# SCAMS – MANDATORY INDUSTRY CODES

## SUBMISSION TO THE TREASURY

January 2024

# EXECUTIVE SUMMARY

1. We thank the Treasury (**Treasury**) for the opportunity to comment on the *Scams – Mandatory Industry Codes* consultation paper (**Paper**). We welcome the development of a whole-of-ecosystem Scams Code Framework (**Framework**) to set clear roles and responsibilities for addressing scams. To assist the Treasury to achieve its policy objectives, we have made some observations on the Paper. These comments are made within the context of our overall support for the development of the Framework.

2. Our key points for Treasury's consideration are summarised below.

    - **Exclude large businesses and institutional banking customers**

      We believe the Framework should support retail and small business banking customers as they face an increased incidence of scams.[1] There would be significant unintended consequences for our clients if larger businesses and institutional banking customers were captured. This could be mitigated by applying the Framework to retail and small business banking consumers only.

    - **Ensure clear delineation between the Framework and the ePayments Code**

      We encourage clear delineation between this Framework and the ePayments Code to help achieve timely and consistent outcomes for consumers. To achieve this, we believe scams, as defined by the Framework, should be explicitly excluded from the ePayments Code. This will make it clear which set of standards apply to specific harms.

    - **Prioritise clarity of obligations**

      We believe the principles-based obligations would benefit from further clarity to provide greater certainty for industry, limit interpretation challenges and ensure more consistent consumer experiences. To assist with this, the industry specific Codes could be used to define the overarching obligations.

    - **Streamline information sharing**

      For the benefits of information sharing to be realised, it is important reporting is streamlined and provided in an easily ingestible format.

    - **Prioritise consumer outcomes and experience**

[1] ACCC (2023), *Targeting scams: report of the ACCC on scams activity 2022*, ACCC, accessed 16 January 2024.

Clear and simple redress pathways for consumers should be prioritised when selecting an external dispute resolution (**EDR**) model. As such, we would support the establishment of a standalone scams ombudsman to provide timely and consistent outcomes for consumers and a fair allocation of liability among all participants if the Framework's obligations are not met.

3. We look forward to the next steps in Treasury's reforms and would welcome the opportunity to discuss the points in this submission if that would be useful.

# KEY POINTS

## Exclude large businesses and institutional banking customers

4. The Paper adopts a broad definition of consumer.[2] However, the Framework more appropriately addresses the circumstances of retail banking consumers and small businesses. The actions contemplated by the Framework are, in many cases, not well suited to the needs or circumstances of institutional banking customers and larger businesses (**Large Businesses**).

5. For example, adding friction by blocking or suspending payments made by Large Businesses could have adverse consequences when they anticipate that payments will be made in real time. Examples of payment types that, if blocked or suspended, could cause negative consequences for customers include: pay to employees, market infrastructure settlement payments and share trading platform payments.

6. Large Businesses are usually also better able to put in place their own systems, processes and practices which minimise the risk they will fall victim to a scam while also being tailored to their particular business environment.

7. Further, the concept of consumer used in the Paper, coupled with the application of the Framework to 'authorised deposit taking institutions' as a whole, would capture customers to which ANZ provides platform infrastructure services together with their customers.

8. For example, we provide agency representation services to other banks and non-bank financial institutions (clients) to access the payments infrastructure. Under these service arrangements, our clients provide us with instructions to carry out a transaction for their customer. ANZ acts as an intermediary to pass on payments to and from other banks and financial institutions.

---

[2] As outlined in the Paper: "*For the purposes of this paper, a consumer refers to a customer or user of a service or platform that is offered by a regulated business subject to the Framework (i.e. banking, or telecommunications service or digital platform). This could include individuals or businesses.*"

9. In these instances, it would not be clear which entity is accountable under the Framework. We believe the entity providing the service to the end consumer or account holder (e.g. the entity in contractual privity with them) should be the entity subject to the Framework obligations.

10. As ANZ is not the holder of the payer account, we lack the information to carry out all proposed obligations under the Framework. For example, we do not have the information to assess a transaction as higher risk or have the ability to identify whether the payer is a vulnerable person. The entity providing the service to the end customer is the one with the relationship and the relevant information to prevent, detect and disrupt and respond to scam activity.

11. Narrowing the scope of the Framework to retail banking consumers and small businesses should help to address these concerns. This is because the clients to whom these agency representation services are provided would be Large Businesses.

12. We note there are multiple definitions of 'small business'. Treasury may wish to consider adopting the Banking Code of Practice definition for the Framework. This may assist to ease regulatory burden as banks already have systems in place to cater for different requirements for these businesses.

## Clear delineation between the Framework and the ePayments Code

13. The broad definition of scam proposed would capture 'authorised' and some 'unauthorised' payments.[3] As a result, some activities that may fall under the ePayments Code could also be captured by the Framework.[4]

14. We do not believe restricting the definition of scams to 'authorised' payments and keeping the scope of the ePayments Code unchanged is a feasible solution. Under this approach, phishing and remote access scams that result in unauthorised transactions being made by the scammer would not be covered by the Framework but may be covered by the ePayments Code. However, remote access scams that result in the consumer being tricked by the scammer into making the payment themselves would be covered by the Framework only. This distinction:

[3] The proposed definition of a scam for the purposes of the Framework is 'a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means'.
[4] AFCA have recently, in some instances, taken the view that activities such as phishing and remote access scams could fall under the ePayments Code. For example, in AFCA determination 927566 AFCA took the view that certain digital wallet scams are captured by the ePayments Code.

- Does not reflect the evolving scams environment, where the boundary between 'authorised' and 'unauthorised' transactions is harder to distinguish
- Is more likely to lead to inconsistent outcomes for customers, given the existing technical provisions of the ePayments Code
- Would not incentivise cross sector action to stop scams that might involve 'unauthorised' activity as other sectors do not have an equivalent code.

15. The challenges created by this can be highlighted by comparing two scenarios:

    - Scenario A: A customer provided their bank or credit card details in response to an impersonation scam and the scammer used those details to make a transaction. This could be classified as an 'unauthorised' transaction
    - Scenario B: A customer was tricked into making a transaction themselves (e.g. transferring money to another account) by a scammer impersonating their bank. This transaction could be considered an 'authorised' transaction.

    Currently, the proposed definition of scam in the Framework would capture both scenarios. In addition, Scenario A may also be captured by the ePayments Code. If the definition of scam were restricted to 'authorised' transactions, Scenario A would be excluded from the Framework (but could still be captured by the ePayments Code). This could lead to the same type of scam leading to different outcomes for the consumer. It would also mean that other sectors in the scams ecosystem would not be obligated to prevent, detect and disrupt or respond to scams leading to 'unauthorised' transactions (Scenario A).

16. To ensure only one code applies to scam activity, Treasury should explicitly exclude scams, as defined in the Framework, from the ePayments Code (including those leading to unauthorised transactions).

17. We believe clarifying that all scam activity is excluded from the ePayments Code would derive the best outcome for consumers. This approach would likely lead to greater consistency of consumer outcomes, greater alignment across all sectors of the ecosystem and greater coverage of the Framework.

## Prioritise clarity of obligations

### Clear and enforceable obligations

18. To balance the utility of principles-based obligations in accommodating differences in regulated businesses and changes in the operating environment with the need for clear and enforceable obligations, we believe the industry specific Codes could be used to define the overarching obligations.

19. For example, the proposed obligation to provide consumers or users tools to verify information in real time lacks the specificity that would assist banks to take appropriate and consistent action. If the legislation specifies that the industry specific Codes define how the obligations are to be met, this could enable the Code to provide this clarity, whilst also retaining the flexibility to amend Code obligations over time as appropriate.

## Streamline information sharing

20. Based on ANZ's experience to date in information sharing to identify, prevent and respond to scams, we believe that it is critical that information:

    - Can be exchanged via a central platform
    - Is verified and actionable
    - Is provided in a prescribed format to ensure it is easily ingestible.

21. This would enable businesses to share, ingest and act on intelligence with greater speed. We would note that these requirements are yet to be specified within the Framework and would encourage Treasury to consider what they should be.

22. We support leveraging the Australian Financial Crimes Exchange to streamline information sharing, ahead of the National Anti-Scams Centre building its data-sharing capability.

23. Currently, banks share certain scam information with AUSTRAC. When a suspicious matter report is submitted to AUSTRAC, AUSTRAC is responsible for disseminating the information to other law enforcement agencies. This approach assists in managing tipping off risks: Banks are prohibited from disclosing the suspicious matter report to others, subject to limited exceptions.

24. The proposed reporting obligations risk forcing entities to breach their tipping off obligations, particularly when sharing information with other businesses.

25. It may be appropriate for Treasury to consider a new exception to the tipping off provisions to allow the contemplated information sharing.

## Prioritise consumer outcomes and experience

26. The Paper notes that under the Framework there would be clear redress pathways for consumers.

27. We believe this would be best achieved through a standalone scams EDR scheme as opposed to relying on the existing EDR schemes which do not have the ability to share information or consider the role of entities from more than one sector and have inconsistent scope, time limits and monetary compensation caps.

28. From a consumer perspective, a standalone scam ombudsman would:

- Provide a clear redress pathway for consumers, without the need to refer a consumer to a different scheme to have the role of each industry participant considered
- Improve timeliness of outcomes
- Ensure specialised and consistent interpretation of the Framework which would otherwise likely be challenging to achieve given principles-based obligations
- Ensure all industries in the scams ecosystem are held accountable if they fail to meet their obligations under the Framework. This would ensure all industries are incentivised to develop innovative and effective measures to combat scams which is critical to ensuring a reduction in the overall incidence of scams targeting Australians.

**ENDS**