NATIONAL AUSTRALIA BANK SUBMISSION

Scams – Mandatory Industry Codes

2 February 2024

National Australia Bank Limited ABN 12 004 044 937 AFSL and Australian Credit Licence 230686

Introduction

National Australia Bank (NAB) welcomes the opportunity to respond to the Department of Treasury (Treasury) consultation on Scams – Mandatory Industry Codes (Consultation Paper).

NAB's response is guided by the 45 questions in the Consultation Paper and some responses address multiple questions at once. As a member of the Australian Banking Association (ABA), NAB has contributed to their submission to the Consultation.

Scams are a global epidemic with devastating impact on people and society. They are an increasing part of the sophistication of global organised crime working beyond laws, regulation and ethics.

NAB has engaged closely with Government and other agencies for several years on scams and welcomes the Government's action to date. NAB has strongly encouraged a cross-sector approach and looks forward to enhanced coordination of Australia's national response between the public and private sectors, and across sectors that the Mandatory Code will apply to.

NAB has a comprehensive, bank-wide scam strategy in place with 33 initiatives delivered in NAB's 2023 financial year to reduce the impact of fraud and scams on customers. NAB is also mindful that criminals gravitate towards points of least resistance when seeking to steal from customers, so we seek to contribute as much as possible to the coordinated national response. This is the best way we can stop the crime before it occurs and make Australia a difficult place for criminals to be successful.

Executive summary

NAB supports establishing an ecosystem approach with overarching obligations augmented with those for specific sectors. NAB encourages the rapid inclusion of additional sectors beyond the three initially proposed to ensure we can best protect our customers and the community. NAB also urges the proposed obligations for digital communication platforms and telecommunication providers to be strengthened so these sectors face obligations which are more consequential and better aligned to those proposed for the banking sector.

In relation to other key issues, NAB:

- Supports the proposed multi-regulator model but believes that consistency and coordination in enforcement between regulators is critical for comparable outcomes.
- Urges that existing infrastructure and mechanisms for sharing data, such as those provided by the Australian Financial Crimes Exchange (AFCX), be fully utilised and prioritised.
- Believes there is merit in having a single external dispute resolution (EDR) scheme for all scam complaints, particularly as the framework matures and additional sectors are added over time. If a single scheme is not adopted, then greater alignment between existing industry specific EDR schemes is needed to ensure more consistent decision making for scam-related cases.

Further refinements and more detail on several components of the proposed Framework will be required to give greater clarity to the proposed obligations.

Section 1: Proposed Framework

Question 1: Does the Framework appropriately address the harm of scams, considering the initial designated sectors and the proposed obligations outlined later in this paper?

NAB welcomes the Government's commitment to developing an ecosystem approach and supports the initial focus on banks, telecommunications providers and digital communications platforms. However, there are other sectors (e.g. digital currency exchanges, online marketplaces, payment system operators) that should also be an initial designated sector, or added at the first available opportunity when additional sectors are designated.

In order to answer the question of whether the Framework appropriately addresses the harm of scams, NAB requires further information on how the Framework is intended to operate with respect to scam activity that involves one or more of the designated sectors as well as one or more businesses in sectors not covered by the Framework. Clarity on how liability will be apportioned across sectors will also be critical to ensure the success of the ecosystem approach.

NAB supports the Government's intention to make the Framework flexible and responsive. Organised criminal groups involved in scam activity are adept at identifying weaknesses in systems and controls. In this respect, the legislation and associated regulations will need to be drafted with sufficient flexibility to enable quick responses to any changes in the operational environment.

Question 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?

NAB believes the proposed two-layer approach is sound in terms of principles and obligations. We note the Government's intent for the Framework to complement and leverage existing interrelated regimes, systems and initiatives. As such, NAB supports the Framework's focus on establishing general principles-based obligations and recommends complaints related to individual scam instances continue to be managed separately through EDR schemes (see response to Section 6 for further detail).

Question 3: Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?

NAB agrees the Australian Competition and Consumer Commission (ACCC) is the appropriate regulator for consumer protections from scams across all sectors. However, it is unclear how the ACCC's "principles-based" approach would be legislated. This could potentially be managed in a manner similar to the "general obligations" in section 912A of the Corporations Act 2001.

NAB also agrees the Australian Securities and Investments Commission (ASIC) is the appropriate regulator for a code containing bank-specific obligations. NAB believes there is merit in having a single EDR scheme for all scam complaints, particularly as the Framework matures and additional sectors are added over time. In utilising a single EDR scheme, NAB encourages using the expertise

and structures of existing entities to benefit consumers rather than establishing new structures. Regardless of whether a single or multi EDR model is adopted, it is critically important that consumers have access to EDR schemes from the commencement of the Framework.

Irrespective of the mechanisms and regulators adopted, successful implementation will require clarity and coordination between all entities, including those not directly responsible for overseeing the Framework. For example, scams are considered a predicate offence under the *Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act 2006,* which places responsibilities upon reporting entities enforced by AUSTRAC.

Question 4: Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors?

The enforcement mechanisms need to be clarified. A Framework involving multiple sector-specific codes creates potential inconsistencies in the application and effect of those enforcement mechanisms. The requirements on each sector also have significant differences, so the specifics of the obligations are likely to vary. Noting these challenges, enforcement should still aim to be as consistent and coordinated as possible through existing authorities.

Further detail on the specific roles of the ACCC, the National Anti-Scams Centre (NASC) and the various sector-specific regulators will help identify issues that might need to be addressed. This includes the need for clarity on which regulator will take the lead and how regulators will coordinate their response. As noted later in our response, there should be clear delineation between the enforcement role of principle regulators (the Australian Communications and Media Authority, ASIC, ACCC), AUSTRAC and EDR entities.

Question 5: Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?

NAB believes the Framework is capable of capturing other sectors where scams may take place currently provided obligations are consistent across sectors and there is a common minimum standard enforced by regulators. The Framework should be the subject of ongoing review as new and most likely more complex criminal typologies are introduced by organised crime.

Question 6: What future sectors should be designated and brought under the Framework?

NAB believes there are a number of priority sectors the Government should consider bringing under the Framework, either initially or at the first available opportunity when additional sectors are designated. These include:

- digital currency exchanges
- online marketplaces
- payment system operators (e.g. digital wallets)

While NAB recognises the value of a phased approach, scam activity is already prevalent in these sectors and in some cases, easily perpetrated by opportunistic individuals as much as organised

groups. They often play a pivotal role in facilitating the movement of illicit proceeds from scams. Excluding or delaying the inclusion of these sectors will potentially increase the risk that scammers will shift their activities to sectors with weaker systems and controls.

In addition, other sectors that could be designated in future include: non-bank financial institutions, providers of Artificial Intelligence services, managed funds and superannuation, insurance companies, and gambling service providers. If new platforms, services or disruptors enter the market and are identified as sectors where scam activity is becoming increasingly prevalent, they should also be brought under the Framework as a priority. Protecting customers should be the primary focus, regardless of the avenue of the scam activity.

Question 7: What impacts should the Government consider in deciding a final structure of the Framework?

While the Framework's principles and obligations on the banking sector appear sound, more detail is required on their practical application. The detail of what banks need to do to be considered compliant with the Framework will be crucial to understanding the timeframe and cost of achieving compliance.

The impact on the customer should be a driving factor when considering the final structure of the Framework. Considerations should include how to protect customers from scams while not stifling innovation, ensuring customers can easily navigate the 'ecosystem' after experiencing scam activity, and clearly specifying consumer's obligations in the use of banking and other designated sector products and services.

The Government should also consider other relevant changes that banks may concurrently be implementing at a similar time to complying with the new Scams Code, such as the proposed AML/CTF legislative reform currently under consideration (known as tranche two reforms). Another consideration, which would be dependent on the level of change required, is the possibility for unintended consequences. How the Government expects the Framework to interplay with the ePayments Code will also be an important factor.

Section 2: Definitions

Question 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?

Maintaining alignment between definitions of 'scam' and 'fraud' is crucial. The definition of 'scam' is important as it will determine what is in and out of scope under the Framework obligations and will determine 'jurisdiction' under the Code for regulators and EDR entities. The definition should provide comprehensive coverage of 'scams' while not overlapping with existing definitions and obligations for other scenarios, such as fraud (unauthorised), disputes covered by the ePayments Code, and financial abuse. NAB encourages the Government to consider definitions used in overseas

jurisdictions and to focus on the types of criminal conduct that have the most serious impact on consumers as it finalises the definition of a scam.

Question 9: Does a 'dishonest invitation, request, notification, or offer' appropriately cover the types of conduct that scammers engage in?

NAB recognises the challenge in agreeing a definition of a 'scam' and strongly supports the Government's intention to agree a definition that can be consistently applied across sectors and regulatory regimes.

Specific feedback for consideration is adding the below two highlighted words:

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

Other general points for consideration include:

- Reference to the victim knowingly and willingly facilitating the payment, transaction or provision of information to the offender that permits the scam to be completed. This is a distinct feature of scams and differentiates almost all scams from other types of fraud.
- Whether the definition could blur delineation between financial abuse and scam events.
- If there should be any reference to a payment being made.
- How to appropriately capture the criminality aspect, which differentiates scams from other types of consumer disputes that could otherwise unintentionally be captured by the Framework.
- Making clear that the scammer need not be successful.

Question 10: Does the proposed definition of a scam appropriately capture the scope of harms that should be regulated under the Framework?

The Consultation Paper states that *"the proposed definition is not intended to capture unauthorised fraud, such as cybercrimes that may use hacking, data breaches, and identity theft, that do not involve the deception of a consumer into 'authorising' the fraud."* However, the definition is intended to cover scams such as phishing and remote access, both of which are typically considered 'notifiable data breaches' under the *Privacy Act* 1988. To clarify the definition, one approach could be to define what the Framework excludes (in terms of activities) so it is clear when certain conduct will not be governed by the Framework.

The proposed definition is also limited to 'personal information' or a 'financial benefit'. NAB questions whether the Government also intends for scams involving 'sensitive commercial information' to be in scope of the Framework. The Government may also wish to consider including 'causing a harm or loss' within the definition.

Question 11: What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?

Flexibility and adaptability in a rapidly changing operational environment will be critical, as will clarity of application (such as what is in and out of scope). Some types of scams should clearly be in scope – for example, investment, romance and invoice scams – but other activity is less clear and needs careful consideration. This includes activity related to the sale of goods and services, as described in the Consultation Paper. On digital communication platforms and online marketplaces, it is often unclear when a seller is not legitimate. In NAB's view, it would be inequitable to introduce obligations on banks to address these types of scams when the enablers (in this case, the digital communication platform or online marketplace) have no obligations under the Framework and the activity leading to the scam is unlikely to be visible to a bank.

Even when a definition of 'scam' has been agreed, it is important to recognise there will still be instances where it will be challenging to attribute a specific event to be the result of a fraud, scam or other scenario (such as a dispute or financial abuse). There are a variety of ways that criminals communicate with victims or enable a scam. Typically, these communications and interactions between victim and criminal are not visible to a bank. While a bank may (unknowingly) assist a victim in facilitating a payment that is subsequently discovered to be a scam, the context and background to the payment will often only be provided to the bank when the victim reports the event.

Other challenges may arise for banks in understanding which transactions are in scope of the Framework. As a practical example, a scam event may consist of several transaction 'hops', involving a 'sending' bank alongside any number of other potential 'recipients' followed by further layering of funds across the broader system. Similarly, a scam victim may also seek to transfer or consolidate funds across different banks and/or other payment channels into accounts in their own name, such as a wallet with a Digital Currency Exchange. NAB believes it would be helpful to clarify which of these specific payment events or 'hops' would be considered in scope of the Framework and 'who' specifically would be accountable for any of the obligations under the Framework.

Question 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?

In order to answer the question regarding unintended consequences, further clarity is required on the definition of a digital communications platform and the types of services specified in the Consultation Paper. For example, if goods and services scams are intended to be covered by the 'scams' definition, there is a strong case for online marketplaces (not currently covered by the Framework) to be captured in the digital communication platforms definition.

Question 13: Should the definitions of sectors captured by the Framework be set out in the primary law or in the industry-specific codes?

In NAB's view, the most important consideration will be ensuring there is sufficient flexibility to allow additional sectors to be designated under the Framework as the operational environment evolves.

Question 14: What impacts should the Government consider in deciding the definitions of digital communications platform or ADI?

The Government should consider how to prevent businesses from actively changing their business model to fall outside the scope of the Framework and avoid specific obligations (e.g. the use of 'primary function' in the description of digital platform services intended to be covered by the definition of digital communication platforms). NAB would recommend a wider definition that includes any platform that advertises or hosts links to third parties through which consumers can access information, products or services.

More broadly, NAB believes non-bank financial institutions should also be included in the Framework in the near future. The current proposal to cover only Authorised Deposit-Taking Institutions (ADIs) is likely to result in scammers re-focusing their activity on less regulated financial institutions that are not obliged to put in place prevention, detection and response measures.

Section 3: Overarching principles-based obligations

Question 15: Are there additional overarching obligations the Government should consider for the Framework?

NAB recommends the inclusion of ecosystem-wide obligations with respect to customers experiencing vulnerability. Customers experiencing vulnerability should be given extra care and support beyond the proposed obligations. If this is not included as a system-wide obligation, then supporting vulnerable customers should be an obligation in both the initial telecommunications and digital communication platform sector requirements to align with the proposed banking obligations.

There are a number of additional obligations NAB believes the Government should consider for the Framework. Those proposed obligations are listed below:

Designated sectors

How designated sectors will be expected to collaborate on prevention, detection and response initiatives should be included as an overarching obligation.

Government, regulators and consumers

Further clarity would also be welcome on obligations and responsibilities of the Government, regulators and consumers. While designated sectors will strive for compliance with the Framework, it will be ineffective if legislation and regulation do not effectively address or keep pace with the fast-evolving changes in the scams ecosystem; or if regulators do not adequately manage and enforce the Framework. Similarly, there should be consideration of the level of responsibility expected of consumers to minimise the risk of scams (for example, to take reasonable measures to protect themselves). The Government (in addition to designated sectors) will continue to have an important role to play in educating Australians to recognise and report scams.

Question 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?

An overarching consideration for Government as it considers feedback on the proposed Framework will be how to strike the right balance between specificity and ensuring there is adequate flexibility for businesses to adjust focus areas based on assessment of risk.

NAB would welcome further specificity on timeframes, particularly with respect to proposed ecosystem-wide obligations on detection, disruption, and reporting as outlined in the Consultation Paper.

It would also be useful to understand the point at which liability to reimburse a customer is determined, how/by who that is initiated, and which obligations are applicable to the consideration of liability for an individual customer. Currently banks would not be able to compel other entities involved in a scam event (e.g. businesses in other designated sectors) to disclose how they met their obligations to the 'NAB' customer with respect to their scam losses.

Other points for consideration in the drafting of the overarching obligations include:

- Reasonable steps: replacing instances of "all reasonable steps" with "reasonable steps". Current drafting could make it difficult for the regulators and EDR bodies to enforce, given the requirement to consider all measures.
- Prevention obligations: changing "misuse" to "use" in the prevention obligation at the second bullet point; and replacing "anti-scam systems" with "processes, systems and controls". These changes would provide further clarity.
- Detection and disruption obligations: providing greater specificity on expectations on banks with respect to the first, second and final bullet points. Regard should also be given to AML tipping off and potential defamation considerations on the fourth bullet point.
- Reporting: clearer articulation of the role the NASC is expected to play in distributing and sharing information; consideration of the role the AFCX could play along with AUSTRAC's Fintel Alliance (see response to Question 18 for further detail); clarity on the meaning of 'organised large-scale scam activity', as well as the type and format of the reporting required; and greater detail on expectations for record-keeping.

Question 17: Do the overarching obligations affect or interact with existing businesses objectives or mandates around efficient and safe provision of services to consumers?

With respect to complaints handling and dispute resolution, the Framework obligations interact with existing legislation (the *AFCA Act*) and Regulatory Guidance RG271 on internal dispute resolution. The obligations also interact with existing business objectives such as setting risk appetite, enhancing customer experience, and meeting AML/CTF obligations.

Question 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?

Yes, by utilising existing capabilities – specifically and critically the AFCX, a not for profit, independent company formed by NAB and other major banks with the support of the Commonwealth Attorney-General's Department. NAB strongly believes the Government should not seek to replicate or fundamentally alter this arrangement, which is proving effective and successful in helping members coordinate intelligence and data-sharing activities to combat scam activity. NAB would encourage the Government to consider the extent to which the AFCX could serve as the focal point for receipt and distribution of data. This could simplify the provision of legal gateways for exchanging data between businesses and could potentially support AUSTRAC to receive data directly from AFCX feeds, rather than requiring all industry participants to file Suspicious Matter Reports (SMR) for scams. See response to Question 28 for further detail on the utilisation of AFCX.

The Government should also seek to ensure the proposed reporting obligation to "*take reasonable steps to notify other businesses, the NASC and relevant regulators promptly of intelligence about suspected or identified organised large-scale scam activity as well as rapidly emerging or cross-sectoral scam activity*" does not overlap with existing SMR obligations and is enabled through data exchange gateways prescribed in legislation.

Question 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?

Businesses are at different stages of maturity in their approach to addressing scams. For some, the changes required to meet obligations under the Framework may be material. NAB needs further detail to assess the estimated regulatory cost associated with these changes.

Section 4: Anti-scam strategy obligation

Question 20: What additional resources would be required for establishing and maintaining an anti-scam strategy?

NAB currently has a bank-wide anti-scam strategy in place. This includes a Scams, Fraud and Disputes Council. NAB's detection, prevention and response to scams are reported to senior management teams through NAB's Executive Customer Committee and Board Customer

Committee. The detail of the finalised Framework will determine what may be required to ensure NAB is compliant.

NAB supports the proposal that the ACCC would review the anti-scam strategies of businesses in designated sectors. This will help achieve a level of consistency across sectors and business, both in how the strategies are constructed and ultimately how they are reported to regulators for transparency.

Question 21: Are there any other processes or reporting requirements the Government should consider?

NAB would welcome further detail on how the Government envisages the Framework interacting with the incoming Financial Accountability Regime (FAR), along with potential tranche two AML/CTF reforms, and changes from the Government's response to the Privacy Act Review Report.

NAB would also welcome further detail on how other existing strategies, initiatives or regimes would overlap with or impact other anti-scam obligations – for example Confirmation of Payee (led by Australian Payments Plus) and interplay with the ePayments Code.

Question 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?

In November, the ABA and Customer-Owned Banking Association (COBA) announced the Scam-Safe Accord, which makes public commitments about the actions every bank will take to protect customers and harden the system against scams. This is in addition to NAB's own bank-wide anti-scam strategy.

In principle, NAB supports the proposal outlined in the Consultation Paper that the parts of a business' anti-scam strategy that relate to commitments to consumers be made public. NAB also agrees that businesses should not be required to disclose details of the capabilities and techniques they use to prevent and detect scams as doing so would provide significant advantages to organised criminals. Businesses could publish their commitment to adhere to relevant codes and principles, what consumers can reasonably expect from them, what they expect or need in return from consumers, as well as the rights of the consumer. Businesses should also provide transparency on the process they apply when alerted to a scam, and how customers can access complaint handling and dispute resolution processes.

Question 23: How often should businesses be required to review their anti-scam strategies and should this be legislated?

Different businesses will have strategies that vary in complexity. NAB would recommend making the review requirement somewhat flexible and would advise against legislating a specific frequency of review. NAB believes it would be adequate to legislate that businesses in designated sectors have an anti-scam strategy in place, including an obligation for periodic reviews. More frequent reviews

may be triggered due to changes in the operational environment, or as the result of a scam risk assessment. Businesses could also attest that their strategy is current which could reduce the frequency of reviews required.

Question 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?

NAB provides this answer in specific context of financial services organisations. If a bank's anti-scam strategy is intended to operate and have similar effect to its financial crime program (which would appear to be the case), NAB believes Board and/or Executive Leadership Team oversight is appropriate, particularly given the potential penalties for non-compliance. Scam prevention, detection, disruption and response requires an enterprise-wide effort – obligations sit across multiple Banking Executive Accountability Regime (BEAR)/FAR executives with significant interdependency. Progress against NAB's anti-scam strategy and other related issues is presented to NAB's Executive Customer Committee and NAB's Board Customer Committee on a regular basis. NAB believes this level of oversight is appropriate and should be maintained.

Question 25: What level of review and engagement should regulators undertake to support businesses in creating a compliant anti-scam strategy?

Support and engagement from regulators will be important in ensuring business' anti-scam strategies are effective and meet a minimum standard. Enhanced coordination across public and private sectors will be critical, particularly via the timely analysis of information provided by reporting entities to the NASC. Regulators are well placed to play an active role, which could include:

- Outlining expectations about what, at a minimum, should be in an entity's anti-scam strategy to meet legal obligations. This could be shared with an entity informally or through a regulatory guide.
- Regular review and interrogation of business' anti-scam strategies and governance, including provision of business-specific feedback.
- Industry updates on good practice and emerging trends.
- Provision of anonymised industry-wide data.
- Public awareness activities to give confidence to consumers that their interests are being represented.

Section 5: Information sharing requirements

Question 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?

Further guidance and legal clarification would be required on the specific types and information required to be shared under additional arrangements and what entities the information would be shared with beyond what is proposed in the Consultation Paper. This guidance should be cognisant of existing laws or obligations that may currently prevent or limit the scope of information sharing

(such as components of privacy law or AML/CTF requirements in relation to 'tipping-off', see response to Question 27 below).

How an entity is expected to respond to any information or intelligence disclosed to it also warrants further consideration as the consequences could exclude an individual or business from accessing services. It could also be foreshadowed that some shared information might provide unintended commercial insight to direct competitors, depending on how it is shared.

Question 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?

Limitations

Cross and intra-industry sector sharing of scam information – and financial crime information more broadly – is inhibited by both components of the Privacy Act, which constrain the sharing of personal information, and *AML/CTF Act* provisions in relation to 'tipping-off'. These impact on the provision of information to other businesses. Without clear definitions and obligations of when sharing is required and permitted, these existing requirements mean that businesses are likely to take a conservative approach to sharing information.

Safeguards

To effectively combat scams and facilitate greater sharing of information to protect consumers, NAB urges the Government to establish a legal safe harbour to enable banks and other relevant sectors to better share information and intelligence when the purpose is to investigate, prevent or recover funds related to a suspected criminal act. The safe harbour should not apply only to scams but should provide legal protection for designated entities when the purpose of the information sharing/disclosure is to prevent, detect, investigate or respond to all relevant criminal activity.

NAB also supports the legal framework for data exchange being integrated into primary legislation. This would help provide clarity on the responsibility of and protections for participants involved in the exchange of data. For example, entities providing data through such a legal framework could be protected by a legal safe harbour against the risk of legal challenge against them for sharing the data. Further, participants accessing the data may form an independent assessment of a customer (informed by the data) rather than acting on the data alone. One model that could be considered is the legal framework introduced into the Financial Services and Markets (Amendment) Bill in Singapore. This Bill allows for information sharing relating to: i) a participant requesting information from another participant; ii) a participant proactively providing information to another; and iii) a participant placing a customer on a watchlist to alert other participants.

Question 28: What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?

NAB currently shares and monitors data from the AFCX, which is currently the primary channel to coordinate data and intelligence sharing between banks about fraud and scams. This capability is being extended via the AFCX Intel Loop, which will enable sharing with other sectors, initially telecommunications providers. Members can ingest AFCX data into their own fraud and scam platforms. For example, NAB receives information from AFCX that updates NAB's fraud prevention and detection capabilities using 'whole of industry' information providing enhanced protection for customers.

In May 2023, banks and AFCX launched the Fraud Reporting Exchange (FRX) tool which allows banks to report stolen funds and recipient accounts to each other via an online portal. This significantly reduces the delays in communication between banks and improves opportunities for freezing and recovering stolen funds for customers.

For any additional information sharing, NAB urges that the existing infrastructure, mechanisms and processes of the AFCX be leveraged (but supported by the introduction of legal gateways/safe harbour per the response to Question 27). These are already effective, world-leading and would be expensive and inefficient to replicate. As part of the recently announced Scam-Safe Accord, all ABA and COBA members will join the AFCX by the end of 2025 so its coverage will increase over time. Similarly, all ABA and COBA members will be party to the AFCX FRX by the same date.

NAB also believes that wherever possible intelligence generated in our national response to scams should be maximised within the existing national/international criminal intelligence networks (such as the Fintel Alliance), recognising the global origin and nature of the scams threat to Australians.

NAB also encourages that in the Government's response to the Privacy Act Review Report, consideration be given to using that response to a provide legal mechanism for near real time information sharing between banks.

Question 29: Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?

There can be concerns about the veracity of information shared, which may vary depending on the source entity. This could give rise to issues if a business acts on information and it result in adverse consequences for individuals. For example, a legitimate customer's bank account is frozen by a bank relying on unconfirmed or unverified third-party information which results in the customer being unable to make payments, access banking services and incurring penalties. These actions may also increase the risk of vulnerability for victims of scams who have had their accounts utilised to facilitate the movement of scam funds and had these subsequently frozen. Recipients of data would need to complete an independent investigation or risk assessment of a specific piece of data to understand the corresponding customer behaviour and activity, not rely simply on data provided through a gateway by a third party.

Another impediment could be the requirement to share intelligence or information with other businesses, industry bodies or sectors that face a lower level of regulatory or legal requirements. If there was a requirement for banks to share information with significantly less regulated entities or sectors, then an impediment could be how NAB was able to ensure that such information was used and stored appropriately.

Section 6: Consumer reports, complaints handling and dispute resolution

Question 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?

Within the existing EDR schemes, there are differences in approach between sectors, different thresholds, and also differing powers. One difference that should be considered is the basis under which each EDR scheme makes decisions. AFCA, for example, is not bound by precedent and operates on the principle of fairness. If a single EDR scheme is not adopted, then NAB would encourage guidance to be provided to existing EDR schemes operating across different sectors to ensure consistent decision making for scam-related cases.

There is also a limitation in how existing EDR schemes can make decisions in relation to scams. For example, AFCA would likely only be able to assess a case raised by a customer against NAB in a banking context. AFCA can also currently only rule on the 'sending' leg of transaction, it is not able to assess whether the incoming recipient bank has met its obligations – the scope of AFCA's powers would likely need clarification and to be extended to enable it to do so.

The legislation to establish the Code should contain a legislative review mechanism for the EDR provisions to consider if they are operating effectively and consistently across sectors. These reviews would help give entities, subject to the Framework, a better understanding of how EDR schemes are collaborating to ensure consistency of approach.

Question 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?**

In considering the appropriate approach to EDR under the Scams Code, NAB considers a strong starting point is the principles of EDR identified in the 2017 Ramsay Review of EDR schemes.[1] They were:

- Efficiency – outcomes should be provided in an efficient manner.
- Equity – complainants should be treated fairly.

[1] See 2017 Ramsay Review Final Report, pp21-22.

- Complexity – complaints resolution should have minimal complexity.
- Transparency – decisions, including reasons, and processes should be easily observable.
- Accountability – decision makers should account for their actions.
- Comparability of outcomes – both procedurally and substantively as consumers who have similar complaints receive similar outcomes, regardless of which EDR body a complaint is resolved by.
- Regulatory costs – should be minimised to ensure effective user outcomes.

NAB would welcome greater detail on how existing industry process with AFCA would interact with the proposed Code. As previously outlined, NAB believes there is merit in establishing a single EDR scheme for scam complaints. This single EDR scheme would determine if banks have complied with the Code, including the proposed Framework, with ACCC/ASIC to enforce the Framework at a systemic level.

Under this model, the single EDR scheme would be the mechanism for individual consumers to pursue complaints against banks and seek redress if they are unhappy with their outcome after undergoing an IDR process. The EDR scheme would consider the proposed Framework and a bank's anti-scam strategy to guide and inform its determinations. As AFCA currently do, the scheme should also provide reporting regarding scam complaints to both ACCC and ASIC to facilitate their monitoring of trends, issues and compliance. Similarly, as AFCA currently do, a single EDR scheme would make binding determinations requiring banks to compensate customers if appropriate.

ASIC and ACCC could use EDR-provided information to augment their own data to assess whether there are systemic or serious issues (such as non-compliance with the Framework) they need to investigate and potentially take enforcement action. This would ensure both ACCC and ASIC are focused on bank compliance with the Framework's principles and obligations rather than managing individual consumer complaints. This approach would minimise duplication of effort for banks and regulators and leverages the existing mechanisms and expertise of participants.

Question 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?

Compensation caps should be considered but may not be equal across all sectors. For example, losses incurred by one or more consumers from a single scam may be distributed across several banks.

Question 33: Does the Framework set out a clear pathway for compensation to consumers if obligations are breached by regulated businesses?

NAB believes further detail is required on approaches to reimbursing losses to customers as the Framework does not currently set out liability considerations for businesses to be guided by. The Framework is rightly targeted at prevention and minimising the harm – but more detail is required to allow banks to understand the specific obligations they must meet to be compliant with the

Framework. Clarity of these obligations will also assist consumers in navigating both IDR and EDR processes.

NAB believes further clarity is required to provide a clear pathway for compensation to consumers if obligations are breached by regulated businesses. This clarity is sought in either further consultation on the Framework, or through a separate but concurrent process to consider the apportionment of liability across sectors.

It is critical for victims of scams to have clear, readily accessible pathways to first report scam losses to their bank in a timely manner. This is separate to IDR and EDR complaint processes (and should be treated separately, similar to reports of unauthorised transactions under the ePayments Code as outlined in RG271.33d.). This ensures banks are able to respond quickly to secure funds that remain and/or are at risk and attempt to recover any funds already authorised by the customer. Timely reporting to the bank provides an opportunity to secure the customer's banking services and education to prevent further harm.

Currently where any recovery of scam funds has not been successful, it is only generally at this point that a loss has been 'realised' and 'actual' loss values would be available for further assessment by both IDR and EDR schemes for compensation to the customer.

In line with existing IDR regulations, NAB would assess liability, thereby determining compensation against the over-arching Framework as it applied to NAB and the applicable banking specific codes on a case-by-case basis for NAB customers. Banks should not then be required to assess other potential avenues for liability on behalf of or for their customer or to explore potential breaches of the code made by any other bank, business or sector contributing to the scam.

Under existing banking IDR regulations and EDR schemes, consumers can only pursue a complaint or seek compensation from their bank. They cannot pursue through existing IDR processes or EDR schemes the bank that held the account that received the scam funds.

It should also be noted that during any investigation or response to a report of a scam, NAB may identify potential breaches and welcomes further clarity on how this should be handled at any stage.

In seeking further clarity on the proposed IDR and EDR schemes, NAB is seeking to avoid both confusion or creating an overly burdensome process for both customers and entities across all sectors covered by the Code. A clear pathway for compensation to consumers is critical to the community's confidence in the Framework.

Section 7: Sector-specific codes

Question 34: Are sector-specific obligations, in addition to the overarching obligations in the CCA, appropriate to address the rising issue of scams?

Question 35: Are there additional obligations the Government should consider regarding the individual sector codes?

Question 36: Do the obligations considered for each sector reflect appropriate consistency across the scams ecosystem?

NAB supports the establishment of sector-specific codes and would suggest each code have minimum requirements across all elements of a scams framework that are not addressed by ecosystem-wide obligations. Where an obligation is already included at the ecosystem-wide level, NAB believes the sector-specific code should only include it to detail more specific requirements that would not apply universally. They should also endeavour to have comparable requirements, as differences between sector codes may be exploited by scammers and provide less protection for consumers. For example, the telecommunications sector-specific code has a requirement to provide customer education – which is already an ecosystem-wide obligation for all sectors. If possible, this hub and spoke approach to code development should be clear to consumers.

NAB also encourages the Government to consider requiring other sectors to mandatorily implement intelligence and information sharing arrangements, similar to what the banking sector has delivered via the AFCX. One way this could occur is via entities in other sectors covered by a Code becoming AFCX members (as Optus has done). Broader membership would help implement more consistent industry approaches to addressing vulnerabilities that are exploited by criminals. An example of where a lack of industry consistency is impacting consumers is the different approaches to 'alphatags'.

NAB believes obligations for non-banking sectors could be enhanced to give greater consistency across the ecosystem. For example, only banks are proposed to have obligations to identify vulnerable customers at higher risk of being targeted by scams. As previously stated, all proposed and future Codes should place similar requirements on sectors to have processes in place to identify vulnerable cohorts if this is not identified as an ecosystem wide obligation.

Some specific suggestions for the two other initial sectors are:

Telecommunications providers

Greater specificity and detail on the proactive monitoring required by telecommunications providers for scams should be included in their Code to better align with the existing practices and future Code obligations for the banking sector. Consideration should also be given to requiring telecommunications providers to block a known scam number within a fixed period of time once that number has been reported to a provider in order to align to the proposed 24-hour requirement that banks are being asked to meet (see further comments below). Similarly, consideration could

be given to obligating telecommunications providers to prevent customer accounts from being hacked, as is proposed to apply to the digital communication platforms.

Digital Communication Platforms

NAB believes digital communication platforms should have similar obligations to banks to report scams along with the proposed obligations to detect and disrupt them.

Question 37: Are the proposed obligations for the sector-specific codes set at the right level, sufficiently robust, and flexible?

Question 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?

NAB considers the approach to developing sector-specific codes is appropriate but the proposed obligations across sectors require further work to refine and clarify the requirements and address inconsistency between the sectors. As noted in NAB's response to Questions 34, 35 and 36 above, the obligations for telecommunications providers and digital communication platforms could be made more robust. More work is also required to clarify the intent and whether the proposed obligations sufficiently address the challenges posed by scams to the community. The obligations will need to continue to strike the right balance between specificity and allowing the flexibility required for businesses to adjust focus areas based on assessment of risk.

Question 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?

Across all sector codes and obligations, NAB acknowledges the criticality of timely responses to best protect consumers. For banks, this includes timeframes in responding to scams once they are reported to us by customers. For example, how quickly banks advise the recipient financial institution, how quickly the recipient institution moves to hold/restrain any available funds, how quickly and often banks communicate case progress and outcomes to customers and how quickly customers are reimbursed if a bank is liable or recovery is available. Consideration should also be given to how often banks should be required to report on their scam performance and what those reports look like – ideally this should be done at an aggregated level via AFCX.

Even given this importance, NAB considers that the proposed 24-hour hour timeline for banks to revert funds to a customer will not be feasible in many cases. NAB instead suggests that the prescribed timeframe should vary based on a number of different steps in the process across both the sending and receiving bank (which would require definition). A clear definition of what transactions were in-scope would be required as well as guidance on where the requirements would stop as, for example, there is depreciating value in continuing to report and attempt recovery on funds post movement through mule accounts.

For other sectors there should also be clear timeframes for specific actions, such as on taking down phone numbers, alphatags, scam advertisements and other malicious telecommunications methods. For telecommunications obligations, more specificity on the timeline to share information with other providers once a material case has been identified – a requirement to share 'as soon as practicable' is insufficient. For online providers, similar timeframes should apply to removing scam advertisements and other typical scam lures. There should be minimum obligations on online providers to know their advertiser before an advertisement is permitted to go live on a platform. In essence, this is a form of 'Know Your Customer' for advertisers with the intent of prevention rather than recovery. These sectors should be compelled to investigate information provided by banks and provide investigation results to banks in a timely manner.

Question 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?

There are range of changes that may be required depending on the final detail of the sector-specific code. These will likely incur additional costs and time to implement. NAB considers that the key changes would be technology enhancements, personnel requirements (such as additional staff and training), along with legal and other compliance costs. It is difficult to estimate specific costs without more detailed information on the likely principles and obligations in the Framework and implementation timeframes.

Scams are different to other fraud types in that automated capabilities that permit a customer to take action themselves (for example, credit card fraud where a bank can block a card but allow a customer to confirm the transaction is genuine and unblock their card via SMS) are not always appropriate for a scam as customers have often been socially engineered or deceived into believing what they are doing is legitimate. This means a greater level of direct contact is required in engaging with customers individually before blocking a payment or questioning an event.

If, as a result of the obligations, additional friction results in more payments and/or warnings, it is likely this will generate an increase in customer complaints where the suspicion was ultimately unfounded.

Question 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 feedback provided.

Question 42: Are there additional areas the Government should consider in ensuring appropriate interaction between the bank-specific scams code and the ePayments Code?

It is important that the Scams Code does not seek to duplicate any existing requirement. NAB urges that there be no gaps and minimal overlap between the bank specific Scams Code and the updated ePayments Code. Both Codes should be drafted or amended to create clarity on what type of events or payments they apply to so banks can comply to a similar standard, rather than one Code having

duplicative, differing or unclear requirements compared to the other. This consistency will be important for consumer protection, regulators and EDR schemes.

Section 8: Approach to oversight, enforcement and non-compliance

Question 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?

NAB encourages greater clarity on how the Framework will fit with existing regulatory obligations as these requirements could also be a source of liability for potential breaches. The most relevant existing obligations for banks are the obligation to comply with financial services laws, and the obligation to provide financial services efficiently, honestly, and fairly under s912A of the *Corporations Act*. For example, even when the new Code is in place, ASIC could potentially also bring an action against a bank under s912A alleging it has inappropriate systems and processes in place to detect and prevent scams in addition to a breach of the Code. Similarly, there are also prohibitions in the *Corporations Act* and *ASIC Act* for misleading or deceptive conduct or representations. If a bank makes representations to customers as to how it will deal with instances of suspected scams in order to adhere with the Code, and does not act in accordance with those representations, then it may face liability under those provisions. Guidance from Government on how regulators should approach this decision of enforcing a provision under the Code compared to their other obligations would be welcomed.

One challenge NAB can identify is how regulators will interact where there are multiple points of failure across the different sectors. For example, how regulators would identify the points of failure and view accountability across different sectors. NAB believes that Memorandums of Understanding (MOUs) should be utilised between the regulators in order for the regulated entities to have clarity on how the regime will be applied.

Question 44: Are there other factors the Government should consider to ensure a consistent enforcement approach?

NAB supports the legislative design intention to avoid two regulators taking simultaneous action for alleged breaches under the Framework. NAB also encourages clarification that investigations into alleged breaches under the Framework will be initiated by one regulator only.

As the Consultation Paper notes, there is a critical need for consistency in enforcement across the multi-regulator model. This is particularly important when the differing sector regulators have differing resources, powers, penalties and approaches to enforcement in their regulated sector.

As noted in NAB's response to Question 36, any inconsistencies in common requirements detailed in the sector-specific codes may provide challenges when enforced by different regulators and NAB encourages, where possible, to endeavour to have comparable requirements included at the ecosystem level.

NAB believes the ACCC, as the overarching regulator of the Framework, can help ensure consistency in applying any enforcement action under the Framework. The ACCC could provide advice to sector-specific regulators on potential penalties, informed by the actions and experience of regulators in other sectors to comparable breaches of an obligation. As more sectors are added to the Framework and required to adhere to a Code, additional regulators may be brought into the fold, which increases the enforcement complexity and makes the role of the ACCC even more important.

Question 45: Should the penalties for breaches of sector-specific codes, which sit in their respective sector legislation, be equal across all sectors?

NAB encourages that penalties sit within a range for each sector. Factors to be considered when assessing a penalty should be consistent across the sectors. These factors should include the size of entity, the scale of any harm suffered, the degree of departure from the Code, adequacy of process and resources to comply with the Code, and the duration of breach.

Conclusion

Thank you for the opportunity to provide comments on the Consultation Paper. NAB reiterates that enhanced public and private sector coordination is needed to better meet the challenges of scams with sectors such as telecommunications and digital communication platforms working more closely with banks and the Government to best protect consumers. NAB believes that this can occur without imposing undue burden on any one sector or entity.

Coordination across Government will also be critically important to successfully implementing the Framework given the number of Government departments, agencies or regulators that it will interact with.

NAB looks forward to participating in further consultation on this topic in the future. NAB is more than happy to discuss any aspect of this submission with Treasury.