Commonwealth Bank

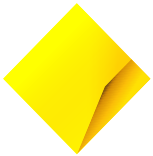
Scams – Mandatory Industry Codes

Response to Treasury's Consultation Paper

31 January 2024

Public

Contents



1. Executive summary

The Commonwealth Bank of Australia (CBA) welcomes the opportunity to respond to Treasury's Consultation Paper, *Scams – Mandatory Industry Codes*, released in November 2023.

Scams pose a significant threat to consumers and the community. In November 2023, the National Anti-Scam Centre (NASC) reported $398 million was lost to scammers between January - September 2023, with investment, dating and romance, false billing, and jobs and employment scams contributing significantly to the losses.[1] These figures are likely to be considerably underestimated given they rely largely on consumers self-reporting. The ACCC's *Targeting Scams* 2022 report notes that at least $3.1 billion was lost to scams in 2022, based on reports to Scamwatch, ReportCyber, the Australian Financial Crimes Exchange, IDCARE, ASIC and other government agencies.[2]

Scammers are becoming increasingly sophisticated and pervasive in their attempts to deceive consumers and can have a significant impact on a consumer's wellbeing, both financially and emotionally. The harm caused by scams is being felt across the world, with the Global State of Scams 2023 Report indicating that around 25.5 per cent of the world's citizens lost money to scams or identity theft in 2023, totalling an estimated $1.026 trillion in losses.[3]

CBA supports the intent of the Scams Code Framework (the Framework), which seeks to set clear roles and responsibilities for government, regulators, and businesses in addressing scams. This is proposed through overarching principles-based obligations under the *Competition and Consumer Act 2010* and supplemented by mandatory sector-specific codes.

CBA continues to invest in and develop new initiatives to protect our customers. In FY23, we invested $750 million in protecting customers from scams, fraud, and financial crime. In addition to significantly increasing our operational capacity to protect and support scam victims, we have implemented initiatives to better protect customers including:

- in-app CallerCheck technology, providing over 300,000 customers every month the confidence the call they are receiving from CBA is legitimate; and
- introducing holds, declines and limits on payments to cryptocurrency; and
- implementing industry-leading NameCheck technology, which has provided information to customers for more than 16 million payment transactions.

We have also contributed to the development of the Australian Banking Association's (ABA) Scam-Safe Accord, which will strengthen industry practice on scams prevention, detection and response.

However, as scams originate outside the banking environment, effectively reducing scams will require a collective effort to disrupt scams as close as possible to their source by preventing scammers targeting, reaching, and deceiving consumers.

CBA welcomes the whole-of-ecosystem approach that underpins the Framework. Scammers typically deceive consumers by using a combination of services from digital platforms (social media, dating apps,

[1] NASC, *National Anti-Scam Centre in Action - Quarterly update (July to September 2023),* (November 2023), available at: <https://www.accc.gov.au/system/files/National%20Anti-Scam%20Centre%20Quarterly%20Report_November%202023_0.pdf>
[2] ACCC, *Targeting scams – Report of the ACCC on scams activity 2022,* (April 2023), available at: <https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf>
[3] Global Anti-Scam Alliance, *The Global State of Scams – 2023,* (2023), available at: <https://www.gasa.org/product-page/global-state-of-scams-report-2023>

websites, emails, advertisement platforms, marketplaces) and telecommunications (phone, messages), to receiving funds from consumers, transferred via financial institutions, payment services providers, and cryptocurrency services. Detecting, disrupting, and deterring scammers therefore requires a coordinated response from businesses across a range of sectors as well as government, regulators, law enforcement, and the community.

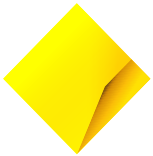
CBA also welcomes the intention for the Framework to be flexible, which will be required to ensure business, government and law enforcement can adapt as scammers respond to the combined effort of the Framework. Flexibility will also be important in ensuring businesses are able to tailor their efforts based on the size and nature of their operations. We recognise the intent to leverage existing regimes to deliver the Framework; however, we note that this should not be at the expense of introducing streamlined approaches that benefit all participants in the ecosystem, particularly consumers.

To combat scams to the greatest effect through the Framework, CBA supports:

- expanding the scope of initial sectors and entities to include cryptocurrency, payment service providers, and a broader range of digital platforms, like transaction-based digital platforms, including online marketplaces. This will help to ensure there are no gaps in the ecosystem approach and therefore provide greater protection of consumers;
- requiring the sharing of scams intelligence across sectors and entities to enable the timely response to verified scams. This would be implemented through the cross-sectoral use of existing and trusted infrastructure, like the Australian Financial Crime Exchange (AFCX), to support the NASC;
- ensuring complaints handling processes provide clarity, efficiency, consistency, and accountability across the ecosystem, which would be best achieved through a single scams external dispute resolution (EDR) mechanism providing consumers with a clear pathway to escalate and resolve issues; and
- establishing a clear regulatory boundary, where all scam types are considered under the Framework, and establishing a clear delineation between the proposed banking-specific scams code and the ePayments Code. This will be important in providing clarity not only for entities, regulators, and the EDR process, but also in terms of the protections provided to consumers.

The development and implementation of the Framework will require a whole-of-government approach, including by ensuring that other government reforms underway, such as digital assets, payment service providers, and digital identity, support the objectives of the Framework. Digital identity should improve how consumers are verified across the economy, reducing sharing of personal information and thereby reducing opportunities for customers to be scammed.

We recognise the effort to combat scams is ongoing and will need to evolve as scammers adapt their methods. We support the role of the Framework in ensuring this is a collective and sustained effort across the ecosystem. This submission outlines CBA's position on the Framework and matters raised in the Consultation Paper and we welcome the opportunity to discuss these further.



2. Proposed Scams Code Framework

Consultation questions:
1. Does the Framework appropriately address the harm of scams, considering the initial designated sectors and the proposed obligations outlined later in this paper?
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?
3. Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?
4. Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors?
5. Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?
6. What future sectors should be designated and brought under the Framework?
7. What impacts should the Government consider in deciding a final structure of the Framework?

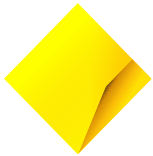
CBA supports strong collaboration across government, industry, regulators, and law enforcement to combat scams nationally and welcomes the overarching intent of the Framework. Any reduction in scams and their impact on Australians can only be achieved through an ecosystem approach.

The Framework reflects that strengthening systemic resilience requires addressing the lifecycle of a scam, which can occur across multiple platforms and channels, and often over an extended period. This requires steps to be taken to identify, prevent and disrupt scams, and actions to mitigate the impact of a scam on a customer. We also welcome the recognition of the need for flexibility and responsiveness to adapt to the evolving nature of scams and scammers.

The following principles guide our feedback on the Framework:

- Clarity – providing customers with the clear guidance and pathways to access support; and for both entities and regulators, establishing a clearly defined regulatory perimeter (for example, between the banking-specific scams code and the ePayments Code).
- Efficiency – minimising complexity, including in intelligence sharing across the ecosystem to enable and mandate the timely response by entities to prevent and respond to scams, and in complaints handling so that cases are resolved for customers in a timely manner.
- Consistency – the obligations are applied in a consistent or congruent manner across the ecosystem for all participants; and the approach to complaints handling, determinations, and monitoring and enforcement by regulators ensures customers' complaints are resolved in a consistent manner.
- Accountability – all parties in the ecosystem are obliged to take reasonable measures and, in the case of customers, act with care. All parties are accountable if they fail to meet their obligations.

We recognise the Government's desire to leverage existing regimes, systems, and initiatives. This approach should be complemented with the flexibility to add new capability if it is going to further support the above principles. The introduction of the NASC is a good example of a new initiative that complements the existing capability within the ACCC. The potential for the adoption of new capability, particularly in relation to information sharing and complaints handling is explored later in the submission.



Designated sectors

CBA supports the inclusion of banking, telecommunications providers, and digital communications platforms within the initial scope of the Framework. This will help to combat scams based on their lifecycle – from initial contact through to authorising transactions – particularly given scam calls and social media were the contact methods resulting in the highest reported losses in 2022.[4] Further, we strongly believe the initial scope should capture a broader range of participants in a scam lifecycle, providing greater protection of consumers.

Treasury's Consultation Paper outlines that initial sectors to be covered by the Framework should be those most targeted by scammers. CBA believes the proposed initial scope is too narrow to appropriately address the wide-ranging harm of scams, providing the opportunity for scammers to concentrate their focus on those sectors and entities initially excluded like digital currency exchanges (e.g. cryptocurrency), other payment service providers (e.g. stored-value facilities, payment facilitation services, payment technology and enablement services), and transaction-based digital platforms (e.g. online marketplaces and booking sites).

Including both payment service providers and digital currency exchanges is critical to preventing and taking timely steps to recover payments made to scammers such as through bank transfers. In the context of a real-time payments environment, where fast payments are immutable and irreversible, it is even more important that high-risk transactions are identified in advance and prevented. Under modern payment arrangements, where multiple parties are involved in a transaction, this cannot be achieved by banks alone.

Adding these sectors to the initial roll out will not only create an incentive for entities that operate in these sectors to meet their responsibility to detect, disrupt and deter scammers but also will increase the likelihood of a customer that has been scammed receiving compensation if the ecosystem does not meet its obligations.

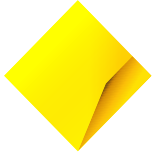
CBA recognises and welcomes the Government's reforms to payments licensing as well as digital and cryptocurrency assets that are underway. The development of sector-specific scam codes alongside these reforms will ensure comprehensive coverage of risks and consumer protections.

Payment service providers and stored value facilities

As noted in the 2021 Review of the Australian Payments System (Farrell Review), new providers and business models have transformed Australia's payments system, consisting of predominantly financial institutions, into a complex payments ecosystem involving a diverse range of payments service providers.[5] Many of these payment service providers now either perform some of the payment functions traditionally offered by a bank or play a role in processing a payment. As noted by the UK Government: "Consumers and businesses are increasingly using Payment Institutions and Electronic Money Institutions as their transactional banking provider to, among other things, access their salaries and savings as well as make payments."[6]

In response to these changes, governments here and overseas are extending bank specific payment obligations to these new players. The Government's payment system reforms recognises that payments

[4] ACCC, *Targeting scams – Report of the ACCC on scams activity 2022,* (April 2023), available at: <https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf>
[5] Farrell, S., *Payments system review – from system to ecosystem,* (June 2021), available at: <https://treasury.gov.au/sites/default/files/2021-08/p2021-198587.pdf>
[6] HM Treasury, *Insolvency changes for payment and electronic money institutions: consultation,* (December 2020), available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940738/201202_Lapwing_consultation_document_with_annexes.pdf>



are highly interconnected and regulatory supervision of all participants that play a role in facilitating or enabling payments is needed to enable intervention if risks arise at any stage of the value chain.

Increasingly, the functions performed by new participants within the payments flow limit banks' ability to identify and mitigate risks. Often banks no longer have visibility of the end-to-end transaction and may be constrained by contractual or service level agreements (SLAs).

For example, PayTo allows customers to set up "payment agreements" with businesses or merchants that enables third parties to request a payment initiation message to be sent to the customer's bank to process payments from the customer's account, according to the terms the customer agreed to. The customer's bank has limited opportunity to identify high-risk transactions as merchant onboarding and customer agreements are handled by the PayTo payment service provider. Under some PayTo arrangements, the end beneficiary of the NPP payment leg may be an overseas money transfer service or a cryptocurrency exchange and a subsequent transaction may off-ramp the funds, making funds impossible to retrieve. The customer's bank has limited ability to hold or decline a payment due to the NPP PayTo service level agreement, which is a prerequisite to participation in the scheme. All major banks are live with PayTo and the RBA has encouraged making the service more widely available to business customers (payee) looking to use PayTo as an alternative to direct debits.[7]

Similarly, digital wallets represent a growing means for Australian consumers to make payment transactions. This includes both payment technology and enablement services and stored-valued facilities. Digital wallet payment platforms enable these payments through being linked to a consumer's bank account, and different wallets have different customer experience requirements that banks need to comply with that may limit banks' ability to apply warnings or introduce friction. The RBA reported, in September 2023, that 35 per cent of in-person card transactions were made by mobile wallets in the June quarter 2023, up from 10 per cent in early 2020.[8] Further, the ACCC's *Interim Report 7* of its Digital Platform Services Inquiry (DPSI), released in September 2023, explores the expanding ecosystems of digital platform service providers and notes that the value of Australian mobile wallet transactions in 2022 was $93 billion.[9]

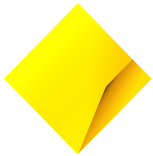
Excluding payment service providers, other than banks, from being obliged to take steps to reduce scams and protect consumers, will allow scammers to adapt, creating a weak link in the ecosystem at the outset and ultimately impacting consumers. Including all bank-like activities from the outset will incentivise providers to invest in prevention, detection and response.

As some payment providers now perform some or part of the payment functions traditionally offered by banks, there is an opportunity to capture banks and payment service providers within one code, where overarching obligations could be established and sub-sections of the code be included for banks and payment service providers, which would provide tailored obligations to reflect the differences in business models.

In many cases the obligations of banks and payment service providers in relation to scams will be similar. For example, implementing processes to verify a transaction is legitimate where a customer undertakes activity that is identified as having a higher risk; implementing and having in place processes to detect

---

[7] Bullock, M., *Modernising Australia's Payment System,* (December 2023), available at: <https://www.rba.gov.au/speeches/2023/sp-gov-2023-12-12.html>
[8] RBA, *Payments System Board Annual Report – 2023,* (2023), available at: <https://www.rba.gov.au/publications/annual-reports/psb/2023/pdf/psb-annual-report-2023.pdf >
[9] ACCC, *Digital platform services inquiry, Interim report 7: Report on expanding ecosystems of digital platform service providers,* (September 2023), available at: <https://www.accc.gov.au/system/files/DPB%20-%20DPSI%20-%20September%202023%20Report%20-%20Interim%20Report%207%20-%20Final%2815835612.1%29.pdf>



higher risk transactions and take appropriate action to warn the customer, block or suspend the transaction; and having in place methods or processes to identify and share information with other entities and to act quickly on information that identifies that an account or transaction is likely to be or is a scam. These examples are proposed as bank-specific code obligations in the Consultation Paper.

CBA also sees the activities of SVFs to be similar to banks in relation to the storing of money. If SVFs are not captured at the same time as banks under the Framework, it is likely that scammers put more reliance on SVFs to support scams and reduce their reliance on banks. The system will only be as strong as its weakest link. Given the approach the Government is considering regarding the regulation of SVFs more broadly, CBA believes there would be synergies in the way that the Framework could apply to both banks and SVFs and so there should not be any delay in incorporating SVFs into the initial code.

We suggest ASIC continue to be the regulator for a code covering banks and payment services providers, with Treasury leading its development. Ensuring there is no overlap between the ePayments Code would also need to be considered in the development of the code, which we elaborate on later in the submission.

Cryptocurrency

AFCX analysis of data reported by its members in June 2023 revealed that 47 per cent of scam funds were directed to accounts associated with cryptocurrency exchanges.[10] The ACCC's *Targeting Scams* report for 2022 also details that 3,910 people reported cryptocurrency as the payment methods for scams, an increase of 162.4 per cent on the prior year, and with $221.3 million lost.[11]

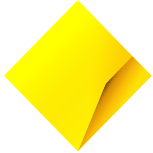
These figures demonstrate the significant role that cryptocurrency plays in the operations of scammers and that it is critical that digital assets are captured within the Framework from the beginning. Cryptocurrency is a destination channel for scammers and their exclusion from the Framework will only entrench this. Currently, where a customer has transferred funds unknowingly to scammer via a cryptocurrency exchange, there are limited procedures in place that require the exchange to recover the funds.

While CBA and some other banks have taken steps to add more friction into high-risk transactions like cryptocurrency, this is not a long-term solution. If cryptocurrency exchanges had consistent obligations under the Framework like the rest of the ecosystem, it would have a significant impact on reducing scams. Excluding such sectors from the Framework creates weaknesses within the ecosystem that will be exploited by scammers and undermine the impact of entities that meet their obligations. Consistent with the approach taken in the regulation of cryptocurrency exchanges by the Government, these exchanges could be subject to their own sector-specific code developed by Treasury and overseen by ASIC.

Digital platforms

The ACCC, through its DPSI, has highlighted the role that platforms should be playing to combat scams and made recommendations on how digital platforms should be regulated, including mandatory processes to prevent and remove scams, mandatory internal dispute resolution standards and access to an independent external dispute resolution scheme. We note the Government's in-principle support for these

[10] AFCX, *Half of all scam funds flow to cryptocurrency,* (August 2023), available at: <https://www.afcx.com.au/2023/08/14/half-of-all-scam-funds-flow-to-cryptocurrency/>
[11] ACCC, *Targeting scams – Report of the ACCC on scams activity 2022,* (April 2023), available at: <https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf>



recommendations and encourage the consideration of these recommendations in the development of the Framework.[12]
We welcome the inclusion of search engines (content aggregation services), social media, online dating, online private messaging (connective media services), and online video sharing platforms (media sharing services) within the Framework.

We note the Consultation Paper states that the digital communications platforms definition is not intended to cover transaction-based digital platforms like online marketplaces. We consider that online classified ad platforms including online marketplaces as well as email platforms would be captured by the 'connective media services' definition proposed in the Consultation Paper.

We suggest the scope of the Framework should include both these types of platforms, given their role in enabling scammers to initiate contact with consumers. The inclusion of transaction-based digital platforms like online marketplaces is also important due to the continuing increase in buying and selling scams, especially high-value purchases like caravans.

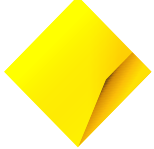
Telecommunications providers

CBA supports the inclusion of telecommunications providers, specifically carriers and carriage service providers, within the Framework. We see the inclusion of ISPs, as carriage service providers, as important given their role in the timely takedown of websites and website content that is scam related. This is particularly important in relation to investment scams, which represented 61 per cent ($241 million) of scam losses in January to September 2023.[13]

It is important that mass SMS and email service providers are captured within the Framework. These providers enable businesses to send messages in bulk to many individuals, and they should ensure their services are used by legitimate businesses and, for mass SMS providers, participate in the Government's SMS Sender ID Registry. We also consider that other facilitation services such as remote access providers and website hosts should be included in the Framework.

Ultimately, it will be important for the Government to consider the Framework beyond its initial sectors and ensure, that as the ecosystem expands, the structure, legislative framework and regulatory approach is clear and consistent.

[12] The Treasury, *Government Response to ACCC Digital Platform Services Inquiry,* (December 2023), available at: <https://treasury.gov.au/sites/default/files/2023-12/p2023-474029.pdf>
[13] NASC, *National Anti-Scam Centre in Action - Quarterly update (July to September 2023),* (November 2023), available at: <https://www.accc.gov.au/system/files/National%20Anti-Scam%20Centre%20Quarterly%20Report_November%202023_0.pdf>



2.1. Definitions

Consultation questions:
8. Is maintaining alignment between the definition of 'scam' and 'fraud' appropriate, and are there any unintended consequences of this approach that the Government should consider?
9. Does a 'dishonest invitation, request, notification, or offer' appropriately cover the types of conduct that scammers engage in?
10. Does the proposed definition of a scam appropriately capture the scope of harms that should be regulated under the Framework?
11. What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?
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?
13. Should the definitions of sectors captured by the Framework be set out in the primary law or in the industry-specific codes?
14. What impacts should the Government consider in deciding the definitions of digital communications platform or ADI?

2.1.1. Scams definition

CBA supports the inclusion of a scam definition in primary law. A clear definition of a scam is crucial to establish an effective Framework, particularly in clarifying the protections offered to consumers, the responsibilities of entities, and the overall regulatory perimeter of the Framework.

Common scam types impacting Australian consumers involve scammers creating a fake persona or profile to deceptively lure a person into:

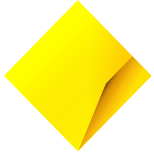
- sending money (e.g. a romance or investment scam). These payments are typically authorised by the victim;
- providing information to a scammer which enables them to make transactions on the victim's accounts (e.g. a phishing scam which prompts victims to enter credit card or online banking credentials into a fake website). These payments made by scammers are typically not authorised by the victim; or
- providing access to devices or apps to a scammer which enables them to make transactions (e.g. a remote access scam where victims provide remote access to a device which allows the scammer to view and in some cases, transact on the victim's accounts). In this case, payments made by scammers are typically not authorised by the victim.

Authorised and unauthorised payments

In order to cover the types of scams identified by the ACCC in its *Targeting Scams* report[14], the definition will need to extend to scams which involve both authorised and unauthorised payments. We note that some of the scam types raised in the Consultation Paper involve transactions that were not authorised by the consumer, such as phishing and remote access.

CBA's view is that the scams definition should be amended to capture all scam types, including but not limited to, dating and romance; investment; buying or selling; IT scams (remote access, phishing); threat or

[14] ACCC, *Targeting scams – Report of the ACCC on scams activity 2022,* (April 2023), available at: <https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf>



demand based; employment; unexpected money; travel, prizes and lottery; fake charity; and business email compromise scams.

In the Consultation Paper, the following definition of a scam is proposed:

> *"A scam is a dishonest invitation, request, notification or offer, designed to obtain personal information[15] or a financial benefit by deceptive means."*

We believe that limiting the scams definition to an "invitation, request, notification or offer" excludes some scam types (e.g. business email compromise scams) and particularly those with coercion and manipulation at their core.

We agree it is important for the scams definition to recognise that some scams seek access to devices, apps and/or information of a consumer, which then leads to financial harm. However, the inclusion of "personal information" may unintentionally limit the scams covered, in that a scammer may obtain access to a customer's banking login details (i.e. client number) and authentication code, but may not obtain sufficient information about the individual to identify them.

While it is important for the definition to be broad and flexible, the current definition makes it difficult to distinguish fraud from scams. Typically, fraud involves dishonestly obtaining a benefit or causing a loss by deception or other means. Scams involve the same broad concepts but are a subset of fraud. The current definition is very broad and may inadvertently catch many types of fraud:

- a prospective employee who contacts an organisation about a job vacancy who falsely claims to have required qualifications;
- a consumer who requests a loan from a bank and falsely represents their income and expenses;
- a consumer who makes an insurance claim and falsely represents details of the event;
- forgery; and
- cheque fraud.

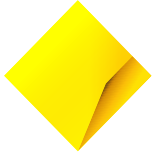
It may also be broad enough to cover some forms of misleading and deceptive conduct (e.g. a deliberately misleading advertisement about the quality of particular goods or services). We note there are existing laws which are sufficient to deal with fraud and misleading and deceptive conduct.

Our view is that the concept of a scam should be clearly defined to include all scams but exclude broader fraud.

We suggest Treasury consider amending the definition to:

> *A scam is an event where a customer may incur a loss because they have been deceived or manipulated into:*
>
> *a. providing a scammer access to, or disclosing information that enables the scammer to transfer the customer's funds or make payments using the customer's account; or*
> *b. making payment/s to another party;*
>
> *in circumstances where:*
>
> *c. the customer is led to believe that the payment or other actions are for a specific purpose when the primary purpose is the theft of funds by the scammer; or*
> *d. the scammer uses a fake identity or otherwise impersonates another.*

[15] 'Personal information' as defined under the *Privacy Act 1988*.



Among other things, the proposed approach reflects two key features of scams being: direct customer involvement in this type of fraud and impersonation. This change would exclude broader fraud and misleading and deceptive conduct from the Framework and help to ensure the definition caters for a broad range of scam types, which will continue to evolve over time, and provide the same protection for all scam victims under the one regulatory regime.

Scams Code Framework and ePayments Code

The ePayments Code concept of an unauthorised transaction is very broad and includes some fraudulent payments as well as payments made in some scams (e.g. phishing scams and remote access scams). We suggest that the legislation make clear that the scams codes are what govern the responsibility of entities relation to their responsibilities when it comes to scams, which in-effect leaves the e-Payments Code to govern other types of fraudulent activity.

Under this proposal, the ePayments Code would continue to address mistaken internet payments and certain other unauthorised payments which might arise from fraud. Examples include:

- payments which are mistakenly made to an incorrect entity, either as a result of a data inputting error, or the incorrect details mistakenly being provided to the customer;
- a merchant inadvertently double charging a customer;
- deliberate double charging by a merchant; and
- customers making the same transaction more than once because they genuinely believed there was an error with the initial transaction proceeding.

CBA believes the scams definition will need to provide a clear distinction between the Framework (under which all scams are captured and considered) and the ePayments Code (under which mistaken payments and unauthorised non-scam payments such as a legitimate seller incorrectly debiting a customer's account more than once are addressed). It will be critical to ensure there is no overlap between the two regimes to provide clarity to entities captured by both, regulators, and dispute resolution mechanisms, and ultimately to ensure appropriate and consistent measures are taken to protect and respond to consumers.

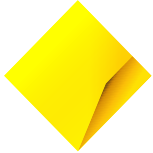
CBA encourages the Government to expedite the review and subsequent implementation of the ePayments Code, ahead of the 2025-26 timeframe proposed in its Strategic Plan for the Payments System.[16] Reviewing the ePayments Code concurrently with the development of the Framework and the payments licensing reforms will help to maximise regulatory coverage for consumers and create as much definitional consistency as possible across regimes.

2.1.2. Designated sector definitions

As noted above, CBA welcomes the inclusion of banks, telecommunications providers, and digital communications platform providers in the Framework. We also suggest that the Framework should be broadened so that it includes from the beginning other payment service providers, stored value facilities, digital currency exchanges, facilitation services such as mass SMS service providers, remote access providers, website hosts, as well as transaction-based digital platforms, such as online marketplaces.

CBA suggests that it is through the designation instrument that sectors captured by the Framework are defined, and we suggest that in addition to a sectoral designation-making power, the Minister should also

[16] Australian Government, *A Strategic Plan for Australia's Payments System,* (June 2023), available at: <https://treasury.gov.au/sites/default/files/2023-06/p2023-404960.pdf>



be given a power to specify a class or classes of entities to whom obligations under the Framework should apply. This should be activity based, i.e. how the activity the entity undertakes is used as part of executing a scam. Consideration should also be given to providing the Minister with the power to modify an obligation.

The Minister should be able to designate classes of entities that do not fit within a current sector but are closely related to those sectors and should be included in the scams ecosystem. The designation powers should in this case specify which code the class should comply with, and which regulator oversees that code. This is important in ensuring that the Framework has flexibility and can adapt in a timely manner as scam types may evolve and expand to use sectors that are not currently being covered or may not currently exist. This also ensures the Minister can designate classes of entities as there are new innovations that do not necessarily qualify as a "sector" for the purposes of designation. We note that similar powers have been proposed in relation to payments participants and systems under the proposed reforms to the *Payments System (Regulation) Act 1998.*

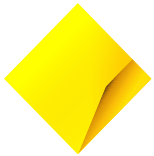
2.2. Principles-based obligations

Consultation questions:
15. Are there additional overarching obligations the Government should consider for 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?
17. Do the overarching obligations affect or interact with existing businesses objectives or mandates around efficient and safe provision of 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?
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?

CBA believes the proposed obligations are appropriately structured to reflect the lifecycle of a scam, requiring steps to be taken to prevent as well as detect, disrupt, and respond to scams to mitigate the impact of a scam on a consumer. Entities that are part of the scam ecosystem should be required to meet the same high-level requirements in responding to scams, which includes knowing their customers, taking a risk-based approach to detect, deter and disrupt scams, and engaging with customers to educate them and support them if they are scammed.

The connection between the overarching principles-based obligations and the sector-specific codes will be important in setting a clear and consistent standard across entities and sectors, creating a consistent experience for customers if they are scammed, minimising weak links in the ecosystem, and establishing a sound foundation for the EDR mechanism to determine whether "at-fault" compensation is required and from which entities.

We suggest the overarching obligations set the expectations for what entities across the ecosystem should do to prevent, detect, and disrupt scams, with any further specificity left to the sector-specific codes and standards, and in some cases, entities' anti-scams strategies. For example, the overarching obligations relating to detection and disruption mention entities acting in a timely manner. Whereas in the equivalent section of the proposed bank-specific code and digital communications platforms code, the expectation is that entities act quickly (noting there is no equivalent requirement in the current telecommunications obligations listed in the Consultation Paper).



The role of a consumer to take appropriate due diligence should also be recognised in the principles-based obligations. While this does not detract from entities' responsibilities, it is important to recognise and help ensure that customers are incentivised to act with care.

We also note that obligations tend to fall into two types:

- evaluative obligations that are predominately preventative obligations where there could be multiple correct approaches to meet the obligation; and
- prescriptive obligations which are predominantly reactive steps that can be prescribed and can be assessed as whether they were satisfied or not, including SLAs.

For evaluative obligations, which will be judged in an ex-post environment, we suggest that obligations outline that entities must demonstrate they have taken "reasonable steps" to comply with an obligation. This provides flexibility and reflects that there may be multiple approaches to meet an obligation and that entities should take a risk-based approach to comply.

It is also important that the obligations are couched as broad obligations, rather than requiring prescriptive actions which may soon be out of date and/or may not suit all organisations or all situations. For example, given the Framework will capture large and smaller organisations, it will be difficult to stipulate specific timeframes for compliance. In some cases, a larger organisation may be expected to meet higher expectations compared to a smaller organisation. Rather than trying to deal with these differences in the principles-based or sector-specific code obligations, it may be that this detail is more effectively captured in the anti-scam strategy that each organisation will be required to prepare (see below section 2.3).

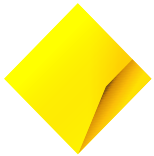
Some initial observations on the proposed overarching principles-based obligations include:

- *Detection and disruption obligations* – We note that the first proposed obligation in this section proposes that "a business must seek to detect, block and prevent scams from initiating contact with consumers". While it's appropriate for all entities to seek to detect, block and prevent scams, not all entities may be able to prevent scammers from initiating contact with consumers given the nature of their business. We therefore suggest that "from initiating contact with consumers" be removed or modified with "where practicable" and the obligation refer to detecting and blocking "scams" and preventing "scammers". We also suggest modifying the obligation for entities to provide "consumers or users with tools to verify information in real time" with "reasonable steps" given an entities' inability to verify all information with complete accuracy in real time.
- *Definition of a consumer* – The obligations refer to "consumers" and we seek clarity on the definition of this term as it applies throughout the Framework.

Principles-based obligations for information sharing

We suggest the overarching reporting obligations should require the sharing of individual incidences of scams. To help streamline the reporting obligations of entities, an information-sharing platform should be used to facilitate the timely sharing of information between entities and across the ecosystem. This would facilitate the obligation for a recipient entity to investigate and act on intelligence promptly.

The use of one platform would enable entities to share once, minimising duplication. Leveraging existing infrastructure like the AFCX would facilitate the faster establishment of ecosystem-wide intelligence sharing and enable the AFCX to support the NASC by providing near real-time data on scams trends. There would be an opportunity for consumers and the NASC to feed information into the AFCX system, providing a one-stop-shop for information sharing.



The NASC could then share the reporting received through the AFCX to other regulators involved in the Framework and could leverage the trend reporting and intelligence on new or emerging scam threats to establish fusion cells and/or initiate communications to consumers to inform them of these threats and actions they should take to protect themselves.

2.3. Anti-scam strategy obligation

Consultation questions:
20. What additional resources would be required for establishing and maintaining an anti-scam strategy?
21. Are there any other processes or reporting requirements the Government should consider?
22. Are there parts of a business's anti-scam strategy that should be made public, for example, commitments to customers that provides customers an understanding of their rights?
23. How often should businesses be required to review their anti-scam strategies and should this be legislated?
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?
25. What level of review and engagement should regulators undertake to support businesses in creating a compliant anti-scam strategy?

CBA supports entities being required to develop and maintain an anti-scam strategy, detailing how they will prevent, detect, and respond to scams. We believe the requirement of an anti-scam strategy in the overall objectives of the Framework can be met by allowing the flexibility of the risks faced by individual business models to be appropriately addressed.

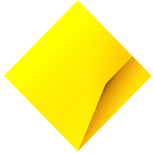
The requirement to have an overarching strategy is a feature of the ABA's Scam-Safe Accord, announced in November 2023. CBA notes that other regulatory regimes, such as the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) regime, require entities to adopt and maintain comprehensive risk programs. For example, an AML/CTF program must specify how an entity complies with AML/CTF obligations, which includes identifying, mitigating, and managing the money laundering and terrorism financing risks it faces in providing products or services to a customer.

AUSTRAC also requires Board and senior management approval and ongoing oversight of Part A of an entity's AML/CTF program. We suggest a similar approach to the anti-scam strategies required under the Framework would be appropriate.

The Framework should provide entities with the flexibility to develop appropriate procedures that are commensurate to their business model, operations, and relevant scams risk. This would enable entities to develop anti-scams strategies that are risk-based according to their size, nature, and level of complexity, and ensure that the allocation of an entity's resources has the maximum impact.

Combatting scams is extremely complex as scammers continually adjust their methods to maximise the chances of being successful but also in response to initiatives of governments and entities. Regular reviews of anti-scams strategies, on a 12-month basis, will be important to ensure entities continue to update and improve their methods for detecting and disrupting scams.

We consider that the anti-scams strategies could be the mechanism through which specific timeframes/SLAs for acting in response to scams are articulated. The inclusion of SLAs in anti-scams strategies will enable entities to tailor their response timeframes based on their size, nature, and risk, with the ACCC providing oversight of appropriateness and consistency across entities and the ecosystem.



We believe the strategies should not be published given their likely sensitive and tactical nature and, in the instance of SLAs, would help avoid divulging information that scammers would seek to exploit and use to adapt their methods. Rather, it could be provided to regulators, and entities may choose to detail on their website an overview of how they seek to protect their customers from scams.

2.4. Information sharing requirements

Consultation questions:
26. What resources would be required for establishing and maintaining additional information sharing arrangements with other businesses, the NASC and sector-specific regulators under the Framework?
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?
28. What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?
29. Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?

CBA strongly supports the overarching requirement for entities to share scams intelligence across the ecosystem. Leveraging the collective knowledge of consumers, entities, and government to detect a scam and act quickly to stop it being used by scammers, through the timely sharing of information will be a crucial tool in minimising the impact on consumers.

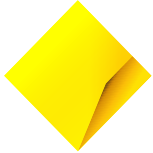
CBA also supports the overarching obligations for information-sharing being reflected in the sector-specific codes. We note as currently drafted, this appears to only require sharing of information between entities within a particular sector. For example, the reporting obligations in the sector-specific codes outlined in the Consultation Paper state that banks must share information with other banks; digital communications providers must share information with other digital communications platform providers and the NASC; and telecommunications providers share information with other providers and ACMA.

We believe this model of information-sharing, where there are multiple reporting mechanisms, wouldn't be effective, as it would involve the sharing of information more than once, increasing the time it takes for entities to receive scams intelligence, and ultimately impacting their ability to respond to or intercept a scam in a prompt manner.

To maximise the effectiveness of the Framework, we suggest the information-sharing obligations under the Framework, including the sector-specific codes, require sharing between all entities and across sectors and a requirement to act on the intelligence. The obligation should also be consistent across sectors and require sharing with regulators, law enforcement, and the NASC. This will support a consistent, efficient, and timely model.

Significant efficiencies can be gained by streamlining reporting processes through the use of one platform to minimise the duplication of one-to-one sharing between entities. The timely sharing of scams intelligence (i.e. the enablers of a scam, such as phone number, social media account, website address, account details) through a single platform will assist entities to take action, and supplemented by SLAs, will help to better protect consumers.

We note that the proposed overarching information-sharing obligations in the Consultation Paper require the sharing of "suspected or identified organised large-scale scam activity as well as rapidly emerging or



cross-sectoral scam activity" and that a "business must share data and information on the incidence of scams, and action taken in response."

CBA suggests the ecosystem should require the timely sharing of all scam incidences through a trusted platform like the AFCX, enabling entities to act to protect consumers. This would provide entities with a richer source of data to assist more timely investigations to verify scam activity and take the appropriate actions, such as blocking phone numbers from making further calls, blocking social media accounts, as well as initiating the trace and recovery of funds.

The AFCX, which is industry-funded, currently has more than 50 members sharing information across the banking, digital currency exchanges, and telecommunications sectors as well as the public sector. In FY2023, $1.5 billion in scams were reported to the AFCX by its members, totalling more than 193,000 transactions.

The AFCX is currently used by members to share data relating to potential fraud including scams through:

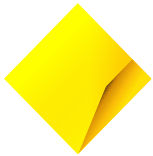
- members sharing with the AFCX over six data catalogues relating to fraud and scams, which assist the data consuming entities in more accurately managing their fraud/scam risk;
- hosting an intelligence-sharing portal for law enforcement and private sector to collaborate together on targeting chosen criminal syndicates; and
- operating a Fraud Reporting Exchange (FRX), which is a platform that permits the timely freezing and recovery of funds by banks for fraud and scammed consumers. It has more than 20 participating members, enabling the trusted and secure sharing of data between issuing and recipient financial institutions to report and act in relation to scam activities. Between January and November 2023, more than 34,000 cases were raised via the FRX.

Under the ABA Scam-Safe Accord, ABA and COBA member banks have all agreed to join the AFCX and receive and use AFCX data to fight scams (if not already members) and use the FRX platform to help accelerate funds recovery processes for consumers. CBA is already participating in these initiatives and most banks are expected to have this capability in place in 2024.

This infrastructure should be leveraged to support the NASC in its information-sharing role and streamline the sharing of information between entities to meet their obligations under the Framework. Given the AFCX is industry-funded, if it is used in this way it would remove the need to duplicate systems and therefore reduce the need for additional government funding.

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

The use of SLAs informed by AFCX data in relation to investigating and acting on verified scams intelligence should supplement the obligation to share individual scams intelligence with other entities and across sectors. A minimum time period to share consumers' reports of a scam and also to commence an investigation into scam intelligence shared through the AFCX could be required within entities' anti-scams strategies. This approach would enable the time periods to reflect the size and nature of different entities. The use of SLAs would also incentivise entities to investigate and act on scams intelligence, as a failure to do so would be a breach of obligations, potentially resulting in compensation being paid and enforcement action.



There may be an opportunity to explore whether the AFCX platform could also be used to report failures to meet timeframes, with reports shared with the ACCC and then subsequently other regulators, such as ACMA and ASIC, as regulators under the Framework. This would further streamline the reporting requirements of entities, and support regulators in their monitoring and enforcement role.

2.5. Consumer reports, complaints handling and dispute resolution requirements

Consultation questions:
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?
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?
32. Should the Government consider establishing compensation caps for EDR mechanisms across different sectors regulated by the Framework? 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?

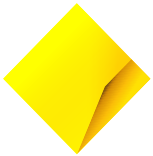
CBA supports providing a means for scam victims to be compensated, via Internal Dispute Resolution (IDR) or External Dispute Resolution (EDR), where it has been determined that an entity or entities have failed to meet their obligations under the Framework.

CBA suggests the EDR mechanism for the Framework should be guided by the following principles:

- Clarity – provide a clear, accessible pathway and one front door for consumers.
- Efficiency – minimise duplication of resources and avoid referrals between mechanisms. The time taken to investigate and resolve a matter for a customer is an important consideration, as well as the overall cost of operating the EDR mechanism.
- Consistency – case investigation processes, criteria for apportioning compensation, and compensation caps should be consistent across the ecosystem. Double recovery should not be possible.
- Accountability – all parties in the ecosystem are obliged to take reasonable measures and, in the case of consumers, act with care. All parties are accountable if they fail to meet their obligations.
- Certainty – any framework should be consistent with existing legal principles on how a consumer who suffers harm receives compensation and have appropriate privacy provisions amended to allow for efficient information sharing between involved parties.

Ultimately, any EDR scheme should incentivise all participants to play their part – for consumers to act with care and due diligence, and for entities to invest in scams prevention and detection.

CBA holds the view that a single scams EDR mechanism will provide customers with a clear pathway to seek redress in a timely manner and provide the clarity, efficiency, consistency, accountability and certainty required to ensure the Framework works most effectively.



Some of the benefits of a single scams EDR approach include:

- providing consumers with a clear pathway to seek redress, avoiding the need for a customer to approach multiple EDRs and limiting the potential for time-consuming referrals between mechanisms;
- providing entities and the EDR mechanism with clarity on the basis for which it is considering a complaint – i.e. complaints can only be made in relation to scams, as defined under the Framework, and only obligations under the Framework and sector-specific codes are considered;
- enabling one body to consider and investigate complaints in line with the scam lifecycle and obligations under the Framework, minimising duplication of resources, and enabling a timely resolution for consumers;
- promoting a consistent approach to investigations, determinations and apportioning of compensation across the ecosystem; and
- complementing the Government's whole-of-ecosystem approach.

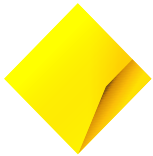
We recognise a single scams EDR mechanism does not completely align with the stated goal of leveraging existing processes and mechanisms and will require the establishment of a new scheme and legislation. However, we note there currently is no EDR mechanism established for digital platforms and the multi-EDR proposal outlined in the Consultation Paper will require legislative changes to the remit and scope of existing mechanisms and will also need to ensure consistency across these schemes in terms of definitions, time limits, compensation caps, and processes to ensure an equivalent customer experience, no matter the mechanism.

On IDR, we welcome IDR being required across all entities under the Framework. Early resolution via IDR may be possible in some instances; however, with the introduction of a new Framework the single scam EDR mechanism may need to play a role in reviewing test complaints or representative cases to establish patterns in key scam scenarios for IDR teams to consider, at least initially. The ultimate design of the EDR should consider supporting the effective operation of IDR schemes across the ecosystem. For example, there may be an asymmetry of information available for EDR and IDR. Generally, there can be some difference in type of information available as a complaint progresses from IDR to EDR. However, in this context there could be a complete absence of information about the potential acts or omissions of another participant in the ecosystem. Such information would be relevant to assessing the overall outcome for a consumer but may only be available at the EDR stage of a complaint. This is an issue that does normally manifest in a typical IDR-EDR context.

Further, where sectors and associated entities have been excluded from the Framework, consideration will need to be given to the impact of this on consumers and their right to seek compensation, particularly when entities within designated sectors have met their obligations (particularly, but not exclusively cryptocurrency exchanges). Ensuring that the Framework has broad coverage and few, if any, exemptions will help to ensure entities are incentivised to prevent scams and where consumers do fall victim, appropriate redress is available where entities fail to meet their obligations under the Framework.

Complaints and compensation

All parties in the ecosystem should be obliged to take reasonable measures and, in the case of consumers, act with care, and should be accountable if they fail to meet their obligations. Where a consumer has acted with reasonable care and one or more entities did not comply with their obligations, then compensation would be payable under the IDR or EDR processes. Where there is no breach of obligations from any of the entities involved, then compensation would not be payable. Determining whether compensation is payable would require identification of whether any of the participants have failed to meet their obligations.



The EDR mechanism should be a body that solely determines whether an entity or entities have breached their obligations under the established Framework and determines compensation where breaches have occurred. Guidance on how entities may comply with the codes should remain within the domain of regulators under the Framework (i.e. ACCC, ASIC or ACMA).

Overall, CBA believes the EDR scheme should seek to ensure clarity is provided for all participants, consistency in approach is achieved, duplication and complexity is minimised to enable the efficient resolution of complaints, and all parties are incentivised to act to address scams. This will lead to a better customer experience and reinforces responsibility for scam prevention and response across the whole ecosystem.

3. Sector-specific codes and standards

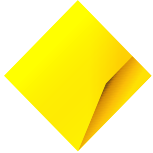
Consultation questions:
34. Are sector-specific obligations, in addition to the overarching obligations in the CCA, appropriate to address the rising issue of scams?
35. Are there additional obligations the Government should consider regarding the individual sector codes?
36. Do the obligations considered for each sector reflect appropriate consistency across the scams ecosystem?
37. Are the proposed obligations for the sector-specific codes set at the right level, sufficiently robust, and flexible?
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?
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?
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?
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?
42. Are there additional areas the Government should consider in ensuring appropriate interaction between the bank-specific scams code and the ePayments Code?

CBA supports the inclusion of sector-specific codes in the Framework, which will help drive consistency in the prevention, detection and disruption, response and reporting actions undertaken by individual entities across the ecosystem.

Where sector-specific codes apply to a range of entities, we suggest that the codes set overarching obligations for all entities captured under that code to comply with, along with sub-sector obligations that are activity-based to capture for the different nature of business activities (in the context of scams).

Overall, the sector-specific obligations should align with each of the overarching principles-based obligations, to help promote consistency across the ecosystem. We note that our earlier comments relating to Framework obligations around evaluative versus prescriptive obligations are also relevant to sector-specific code obligations.

With obligations under the Framework, entities should be able to implement solutions which are fit-for-purpose given their particular operating environments. The regulatory framework must have flexibility to ensure that entities can develop appropriate procedures that are commensurate to their business model, operations and relevant scam risk. Flexibility will also be important in enabling entities to adjust as scammers do and develop new and innovative initiatives to combat scams.



The inclusion of SLAs in anti-scams strategies will enable entities to tailor their response timeframes based on their size, nature, and risk, with the ACCC providing oversight of appropriateness and consistency across sectors and the ecosystem. Timeframes should balance what demonstrates reasonable steps across a range of entities, with uplifting standards across the ecosystem.

To ensure greater consistency is achieved, a more coordinated approach could be taken in the development of the sector-specific codes. In the Consultation Paper, two different methods are proposed – one is industry-led for the telecommunications providers code and the other is government-led for the development of the banking and digital communications platforms codes.

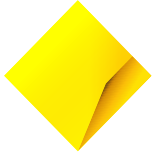
We suggest that all codes be developed centrally and led by government to ensure a consistent approach is taken to establishing obligations across the lifecycle of a scam, particularly where a scam is initiated via one provider's systems and takes place on another platform. This approach is critical as the obligations established under each code should set a consistent experience for consumers and will underpin the dispute resolution mechanism implemented under the Framework. A consistent approach to the future review and update of codes will be required as well.

Possible bank-specific code obligations

CBA notes the Consultation Paper includes possible bank-specific code obligations and we make the following initial observations.

Prevention

- *Confirmation of the identity of a payee* – the banking industry has committed, via the ABA Scam-Safe Accord, to roll out name checking technology, where entities have not already done so. This technology will assist consumers to know who they are dealing with. We note that this technology will be rolled out for payments made via the New Payments Platform (NPP), accounting for an increasing share of transactions via that platform as other ageing platforms, like direct entry, are being phased out. This obligation should be updated to reflect this.
- *Identification of high-risk transactions* –
    - this obligation states "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." We consider that the obligations should express that banks must have processes in place that are designed to detect high-risk activity, rather than stipulating an entity must determine what individual consumers 'normal activity' may be, which can be variable for a range of reasons. This reflects the fact that the EDR will be judging the transaction ex-post, while the bank is operating in an ex-ante environment. As an evaluative obligation, we consider that the requirement should be modified to "A bank must implement processes ***to seek to*** verify a transaction is legitimate where a ***consumer*** undertakes activity that is identified as ***high risk*** and is or is likely to be a scam."
    - there may also be challenges in complying with this obligation when multiple parties, including non-banks are involved in a transaction. For example, in PayTo transactions which allows 'nested' payment requests where a payment provider can onboard other payment providers (i.e. sponsored third parties, who can also sponsor other third parties). As a result, three or four payment providers may be involved in processing a payment from the consumer's bank. The payment initiator has responsibility for conducting due diligence when on-boarding the final merchant or ultimate beneficiary. The customer's ("payer") bank has no visibility over the end-to-end transaction and is obliged to execute a validly authorised PayTo agreement unless they have fraud concerns. In this scenario, the multiple parties involved between the sending and receiving bank are in a position to assist with trace and recovery that would increase likelihood of returning a customer's funds.



- *Warnings* – while we agree with the need for warnings, we want to ensure warnings are timely and purposeful to avoid desensitisation. Too many warnings of the same nature (e.g. pop up text boxes or check boxes) can lead to warning blindness and ultimately become ineffective. We also note that a bank does not have the ability to issue warnings on some payment channels, like digital wallets.

Response (obligations to consumers)

- *Methods for consumers to take immediate action* – we support the need for consumers to have a clear and easy pathway to report scams and act in response. We note the Consultation Paper includes an example of an "in-app freeze switch". An immediate freeze on accounts could have a range of unintended consequences, such as consumers missing critical payment deadlines, not receiving payments, and being unable to undertake routine activities. In addition, it may not address all scam types, like account takeover, and would be complex to implement. In the case of authorised payments (like an investment scam), the freeze functionality would not be effective as the consumer's account has not been compromised, given it is the genuine consumer making the transaction.
- *Trace and recover* – banks have committed to using the FRX to action trace and recoveries. We suggest the statement of "a receiving bank to revert a transfer" should be amended to remove the word "revert" and specify that this is only possible where recoveries are available.
    - Currently, the ePayments Code prescribes the process and obligations of ADIs to co-operate to trace and recover funds from an unintended recipient's account in the case of mistaken or unauthorised payments.
    - As noted above, numerous non-bank and bank intermediaries may now be involved in processing a single transaction. To increase the likelihood of recovering consumer funds, all participants (both sending and receiving institutions) should have obligations to participate in the process to retrieve misdirected funds and minimise financial loss by consumers.

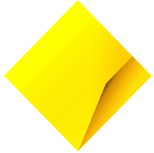
Proposed obligations for other sectors

The Consultation Paper notes that possible bank-specific obligations may require banks to "have processes in place to identify consumers at a higher risk of being targeted by scammers (vulnerable cohorts)". We suggest this should be an obligation on all sectors covered by the Framework, given the susceptibility of vulnerable consumers to being deceived by scammers. In doing so, a consistent definition of "vulnerability" will be required across all sectors within the Framework. In its *Targeting Scams* report for 2022, the ACCC highlights those Australians continuing to lose more money to scammers tend to be those who are older, Indigenous, Culturally and Linguistically Diverse Communities (CALD), and people with a disability.[17]

We also note the Consultation Paper outlines some of the current obligations of the existing telecommunications Reducing Scam Calls and Scam Short Messages Code, as well as possible obligations for digital communications platforms.

An issue that impacts businesses across the economy is scammers imitating companies' alpha tags (i.e. SMS sender name) to insert fake SMS' into an existing SMS chain of a genuine business. This deceives consumers and gives them the impression that they are dealing with a genuine business, putting consumers at risk of engaging with the message and ultimately the scammer. These phishing/smishing scams are widely seen, with recent examples involving Linkt, AusPost as well as financial institutions,

[17] ACCC, *Targeting scams – Report of the ACCC on scams activity 2022,* (April 2023), available at: <https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf>



amongst others. Further, more than 47 per cent of Australians have reported exposure to fake or deceptive text messages.[18]

To help address the misuse of alpha tags, telecommunications providers and mass SMS service providers should be required to remove this method for a scammer to initiate contact with and deceive consumers. We welcome the development of the Government's SMS Sender ID registry, which will play an important role in combatting this practice of scammers, and welcome the intent to mandate its use.

We seek clarity on whether use of the SMS Sender ID registry will be mandated through obligations in the sector-specific codes and for telecommunications providers, whether this obligation would extend to ensuring they use the registry to protect their business-to-business customers who may or may not be captured by the Framework.

This would align with the proposed overarching principles-based obligations that a business "must seek to detect, block and prevent scams from initiating contact with consumers" and "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."

An equivalent approach could be taken in relation to website hosts to ensure that scammers cannot create websites and domain names imitating legitimate businesses. Similar to alpha tags, there may be an opportunity to require more rigour and obligations to verify the details of persons registering domain names.

4. Approach to oversight, enforcement, and non-compliance

Consultation questions:
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?
44. Are there other factors the Government should consider to ensure a consistent enforcement approach?
45. Should the penalties for breaches of sector-specific codes, which sit in their respective sector legislation, be equal across all sectors?

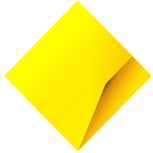
In leveraging existing regulators to monitor and enforce sector-specific codes, regulators should have commensurate powers, resourcing, and capabilities to undertake these roles in a consistent manner.

To ensure additional costs and duplication are minimised, the monitoring and enforcement roles of existing regulators (e.g. ASIC, ACMA) should be leveraged for the Framework. The use of one information-sharing platform would also help to streamline reporting between entities and regulators, again reducing duplication and improving efficiency of the overall Framework.

The Government may seek to achieve consistency in oversight and enforcement through:

- Alignment between each set of sector-specific codes obligations and the overarching principles-based obligations.
- Equivalent monitoring and enforcement powers, including penalties, embedded within legislation for breaches of sector-specific codes.
- Establishing scams as a priority area for each regulator, such as through statements of expectations.

[18] Australian Government, *SMS Sender ID Registry set to protect more Australians from scammers,* (December 2023), available at: <https://minister.infrastructure.gov.au/rowland/media-release/sms-sender-id-registry-set-protect-more-australians-scammers>



- Establishing Memorandum of Understanding and/or an equivalent of the Council of Financial Regulators to ensure ecosystem regulators are coordinated and consistent in their approach to scams.

CBA supports penalties for sector-specific code breaches being equivalent across sectors to the extent possible. This will ensure businesses are equally incentivised to meet their obligations, uplifting standards and protections across the ecosystem, and will help ensure a consistent regulator enforcement approach.

An important consideration in the implementation of multi-regulator oversight of the Framework are the penalties to which an entity could be subject to for breaching an obligation. The enforcement penalties should be commensurate to the seriousness of the breach, for example repeated offences or systemic failures.

5. Conclusion

Collective action and the timely sharing of information across the ecosystem is required to combat scammers and protect consumers, and we welcome the whole-of-ecosystem approach underpinning the Framework.

The Framework will change the scams environment in Australia. To ensure the Framework achieves maximum effect from the outset, we also suggest the development of the Framework take into consideration the need for clarity, efficiency, consistency, and accountability to incentivise the right outcomes. We also encourage minimising exceptions to ensure scammers have less opportunity to adapt.

We would welcome the opportunity to further contribute to the development of the Framework and the sector-specific codes.