29 January 2024
Scams Taskforce
Market Conduct and Digital Division
Treasury
Langton Cres
Parkes ACT 2600

Via email: scamspolicy@treasury.gov.au

Bendigo and Adelaide Bank Submission into the Scams – Mandatory Industry Codes Consultation

Thank you for the opportunity to provide a submission into Treasury's consultation into the mandatory industry code on scams (the Framework).

Bendigo and Adelaide Bank's vision is to be Australia's bank of choice, driven by our purpose to feed into the prosperity of our customers and communities, not off it. This purpose underpins everything we stand for and the action we take. We believe our success is driven by helping our customers, and the communities in which they operate, to be successful.

Our Bank is proudly digital by design, but human when it matters. We have a long and strong record of innovation, agility and delivering customer-led solutions, with the trust of our customers at the core of our business. We take cyber security very seriously and use a combination of standard industry practices to protect our more than 2.3 million customers and safeguard our systems. Our Bank has tightened transaction rules blocking high-risk payments to cryptocurrency platforms, removed all links from SMS messages and significantly increased the size of its fraud prevention and response team. In the past financial year, we stopped $38.6 million in fraudulent transactions or around $105,000 per day.

Our workforce of around 8,000 people across Australia actively encourages customer vigilance, while our fraud specialists work closely with Australian cybersecurity agencies, intelligence, and technology partners to detect and respond to malicious or abnormal behaviour.

We play an active role in educating the communities in which we operate in and support programs that uplift digital literacy, as well as targeted media and advocacy campaigns to ensure our customers are aware and able to protect themselves. We also provide regular alerts about current scams targeting customers. By working together with our customers, we can further reduce the incidence of scams and fraud. We are proactively helping customers to better understand and enhance personal security measures and digital literacy.

Registered head office
The Bendigo Centre
Bendigo VIC Australia 3550
Telephone: 1300 236 344
+61 3 5445 0666 (overseas)
www.bendigobank.com.au

Bendigo and Adelaide Bank Limited
ABN 11 068 049 178
AFSL 237879

In 2023, our Bank also launched a face-to-face education approach to help our customers safely navigate digital banking. Through our new Banking Safely Online sessions, we are enabling one-on-one connections between our Bank and our customers to help grow digital capability, confidence, and security. Designed to be delivered by our experienced employees at any of our 430 locations nation-wide, with over 1,000 participants so far, customers and local community groups can enquire about a Banking Safely Online session at their local branch.

Further to this, we are a signatory to the Scam Safe Accord and actively work with industry and government to foster a collective effort that builds a strong ecosystem approach to intercepting and preventing scams. However, we cannot do this alone. Cyber fraud is a complex, growing, and ongoing challenge that will require considerable and collaborative effort from government, regulators, law enforcement, industry, and consumers to combat this organised criminal activity. Our Bank welcomes the scam mandatory industry code framework as another step closer to addressing this concerning trend.

Yours sincerely

Richard Fennell
Chief Customer Officer

Contents

1. Introduction

Bendigo Bank supports calls for a comprehensive and consistent whole-of-ecoystem approach to addressing scams. Urgent and effective action is required to tackle fraud, and provide incentives to better protect customers across the whole system.

As one of Australia's largest non-major banks, we take our role in keeping customers safe against cyber criminals extremely seriously. Bendigo Bank continues to invest heavily into scam prevention and cyber security measures. Our priority is investing in fraud detection technology, while uplifting customer education on scams. As a result of these proactive interventions, Bendigo Bank has stopped $38.6 in scam transactions to date.

We welcome the government's proactive, whole-of-government action on scams and its focus on keeping Australians safe online. We encourage a continuation of the open dialogue with industry. Whilst we know that the sector still has further work to do, we also know that scam attemps are often due to lack of incentives outside of the banking system and poor collaboration between sectors. The whole-of-ecosystem approach outlined in the consultation document will work to strengthen other sectors' responses and create a stronger, united front against criminals.

2. Definitions

Our Bank agrees with the proposal to include a new definition for scams, separate to fraud. However, we consider that it could be strengthened by including the word 'threat' into the scam definition. In our experience, threats are prevalent in impersonation scams and extortion, implying harm as a consequence, unlike an innocuous 'request'.

Further, we consider that the overall application of this definition by industry should be extended to the precursive or successive instruments to facilitating a scam, such as products and services used across all sectors to facilitate scam activity. This includes social media, cryptocurrency and muling accounts, as some examples. Further consultation should be had to ensure that this does not overlap with obligations in the ePayments code.

Building flexibility into the Framework is crucial to maximise durability. This can be achieved through embedding definitions of specific sectors into industry-specific codes, not primary law. This will allow them to be adapted to capture the changing nature of the scam and financial crime environment and ensures the codes continue to effectively capture the intended businesses in each sector, including businesses that enter a sector in future, but due to its non-traditional model, do not fall within the sector definition.

3. Role of regulators

Regulators are integral to the success of the Framework. The consultation document discusses an 'ecosystem' approach, while simultaneously siloing sectors through separate codes and regulators. The interconnectedness of these sectors needs to be

acknowledged and, more importantly, reflected in the draft codes and the overarching legislation.

To achieve this, a single regulator should have oversight of the Framework with the ability to enforce compliance of the Framework and the sector-specific codes, instead of the proposed multi-regulator approach. This regulator can apply a cross-sector lens to review the conduct of sectors through assessing adherence to the Framework, and if necessary, use its powers for enforcement. These broad powers should extend to the use of issuing enforceable undertakings and civil penalties to specific businesses for gross and systemic non-compliance. This is essential in establishing a fair distribution of accountability and action.

Similarly, consistency across sectors in response to non-compliance including reporting requirements and penalties is important to ensure all parties in the ecosystem respond and adapt effectively. For example, where one sector has a higher number of scam incidences, there should be the ability to initiate a review to identify the weaknesses of the sector and have the power to either uplift the existing code or ensure it is better enforced.

Moreover, educating consumers on how to better identify and respond to a scam will reduce the amount of scam incidents. Our Bank takes our responsibility of educating our customers extremely seriously. In September 2023, our Bank launched a face-to-face education approach to help customers safely navigate digital banking. Through our new Banking Safely Online sessions, of which we've delivered more than 103 across the country in just four months, we enable a 30-minute one-on-one connection between our Bank and our customers to help grow digital capability, confidence, and security. While, industry campaigns have been successful, scaling up these initiatives in collaboration with government would significantly lift digital literacy levels.

4. Cross-sector information sharing

Facilitating seamless information sharing between various sectors is paramount in fostering a secure online environment for consumers. Collaboration across the scams ecosystem enables a more comprehensive and dynamic approach to online safety by enhancing the collective ability to detect, prevent, and respond to cyber risks bolstering consumer confidence and trust.

The consultation document notes existing industry initiatives, such as the Australian Financial Crimes Exchange (AFCX), which have been successful in facilitating co-operation across the sectors. To promote co-operation in the Framework, we encourage a consistent approach to information sharing through using a centralised system, such as the AFCX. Alongside this, consideration should be given to best practice approaches to monitoring, storing, and sharing data to ensure that it remains accurate, structured, available and secure as well as centralised into government.

5. External Dispute Resolution

We note the consultation paper does not include any compensation considerations. In the absence of a cross-sector compensation in the consultation document, there must be careful consideration around the amendment of external dispute resolution requirements to ensure there is acknowledgement of the intersection and interplay between multiple sectors on scam activity, and what this might mean for enforcement.

For example, under the current regime, when considering a customer complaint, the Australian Financial Complaints Authority (AFCA) can look at the complainant's actions and the sending bank's behaviour. This limited jurisdiction does not enable AFCA to consider actions of the receiving bank, the bank's adherence to the anti-scam strategy, or any other sector, such as telecommunications or social media company that contributed to the scam activity. Further, findings will not be enforceable to any business which is not an APRA-regulated entity.

Therefore, it is important that any external dispute resolution can review the scam activity across the end-to-end ecosystem and attribute customer reimbursement appropriately. First and foremost, we encourage the government to consider establishing a new central ombudsman with the capacity and expertise to manage these requests. In our view, an existing regulator does not have the ability to deal with these kinds of requests due to the complexity in attributing blame across sectors.

In this way, additional powers for AFCA and other regulators, such as the Telecommunications Industry Ombudsman, to enforce the central ombudsman's findings on scam complaints is necessary.

6. Anti-Scam Strategy

Our Bank welcomes the proposed addition of an anti-scam strategy (the strategy). The strategy will be useful to ensure an ongoing and concerted effort by businesses to prevent the misuse of their products by scammers.

Regulatory guidance on the requirements of the strategy is necessary to provide support to businesses in drafting their strategy and will help boost compliance by providing a clear and consistent approach. Guidance may be through publishing a minimum requirements list or a proposed structure of a strategy by the regulator with oversight of the Framework. The AML/CTF Program requirements, which includes a guide and checklist for implementing an AML/CTF program, is a good example of a successful industry template.

Flexibility of a business' strategy is required to accommodate a dynamic threat environment and organisational prioritisation. Therefore, while the central regulator should be able to review each business' anti-scam strategy, approval should not be a requirement for the development, or to changes, of the strategy (unless required due to systemic non-compliance with the Framework). An approval process would be time-consuming and create unnecessary barriers that lower a business' ability to be agile in adapting and responding to threats.

Similarly, we do not suggest that reviews should be explicitly regulated. Instead, guidelines by the central regulator should encourage a three-year review cycle to ensure that organisations are regularly revisiting their strategy.

Furthermore, we caution against mandatory publication, even of certain parts, of the strategy. It is not common to publish security measures as it creates a roadmap for criminals to navigate around defences. Instead, individual businesses should be able to determine which parts are made public to provide reassurance for customers of measures that are in place at a high level, such as the publication of the complaints handling and dispute resolution components of the strategy.

7. Mandatory Banking Sector Scam Code

The banking sector has been active in establishing a strong industry protection for consumers through the Scams Accord initiative. The Scams Accord initiative commits the sector to obligations that seek to balance consumer protections with disincentivising consumers to make high-risk transactions. The proposed obligations under the proposed mandatory banking sector scam code (Banking Code) go some way in embedding these obligations, however, small amendments can be made to strengthen the effectiveness of the code.

We appreciate the sentiment behind the additional safeguard for vulnerable customers; that it attempts to ensure a higher level of care is afforded to this cohort in the Banking Code. However, we query the additional benefit derived from this obligation, as banks already have numerous and sufficient safeguards in place through the Australian Banking Association's Banking Code of Conduct and other industry initiatives to identify and protect these cohorts.

Additionally, the proposed obligation in the Banking Code to trace and recover funds within 24 hours of receiving a recall request may be difficult to achieve - even with streamlined processes and automation opportunities for banks. Due to the varied and inconsistent nature of recovery submissions, investigation complexity, scenarios, customer contact, agreement on reimbursement, downstream fund recoveries and financial institution response times, recovery times can vary. Instead, we consider a broader obligation to respond to customers and begin the tracing and recovery of funds within a timely manner would help to meet the intended outcome of the obligation, whilst giving more weight to these outside factors.

Further, caution should be exercised when mandating banking friction mechanisms that limit or restrict customer autonomy without clearly articulated guidelines. While these are appropriate in some circumstances, if the mechanism is not considerately applied, it can create unintended consequences for customers. Customers are already empowered to freeze transactions on their debit or credit card, and banks that observe suspicious activity can also intervene and place stops on accounts. In implementing this requirement, the phrasing should be broad enough to ensure that banks can still override and maintain existing account holds and blocks without these being removed.

8. Sector-specific codes

Cyber criminals are innovative and will respond to obstacles placed by governments, businesses and law enforcement alike. According to the Australian Competition and Consumer Commission (ACCC), romance and investment scams account for more than 70 percent of all scams reported to ScamWatch. These types of scams are made possible due to scammers' ability to create fake social media accounts and use social engineering techniques to target scam victims. This becomes easier through the rise of artificial intelligence and language models, such as ChatGPT and other applications that can quickly provide context and imagery that reflect the scammer's purported identity. The cost of these scams are devastating for the victims and customers usually turn to banks to attempt to recoup lost funds without contacting the digital platform or telecommunication provider that facilitated the scam.

Our Bank takes this responsibility seriously and has put steps in place, including payment delays to high-risk third parties, to assist customers before these payments go through to scammers. However, we would like to see strict requirements placed on digital platform providers to curb the ability to create fake social media accounts, especially where these fake social media accounts impersonate real people, including celebrities and trusted public figures.

We also consider telecommunication provider codes should be uplifted to a minimum standard outlined in the Framework. More attention needs to be applied to encourage the sharing of information between telecommunications providers and other parts of the scams ecosystem.

9. Other sectors to be brought into the Framework

We strongly encourage a number of other sectors to be included in the Framework.

In FY23, AFCA recived a record number of scam complaints, with over 800 of them payment scams complaints, and reports that payment and credit card scams are a growing area of concern. The Framework should be extended to payment providers to ensure stronger customer protections and enable greater cross-sector collaboration in addressing scams. The financial services sector is highly interconnected and therefore, the inclusion of payment providers ensures adequate product design, implementation and scam prevention measures. Further, as noted in the consultation document, the ePayments code is not sufficient to deal with scams and fraudulent transactions, therefore, there is merit in extending the Framework to ensure consistency in application across sectors.

We encourage the government to consider broadening the definition of "Digital Communication Platform" to include search engines, Virtual Personal Network (VPN) providers and Internet Service Providers (ISPs). According to the ACCC, Australians lose around $1.5bn to investment scams each year. While, work has been done alongside ISPs and search engines in the National Anti-Scam Centre, we consider more can be done to strenghten consumer protections in this space.

Obligations for identity verification when setting up a website, taking down illegitimate websites promptly and sharing information between sectors would help to prevent scam websites from being created. Meta, for example, requires identity verification for any advertisement placed by companies on its platform. However, this is not a requirement for setting up a website or an davert. We consider that extending the obligations to these businesses would go a long way in curbing the instances of scams on these platforms.

Alongside this, we raise serious concerns about omitting crypto-currency platforms from the Framework. Cryptocurrency platforms are a common destination for scammed funds and in some cases the current framework lacks the acknowledgment and accountability of these platforms. We strongly encourage the government to consider extending the Framework obligations to cryptocurrency platforms.

10. Other considerations

The consultation paper suggests the Framework will include obligations for the sharing of information between providers within, and across, sectors. Exemptions to the Privacy Act and anti-competitive legislation should be considered in this consultation, as these would ordinarily prohibit the sharing of personal information.

Further, to ensure the regulation can keep pace with the changes in scam activity and behaviour, we expect the Framework to include a review provision for the central regulator to assess the effectiveness of codes, as well as the overarching framework. This would include conducting risk assessments and broad consultation with industry stakeholders and consumer advocacy groups as well as cybersecurity experts.

11. Conclusion

A strong scams framework will provide greater protection to consumers. As a bank, we understand the important role we play within the scams ecosystem and take this duty very seriously. Sufficient regulatory oversight and consistency in application of the law is important to ensure the success of the Framework. We urge the government to consider a broader range of sectors to include in the initial framework, including payment providers and cryptocurrency platforms, as they are important players within the scams ecosystem.

12. Summary of recommendations

Recommendation 1: Include the word ‘threat’ alongside ‘dishonest invitation, request, notification, or offer’ to appropriately cover the types of conduct that scammers engage in.

Recommendation 2: Overall application of this definition by industry should be extended to the precursive or successive instruments to facilitating a scam, such as products and services used across all sectors to facilitate scam activity. Consideration to ensure it does not overlap with the ePayments code.

Recommendation 3: Definitions of specific sectors into industry-specific codes, not primary law.

Recommendation 4. A central regulator should be appointed to have oversight of the scams framework, instead of a multi-regulator approach. This regulator should have broad powers, including investigation and review powers, enforceable undertakings and civil penalties to specific businesses for gross and systemic non-compliance.

Recommendation 5. Through the Budget, funding should be considered for a consumer education campaign by the government in collaboration with industry.

Recommendation 6. The AFCX should be used to facilitate centralised cross-sector information-sharing.

Recommendation 7. Consideration should be given to best practice approaches to monitoring, storing and sharing data to ensure that it remains accurate, structured, available and secure as well as centralised.

Recommendation 8. Careful consideration around amending external dispute resolution requirements**.**

Recommendation 9. Establishment of a centralised ombudsman that has the capability and capacity to adjudicate customer scam complaints and have ability to apportion fault across the scams ecosystem.

Recommendation 10. Powers to other regulatory bodies to enforce a central ombudsman findings.

Recommendation 11. Publication of a list of minimum requirements and a proposed structure of an anti-scam strategy.

Recommendation 12. Approval by a central regulator should not be required for the anti-scam strategy.

Recommendation 13. No obligation for mandatory publication of an individual company’s anti-scam strategy.

Recommendation 14. No specific inclusion of vulnerable customers into the Banking Code.

Recommendation 15. Broad obligation to respond to customers and begin trace and recovery within a timely manner.

Recommendation 16. Consideration to be given to the specificity and flow on impacts of the inclusion of mandated banking friction.

Recommendation 17. Strict requirements placed on digital platform providers to curb the ability to create fake social media accounts and advertising.

Recommendation 18. Uplift of the telecommunication code to encourage the sharing of information between telecommunication providers and other parts of the scams ecosystem.

Recommendation 19. Broaden the definition of “Digital Communication Platform” to include search engines, Virtual Personal Network (VPN) providers and Internet Service Providers (ISPs).

Recommendation 20. The Framework should be extended to payment providers, to ensure stronger customer protections and enable greater cross-sector collaboration in addressing scams.

Recommendation 21. We strongly encourage the government to consider extending the scam framework obligations to cryptocurrency platforms.

Recommendation 22. Consideration of exemptions to the Privacy Act and anti-competitive legislation.

Recommendation 23. Legislated review by the central regulator to assess the effectiveness of codes, as well as the overarching framework.

.

-