal and constitutional reasons to do so. See response to Question 3 for more detail. If the multi-regulator approach is pursued, then there will need to be a consistent approach agreed to and adopted by the regulators. There should also not be duplicative investigations by multiple regulators on the same issue. If an issue cuts across sectors, then a lead regulator should be appointed to lead the issue with input from the other agencies. The regulators could prepare and issue guidance to regulated entities to assist them with complying with the regime. We recommend that any guidance prepared should be issued in draft form and consulted on with industry. We also recommend that the regulators take an educative approach for the 12 months following commencement to assist regulated entities with complying with the new regime rather than taking a punitive approach.
45	Should the penalties for breaches of sector-specific codes, which sit in their respective sector legislation, be equal across all sectors?	The penalty and enforcement regime should be in the same primary law that establishes the framework and not split across the various sector specific laws and codes. As a broad principle there should be equality in the penalties imposed on each sector, however, there should be some discretion provided in the awarding of these penalties to recognise the individual circumstances of each case or potential breach by the regulated entity.

Appendix B – COBA response to proposed overarching obligations

Proposed Obligation	COBA Comment
Prevention	
A business must develop, maintain, and implement an anti-scam strategy that sets out the business' approach to scam prevention, detection, disruption and response, based on its assessment of its risk in the scams ecosystem.	COBA thinks that this is conceptually an appropriate obligation in that it makes entities collate an entity-wide view of the scams approach. The development of an anti-scams strategy is consistent with the Scams-Safe Accord entered into by all Australian banks. It would be beneficial for our members in implementing and developing these strategies that they be provided with minimum expectations of what is expected in these strategies by the Regulator. This could be in the form of some guidance that is issued by the Regulator and may not need to be prescribed in the law or in the code. We note that ASIC is currently examining smaller banks' scams approach, including for some of COBA's largest members. This is likely to feed into guidance on this requirement. Minimum expectations would also be beneficial in that it would create consistency across the regulated sectors. COBA does not support mandated public disclosure of the strategy but rather have discretion on what they make publicly available. This is because if they are compelled to release the detail on what their 'playbook' is in responding to scams it will provide this information to scammers and it will assist them in getting around the bank's protective measures. Our members are likely to prepare internal and external documents. The internal document would be the strategy itself while the external document is the high-level information that would be made available to their customers to provide them with reassurance and information on the seriousness with which the bank treats this issue.
A business must take all reasonable steps to prevent misuse of its services by scammers, so that an undue burden is not placed on consumers or other market participants to prevent scams.	We seek clarity on what this would mean practically for banks. Is this primarily meant to target the misuse of bank accounts (mule accounts) or is this meant to address something else? If this is not the case, then this provision may make more sense as a specific obligation primarily imposed on the telcos and digital platforms as this where there is more scope for the business to take actions to prevent misuse of services. Does this also include banks listing their phone numbers on the 'Do Not Originate' list? Beyond the mule account issue, which members are already combatting, and trying to be added to the DNO list it is unclear what further steps would be required from banks.

	Additionally, guidance will be required as to what would constitute "reasonable steps" and how this would tie into liability. Will the onus be on banks to demonstrate that customers did not take care?
A business must implement anti-scam systems that are responsive to new products, services, designs, technologies, and delivery channels.	We query what is meant by the term 'system'. Was this meant to be a reference to the anti-scam strategy or to technology? We would prefer this to be a more neutral term in order to capture processes and not just technology (potentiality 'capability'). Adopting or creating new technologies can be uneconomical for smaller banks due to smaller customer bases. Some banks may take a technology approach in managing this issue while others may prefer to incorporate into their processes and take a more manual approach or to utilise less complex technology. Some banks are more easily able to use manual processes to address these issues as their model may have stronger personal relationships with their customers so can take a manual response in monitoring and responding to scam activities. This approach is reflected in the Scams-Safe Accord where a technology neutral approach is adopted. We suggest that a similar technology neutral and flexible approach also be taken with the code, and that a proportional approach acknowledging the business's size be taken. We also seek clarification as to whether "new products, services, designs, technologies" refer to what is provided by the banking institution, or what is available in the market. It is one thing to say a bank must implement anti-scam systems having regard to its own new products, services, designs and technologies; it is different to say the bank must also have regard to external factors e,g, products (e.g. crypto assets) and technologies that are used in the wider market which may have an impact on the transactions and interactions which banks can be involved in (even if the bank itself does not provide those products or use those technologies).
A business must provide their consumers or users with information about how to identify and minimise the risk of being scammed.	We ask if this obligation can be satisfied with ensuring that there is appropriate and sufficient information made available to customers prominently and publicly on an entity's website and provide a hotline number that can be called? Or is this asking businesses to provide more information during onboarding or to undertake ongoing education? If it is not clear what is being imposed here, then there is likely to be divergencies between and within the different sectors.

	Expectations under this obligation should be reasonable and scalable as there are differing resources and capacity between, for example, the large banks and telcos, and smaller banks. We also suggest that an industry model or approach could be helpful, potentially via the National Anti-Scam Centre as it would provide for standardised content that is usable across a sector that can be tailored to each business/brand.
A business must train staff to identify and respond to scams.	Additional detail is sought on what this is intending to cover: • Is this meant to be for all staff at a business or only those staff dedicated to combatting scams? • How regularly does this training need to occur? As a one-off course seems insufficient. • To what level or standard do these courses need to be completed to? • Will evidence of the completion of training through online compliance modules be sufficient? COBA is seeking clarity on what the intention is behind this proposal and does not propose that the answer to these questions be prescribed in legislation but rather could be addressed through guidance or expectations of minimums provided by the regulators. We think it is desirable for there to be flexibility in how businesses respond to this obligation in line with other regulatory regimes.
Detection and disruption	
A business must seek to detect, block and prevent scams from initiating contact with consumers.	It is unclear how this would be applied to banks as the focus is on 'initiating contact'. This obligation appears to be more tailored towards the telcos and digital platforms and we would suggest its inclusion in their respective codes. It could be beneficial for guidance to be provided to assist industry understand what the minimum expectations would be. We also assume that this refers to 'scammers' rather than 'scams'. This obligation also requires guidance about what expectations are for different types of entities.
A business must seek to verify and trace scams where scam intelligence has been received.	Scam monitoring can detect thousands of potential scam attempts each with varying degrees of risk attached. More clarity is needed on what expectations would be applied to banks here. Are these meant to be primarily focused on

A business must act in a timely manner on scam intelligence received through information sharing, consumer reports, complaints and other means.	ensuring banks are cooperating with third parties and acting where appropriate? Or is it something else?
Where a business receives intelligence that a consumer is or may be a target of a scam, the business must take steps to disclose this to the consumer in a timely manner to minimise the risk of consumer harm or loss.	More clarity is needed on what is being expected of banks here. Are they being obliged to advise customers of each instance they appear at or is only when a bank receives direct information or intelligence that this specific customer is at risk? If it is the former, and noting the sheer volume of scam attempts, this is likely to see a saturation of notifications to customers of potential risks regardless of the degree of risk to the individual customer. This will likely annoy customers who will ignore the continual notices being received. It would make it difficult for the customer to know when and how to act when there is a genuine threat as they would likely 'tune out' the warnings due to the sheer amount of 'noise' that they experience daily.
A business must provide their consumers or users with tools to verify information in real time.	It is unclear how this would be applied to banks. What does 'information' intend to cover? Is it confirmation of payee? Is it verifying bank employees on outbound calls? In a banking situation Is this meant to be covering the confirmation of payee changes or the ability for customers to access information on their accounts? Otherwise, this obligation appears to be more tailored towards the telcos and digital platforms and we would suggest its inclusion in their respective codes.
Response (obligations with respect to consumers)	
Where a consumer has identified they have been affected by a scam, businesses must take all reasonable steps to prevent further loss to the consumer and treat consumers fairly and consistently.	COBA believes that a 'reasonable steps' test is appropriate as it is a common threshold in regulatory schemes, however, we would seek clarification on the difference between 'reasonable steps' and 'all reasonable steps'. We also seek clarity on what is meant by 'fairly and consistently' in a practical sense. The challenge is that each scam case is different which means that while banks will take all reasonable steps in each situation and will seek to treat customers fairly, it may be difficult to always be consistent. Guidance on what would constitute "all reasonable steps" would be required. We also note that either in this provision or elsewhere, there needs to be clear recognition that there is a discretion on the banks in the awarding of reimbursements to the customer that is dependent on the individual

	circumstances. We also note the interaction that this may have with the ePayments Code in determining liability of the consumer and the bank for the ePayments Code covers fraud and this code will cover scams. The differences between the two need to be noted but also seamless so that customers do not fall between the cracks.
A business must have user-friendly, effective, efficient, transparent, and accessible options for consumers or users to report a scam, including people not directly targeted by a scam.	We suggest that this not be a requirement for a technology solution noting the challenges and expense that can exist for smaller banks to adopt these. We suggest that this be technology neutral and be sufficiently broad to allow regulated entities flexibility in how they apply this. For example, we suggest that making available information prominently and publicly on an entity's website that directs customers to a dedicated hotline or call centre should be sufficient to address this issue. The terms "effective, efficient, transparent" are vague. It would be helpful to understand what would be considered "effective, efficient, transparent". Also, if only one of these are not met (e.g. something is user-friendly but not necessarily "transparent" or "effective") – would that breach the code requirement? Or do all five components need to be not met, in order for an institution to have breached this obligation? Do these components all have equal weighting (or some more important than other in determining whether the obligation was breached?
A business must have user-friendly, effective, transparent, and accessible complaints handling processes for consumers or users to make a complaint about how a scam report was handled or in relation to a business's response to scam activity (including steps taken to prevent, detect, disrupt and respond to scam activity).	These are standard per existing internal dispute resolution and external dispute resolution requirements for banks. There could be some overlap with pre-existing obligations, however, we note that these obligations may be necessary for the other sectors that may not be as mature as banks on IDR and EDR matters.
Where a consumer escalates concerns with a business, they should be dealt with fairly and promptly, and consumers should be given access to information about dispute resolution options where applicable.	
Reporting (obligations to regulators and other businesses	
A business must take reasonable steps to notify other businesses, the NASC and relevant regulators promptly of intelligence about	We ask for clarification on the purposes of these provisions. What is to be the interaction between the code, NASC and AFCX? There is a risk that smaller

suspected or identified organised large-scale scam activity as well as rapidly emerging or cross-sectoral scam activity.	banks could be using AFCX to share data and not have appropriate insights to know when to engage law enforcement, regulators or the NASC per these provisions. We assume that there reference to 'other businesses' relates to other regulated businesses in the ecosystem rather than just all 'other businesses'. We note that whichever reporting body is mandated for information to be disclosed to that it be done so there is a clear legal mandate to do so in order to cover the business's privacy obligations.
A business must share data and information on the incidence of scams, and action taken in response, with designated industry bodies, law enforcement and regulators, and the NASC.	
A business must keep records of incidences of scams, and the action taken in response.	
A business must respond to an information request from the ACCC within the timeframe specified.	We question if this is necessary as assumedly it will either be covered by pre-existing laws, or an obligation will be inserted into the primary law.

Appendix C – COBA response to bank specific obligations

Proposed obligation	COBA Comment
Prevention	
A bank must implement processes to enable confirmation of the identity of a payee to reduce payments to scam accounts.	We suggest amending this provision to align with the intent of confirmation of payee. The Scams-Safe Accord jointly announced by COBA and the ABA commits the banking industry to develop a confirmation of payee system. This provision is reliant on an industry solution that is still being built and as such industry cannot be compliant with this provision until it is delivered. For clarity this system will only verify whether the name of the recipient account matches the name that the customer has entered (i.e. they are paying the name who they think they are paying). There is no confirmation of the identity of the payee in this process. We note that the payee's name can be the scammer's name or be subject to an ID takeover or is the name of the mule account. In each of these circumstances the confirmation of payee system could confirm a match in the name but does not have any further ability to confirm the identity of the payee.
A bank must implement processes to verify a transaction is legitimate where a consumer undertakes activity that is identified as having a higher risk than their normal activity and is or is likely to be a scam. a) A bank must have processes in place to identify consumers at a higher risk of being targeted by scammers (vulnerable cohorts). Additional steps must be taken if the consumer is identified as having a higher propensity to be affected by a scam.	We suggest clarifying what it means to be 'legitimate' in this context. COBA is concerned that this provision could impose a liability on a bank if a scam is not prevented. For example, where a transaction is not identified as illegitimate. We consider this provision's use of 'legitimate transaction' as being unclear. This term brings a subjective element where the bank has to determine that the payment is legitimate or illegitimate. A scam usually involves an authorised transaction by the customer that is used to perpetrate a fraud. Using the term 'legitimate' will make the provision significantly open to interpretation and require more due diligence on payments. Legitimate could be considered following the customer's orders, even if it is to an illegitimate recipient. This obligation could create liability shift as larger banks introduce more robust fraud detection methods that are beyond the ability for smaller banks to adopt. However, it is likely that the EDR body would require smaller banks to take similar measures. For more on the definition of 'scam' see our response to Question 10 in **Appendix A**. We note that this also refers to having process rather than the specific outcome. These processes are likely to be probabilistic and will not be able to prevent all scams and this needs to be reflected in any interpretation if a scam is not prevented.

	Vulnerable consumers COBA supports measures to protect customers with vulnerability. Our Customer Owned Banking Code of Practice notes "We will adapt our customer service standards where reasonably practicable, and take extra care where we are aware that you are experiencing vulnerable circumstances". Banks can put in place processes to identify these cohorts but we consider what are "additional steps" that banks should they then take and how far can they take it? We note scams can involve very complex levels of social engineering and consumers can be adamant about making these payments. Would banks be able to block payments by these cohorts or debank them due to the risk they pose? These raise questions on banks proactively identifying cohorts of customers who may fall into protected categories under anti-discrimination laws (for example, age) and then treating these cohorts differently compared to other groups. These actions could fall foul of anti-discrimination laws and see banks subject to complaints and actions for breaching these laws. COBA also suggest that the vulnerable consumer provisions should be replicated in other sector specific codes. Finally, we note that some customer owned banks serve communities with a much higher proportion of vulnerable customers relative to larger banks, for example, Traditional Credit Union provides key banking services to remote Aboriginal communities in the Northern Territory. Any obligations should recognise that these banks provide valuable services to communities that may not otherwise have access to banking services, and actions that disproportionately impact these banks may impact their ability to provide services.
A bank must implement and have in place processes and methods to detect higher risk transactions and take appropriate action to warn the consumer, block or suspend the transaction, or as well as *take other measures to reduce scam activity and limit exit channels for the proceeds of scams, including blocking or disabling the scammer account (if in the same bank) or working with the recipient bank to do so.*	We suggest splitting this provision into two separate provisions. The first half (detect, take action and verify process) could be included in the previous provision, and the second half (reducing activity and limit channels when the scammer banks with you and you are aware) could be its own separate provision (*italics*). For the first half, it is not clear what is classified as a 'higher risk transaction' given this is subjective and varies according to different banks. We consider whether this should be defined by individual banks (i.e. having a higher risk transaction policy in place) or as a defined term. It is also not clear what actions would be appropriate once identified.

	If a bank blocks a payment it considers to be 'higher risk' how does this comply with the banker's mandate? What happens if the payment ends up being legitimate and the delay/blocking caused the customer to lose money? Would the bank be considered liable for this action and the loss by the customer?
A bank must have in place methods or processes to identify and share information with other banks that an account or transaction is likely to be or is a scam.	COBA assumes that our member involvement in AFCX in accordance with the Scam-Safe Accord will be sufficient to meet this obligation. If this provision is intended to have a wider application, then we ask for additional information on what is intended to be achieved under this obligation.
A bank must have in place processes to act quickly on information that identifies an account or transaction is likely to be or is a scam, including blocking or disabling the scammer account or the transaction (if in the same bank) or working with the recipient bank to do so.	We seek clarification on what would constitute a bank 'act[ing] quickly'. While this may have been left vague to provide flexibility to banks its likely affect will be that the timeframe will be set by practice via the external dispute resolution scheme. If timeframes are intimated in the code and not explicitly provided for then it will fall to the EDR process to determine, which may not be appropriate. An additional consideration with timeframes is determining when does the clock start? When the bank identifies the account or transaction that is likely to be scammed? Or when the information that would identify the account or transaction is provided to the bank? Or something else? A practicality question is that once AFCX is integrated with our members there is an unknown of the volumes of information being received. If these volumes are significant there could be challenges for smaller banks in digesting and analysing the data and acting on it in a manner that could be considered quickly compared to banks that have more sophisticated and automated technological systems.
A bank must have user-friendly and accessible methods for consumers to immediately take action where they suspect their accounts are compromised or they have been scammed (e.g. an in-app 'freeze switch').	COBA does not support the inclusion of the 'freeze switch' in the provision. We believe a wider provision without the example could provide banks with more flexibility in how they seek to implement it and meets a clearer customer need while balancing the costs and benefits. The specific freeze switch example is likely to be uneconomical given the need for technology builds across multiple banking channels, particularly given significant resources are currently being diverted for confirmation of payee. However, with the explicit calling out of the freeze switch it makes this provision confused, because is the provision about mandating the freeze switch or is it about banks developing methods for consumers to take action in response to a scam? If it is the latter then we suggest removing the reference, if it is the former and the Government is seeking to mandate a freeze switch then we would suggest it be

	provided its own explicit mandating provision similar to the confirmation of payee provision (noting COBA does not support the switch). The provision could also be clearer on what the result of the consumer 'tak[ing] action'? For example, is it to notify the bank of the suspected scam activity or is it intended to stop any transactions, which may not be possible? Clarifying this will be essential because it will allow banks to properly assess what steps they need to take to enable customers to 'take action'. If the reference to the freeze switch is removed, then for many of our members this provision would likely be acted on making possible improvements to their websites and call centres, and developing internal processes to manage this. ***Freeze switch*** The freeze switch concept on its face appears to provide the customer with more control and ability to prevent scams, however, it is misaligned with what happens when a scam is detected. Generally, customers only become aware of a scam when: • The bank identifies the risk and notifies them. • The customer notices funds have been removed from their account. • The customer is proactively participating in the scam (knowingly, or unknowingly). In all three circumstances the freeze switch does not help the customer because the funds have already left their account and the freezing comes too late. Additionally, if a scammer has gained control over the customer's account the first action is usually to change the password and deny the customer access to the account thereby rendering the customer unable to activate the switch via the bank's app or website. We question what value will actually be gained by customers from this switch and do not believe that whatever minimal value is gained it will exceed the costs to banks in developing and incorporating this switch into their systems. This is especially so for our smaller members that lack the resourcing and are reliant on third party providers for their banking and technology systems. Having examined the Singapore model we believe that there are technical and practicality issues with adopting the freeze switch this includes:

	• Providing a mechanism to activate the switch on apps and websites – this would likely be an expensive technological change as it would need to tie into the banking systems in order to freeze the account. • The freezing would also need an option to be able to be done over the phone or in branch where the customer has lost the ability to access the account via the app or website – this raises questions on what would be sufficient identifying measures (especially on the phone) for the bank to verify it is an authentic freezing and not misconduct by another person. • The freezing will also prevent other authorised payments, such as payments for housing, utilities and groceries etc from leaving the account which could cause further issues for customers especially if it makes them default on payments that have consequences, for example, where failure to pay a utility bill sees the severing of the service. • There is potential for the freeze switch to be misused in domestic violence situations where there are joint accounts as the perpetrator could use the freeze switch as another means of controlling and inflicting violence on the victim. This could make it harder for victims to leave the relationship. In situations where the victim has left the perpetrator it could also be used as a means of finding the victim if they are required to visit a branch to reactivate the account. • There is a strong risk of negative impact on vulnerable cohorts where they could be manipulated into blocking their own accounts or who may accidentally block their own accounts.
A bank must assist a consumer to trace and recover transferred funds to the extent that funds are recoverable, including a receiving bank to revert a transfer within 24 hours of receiving a recall request from a sending bank.	COBA suggests that this provision be split into two. The first part of the provision is about assisting customers with tracing and recovering funds while the second part, we assume, is about receiving banks having obligations to respond. On the first part, there is a practicality question, in what would be the expectation on banks. As it is the bank that is tracing and attempting to recover the funds not the customer. Is the bank being expected to provide detailed information on the process of the trace and recovery? How far is this expected to occur if they are overseas banks? On the second part, we have the following issues: • 24 hours is an insufficient time to revert funds — we consider that reverting funds in this time can problematic as it may not be sufficient time to conduct an investigation. We suggest this refers to acknowledgement in line with the relevant provision from FRX where 24 hours is the requirement for a receiving

	bank to acknowledge the request from the sending bank. This would potentially stop the funds moving on. • Will this apply to all trace and recall requests or is it only for scam related requests? • How would this be managed if the receiving bank is an overseas bank? • With recovered funds, how is this to be divided? • There is a potential clash between this provision and the ePayments Code and the Bulk Electronic Clearing System rules. • The need for similar obligations imposed on other payment chain participants (e.g., money remitters, payment service providers) who are not within the code framework.
A business must respond to an information request from ASIC within the timeframe specified.	COBA is uncertain why this provision has been included and suggest it could be duplicative of pre-existing provisions given this is a normal expectation of banks as ASIC-regulated institutions. This may be more appropriate to be an obligation inserted into the primary law if there is a gap in the regulators power to do this. We also would be interested in the threshold level for an information request as these can be quite costly on industry, particularly smaller banks. COBA notes that unlike the other provisions in the bank specific code it uses the word 'business' instead of 'bank'. If there is a reason for this then we seek clarity on why, but if this is an error please update to refer to 'bank'.