

Scams Taskforce
Market Conduct Division
Treasury
1 Langton Crescent
PARKES ACT 2600

Via email: scampolicy@treasury.gov.au

Scams Prevention Framework – exposure draft legislation

Thank you for the opportunity to provide a submission into Treasury's consultation on the Treasury Laws Amendment Bill 2024: Scams Prevention Framework.

Bendigo and Adelaide Bank is one of Australia's largest banks with more than 2.6 million customers and is Australia's most trusted bank. We are an ASX100 listed company, with assets under management of more than \$90 billion and a market capitalisation of approximately \$7 billion.

We have a long and strong history of innovation, agility and delivering customer-led solutions, with the trust of our customers and communities at the core of our business. Our Bank uses a combination of standard industry practices and innovative technology solutions to protect our customers and safeguard our systems. In the past financial year, the Bank stopped \$34.4 million in fraudulent transactions.

Our workforce of around 8,000 people actively encourages customer vigilance, while our fraud specialists work closely with Australian cybersecurity agencies, intelligence, and technology partners to detect, report and respond to malicious or abnormal behaviour. We continue to work hard to proactively detect and prevent the unauthorised use of customer accounts.

We play an active role in educating our customers and the communities in which we operate, with programs to support and 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 so they can stay alert and vigilant. We are proactively helping customers better understand how to enhance personal security measures with the aim to equip them with a higher level of digital literacy.

In 2023, our Bank also launched a proactive education program to help our customers safely navigate digital banking. Through our new Banking Safely Online sessions, we are facilitating face-to-face connections between our Bank and our customers to help enable growth in digital

capability, confidence, and security. Since its launch, we have run more than 200 sessions at over 430 locations nation-wide, with more than 1,000 participants so far. Our local branches also give the opportunity for customers and local community groups to join a Banking Safely Online session closest to them.

Further, we are a signatory to the Scam-Safe Accord and actively work with industry partners and government agencies to foster a collective and collaborative effort to build a strong, whole-of-ecosystem approach to intercepting and preventing scams.

We welcome the Government's whole-of-ecosystem approach through the mandatory Scams Prevention Framework.

Introduction

Bendigo and Adelaide Bank (Bank) continues to invest heavily in scam prevention, reporting and response management, cyber security measures and fraud and scams detection technology. We are also actively uplifting our customers' and community's awareness and education on scams. In doing so, we have:

- established a fraud management framework and an anti-scams strategy
- enabled customers to use facial and/or fingerprint recognition and multi-factor authentication to verify digital banking login credentials
- tightened transaction rules blocking high-risk payments to cryptocurrency platforms
- removed all unexpected links from SMS messages
- increased the size of our financial crime risk team
- participated in a pilot of Commonwealth Bank's confirmation of payee solution, Namecheck, which has prevented more than 61,000 mistaken or scam payments worth more than \$26 million for our customers since February 2024
- participated in the AFCX and FRX and were part of the first National Anti-Scam Centre investment scam fusion cell on investment scams
- provided regular alerts about current scams, including bank impersonation scams, targeting customers and we maintain a webpage with information for customers on how to keep their details safe on our website
- launched our face-to-face Banking Safely Online sessions. More than 200 sessions have been delivered to more than 1,000 community members.

As a result of these proactive interventions, we have seen a downward trend of scam transactions. In the financial year ending June 2024, our Bank prevented \$34.4 million in fraudulent transactions.

Our Bank welcomes the new Scams Protection Framework (SPF) regulation and support the principles-based obligations, the whole-of-ecosystem approach to combatting scams and the intention to designate a single external dispute resolution scheme for scams. We encourage a continuation of the open dialogue with industry through the implementation of the SPF.

Key recommendations

1. Ensure reporting requirements align and strengthen other existing reporting channels

The Treasury Laws Amendment Bill 2024: Scams Prevention Framework (the Bill) outlines reporting requirements for regulated entities to the SPF Regulator and/or the SPF Code Regulator regarding specific scam incidences.¹

The banking sector, through its current industry-led scams framework and existing legislative obligations, has reporting channels for these scam incidences. For example, the Bank has industry reporting mechanisms in place to share information and reach an effective resolution quickly. This includes reporting to the Fraud Reporting Exchange (FRX) by the Australian Financial Crimes Exchange (AFCX), it also allows for shared intelligence and secure

¹ See sections 58BH, 58BR, 58BS etc.

communications between banks with agreed timeframes, reducing the need for multiple phone calls and emails. Our Bank considers these existing channels to be working well.

Additionally, the definition of scam in the Bill overlaps with the fraud definition contained in the *Anti-Money Laundering and Counter-Terrorism Rules Instrument 2007 (No. 1)* (AML/CTF Rules) alongside reporting and information disclosure under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act). Therefore, the reporting requirements for scams could replicate and overlap with existing and well-established reporting to the Australian Reporting and Transaction Analysis Centre (AUSTRAC), namely; Suspicious Matter Reports (SMR) scenarios for suspected fraudulent transactions. The AML/CTF Act also precludes the sharing and disclosure of such information of parties which have been reported in an SMR outside of the parties mentioned in Section 123 of the AML/CTF (the 'Tipping Off' provision) with strict exemptions which would not include providing this information to the ACCC unless, for example, ordered by a court of law or under the amended provision in the AML/CTF Reform Bill, should the ACCC's National Anti-Scam Centre be classified as law enforcement for these purposes. The overlap of these reporting requirements would mean each individual case would have double the reporting obligations to different regulators.

Our Bank, along with other banks of our size, have finite resources and need to prioritise these resources strategically to ensure they are being used most effectively. These resources are best focussed on protecting our customers by monitoring and responding to scam activity.

We consider these increased, and in some cases overlapping, reporting requirements may have little impact on reducing scams, and instead place resource strain on both the regulated entities as well as the regulators in managing the influx of reports. For example, we consider due to the broad definition of 'actionable scam intelligence' where the Bank has received information (such as someone moving money overseas) but has not verified the information or formed reasonable suspicion, it will need to report to the regulator. This amount of information could overwhelm the regulator, limiting the effectiveness of the information, and pull resources from internal fraud departments.

Instead, Treasury should consider using the existing regulatory reporting channels to capture this reporting information, and where possible, utilise existing regulator information sharing provisions, to minimise the amount of duplication required by regulated entities. This includes an additional provision to state when information has already been provided to one regulator, it does not need to be provided to another.

Bendigo and Adelaide Bank recommendation:

- The Framework should allow greater flexibility for regulators to utilise the existing regulator and industry reporting channels to capture this reporting information, such as, where possible, utilise existing regulator information sharing provisions, to minimise the amount of duplication required by regulated entities.
- The addition of a provision to state when information has already been provided to one regulator, it does not need to be provided to another.

2. Clarify the role of the ACCC in targeting significant, egregious breaches of the Framework

The Bill outlines a tiered approach to the civil penalty amounts. These amounts can be upwards of \$50 million (currently the penalty units stipulated in the Bill would result in a pecuniary amount of \$50,000,186). The Bill outlines the Australian Competition and Customer Commission (ACCC) will have supervision of regulated entities' conduct under the SPF.

The ACCC currently has a strong role in monitoring and taking enforcement action for systemic, significant or cross-sectoral breaches of the *Competition and Customer Act 2010* (Competition and Customer Act) and may not be resourced effectively to monitor and enforce all scams reported to the agency when the framework is legislated.

In the 2024-25 Budget, the ACCC received \$37.3 million over four years from 2024–25 (and \$8.6 million per year ongoing) to administer and enforce mandatory industry codes for regulated businesses to address scams on their platforms and services, initially targeting telecommunications, banks and digital platforms services relating to social media, paid search engine advertising and direct messaging.

When this legislation is passed by the Parliament, we naturally foresee increased expectations and pressures on the ACCC to monitor and enforce the framework. We propose, with the ACCC's limited resources, including ongoing funding after four years as outlined in the 2024-25 Budget, the agency should prioritise enforcement of significant and egregious breaches of the obligations to best achieve the policy intent of the legislation. Doing so will maintain confidence in the ACCC among stakeholders subject to the framework and its associated civil penalties.

It is our Bank's view the Bill could be strengthened by including a provision reflecting the policy intent that the penalties will only be imposed for serious and egregious breaches of the principles.

Furthermore, we believe this framework carries a relatively high risk of single breaches being reported to the ACCC under the framework. Noting the subjective nature of reports to be assessed on a case-by-case basis and on their own merits, such purported breaches should not be considered indicative of the overarching conduct by an entity subject to the framework.

Within this, it is our Bank's view the high civil penalty amount does not reflect any other code-related civil penalty regimes. Instead, it reflects the penalties for egregious and serious anti-competitive conduct in Part VI of the Competition and Customer Act, which stipulates \$50 million penalties. We are concerned the penalty is too high for the offending conduct, and instead a penalty reflecting the existing industry codes in the Competition and Customer Act would be more appropriate

Bendigo and Adelaide Bank recommendation:

- Include a specific provision in the Bill that states civil penalties apply for systemic, serious or egregious conduct.
- Reflect penalties for the existing industry codes in the Competition and Consumer Act.

3. Clarify the apportionment of liability to strengthen internal dispute resolution and external dispute resolution

Division 4 of the exposure draft Bill outlines the External Dispute Resolution (EDR) authority (namely: AFCA) mechanism for the SPF. Our Bank supports the single-body EDR scheme proposed in the legislation. We consider this will lead to quicker and more effective outcomes for customers. The single-body EDR scheme will also ensure outcomes are applied consistently and more predictably across the regulated sectors, allowing all regulated entities to be held to a consistent standard, resulting in better outcomes for customers.

While our Bank acknowledges under the SPF Internal Dispute Resolution (IDR) will be the primary method for resolving customer complaints, the Bill remains silent on how liability will be apportioned across the regulated sectors and how coordination across the regulated sectors would occur. The Bill also does not allow regulated entities to add third parties into their IDR processes. The lack of these mechanisms will significantly reduce the impact of effectiveness of the IDR schemes and cause more cases to go to EDR.

FOR EXAMPLE: *A customer is a victim to a scam and initiates an IDR process with their bank. The bank undertakes an examination and finds it was an investment scam advertisement, initiated via a digital platform, which has not met its obligations under the framework.*

Under this scenario, the bank would either offer the customer compensation for the portion of compensation the bank believes it is at fault for or decline compensation if the bank has identified it has complied with all its requirements under the Code. This scenario results in potentially lengthy delays to reach an outcome due to customers either having to go through separate IDR processes, or more cases being escalated to EDR.

Guidance should be provided on liability apportionment. If this was provided, regulated entities would be able to apply this guidance in IDR processes, ensuring customers get satisfactory outcomes quickly.

We consider given the wide-spread impact of the industry, and the experience the banking sector has on implementing dispute resolution procedures, the liability apportionment should be industry-led. Where industry cannot agree within a specific period, the Minister should have the ability to override through a rule-making power.

Bendigo and Adelaide Bank recommendation:

- Replicate the industry code making powers in the *Telecommunications Act 1997*. This includes the ability to request, approve and revoke an industry-code. This would also include an additional rule-making power in Division 4 of the Bill to allow the Minister to make rules about how liability will be apportioned. It is anticipated AFCA will provide guidance on what it considers to be appropriate, fair and honest in its decisions when dealing with complaints.

Additional Recommendations

1. Commencement date for AFCA determinations

Our Bank welcomes the structure of the Bill and commencement of obligations on regulated entities to be stipulated through a Ministerial determination, rather than specified in the primary legislation. This provides flexibility and futureproofing to add further sectors as scams continue to become more complex and impact more areas of our society.

We acknowledge that the Bill remains silent as to when a customer(s) can take action for a breach of obligations under the SPF. Under the Bill, following a determination made by the Minister, regulated entities within a regulated sector must comply with the SPF obligations. Following this date, AFCA will be able to make determinations under the SPF.

It is our Bank's view in the Ministerial determination to bring a regulated entity under the SPF, it should contain a provision which allows a scam to be considered by the SPF, if the scam occurred following the date the regulated sector was designated under the SPF.

There may be instances where a scam is reported post-commencement of the Bill, but prior to the Ministerial determination. The Bill remains ambiguous as to whether scams of this nature (having occurred prior to Ministerial determination but reported post-commencement) would be within scope and subject to regulatory obligations under the SPF.

Bendigo and Adelaide Bank recommendation:

- The Bill, or the Ministerial Determination, should specify that a customer's case under the new SPF regime can only be considered in EDR if the scam occurred following the date the regulated sector was designated to be subject to the SPF. This provides greater clarity for regulated entities.

2. Definitional concerns

Scope of scam definition

The policy scope of the scam definition, as outlined by the explanatory memorandum, is to not cover unauthorised transactions, such as cyber-attacks and hacking. However, we consider that there may be instances which may fall outside the definition of the scams in the Bill but within the policy scope. One example is in respect to Remote Access Scams, whereby customers are deceived into allowing scammers to access their devices, which often contains their bank account information and can result in significant financial losses. Under this scenario, it classifies as a scam, despite the payment being unauthorised.

Bendigo and Adelaide Bank recommendation:

- Explicit clarity in the SPF Rules to ensure the SPF captures scams like Remote Access Scams and whether it relates to one scam incident or a scam typology.

3. Notification requirements to SPF customers

The Bill requires regulated entities to identify and warn high-risk SPF customers who may be subject of a particular scam. The Bill does not define higher risk customers. In practice, our Bank raises concerns that this would require categorisation and potential stereotyping of customers, and, given the broad definition of SPF customers, this also includes people who are not customers of the Bank. The practical considerations of actioning this requirement

would mean banks are, potentially, unfairly categorising people based on sensitive information (age, race, sex etc) or vulnerability. This could lead to unintended consequences of debanking of customers who are too risky, based on their history of falling for scams or potential vulnerabilities. Our Bank does not believe this is in the spirit of the Bill and suggests 'higher risk' is defined in the SPF Rules and explicitly carves-out the obligation to contact non-customers. Otherwise, every Australian is susceptible to scams and the obligation as-is could place regulated sectors at risk of breaching discrimination or privacy legislation.

Second, our Bank raises concerns about providing high-risk customers with warnings about a particular scam. We consider that there needs to be a threshold of when warnings are issued. For example, when there is a high incident rate of a successful scam or a new scam typology that has been identified, it is important that these warnings are provided to customers. But, if regulated entities are required to provide warnings when there is an isolated incident or a small number of common scams, it could dilute the impact of these warnings and cause indifference. It is our view that clarity would best in the Bill, instead of in the sector-specific codes, as to create consistency across the sectors. For example, AUSTRAC releases typologies and case studies, instead of providing detailed accounts of each type of scam. In our view, the sector-specific codes should outline that warnings should only contain information relating to the type of scam and outline educational resources. This approach would help to prevent scams without providing too much information about how they are conducted.

Third, if a customer has a relationship (indirect or direct) with multiple regulated entities across the ecosystem, it could result in multiple notifications from different regulated entities the customer conducts business with. Following this scenario, customers could be receiving an influx of information, which could limit the effectiveness of such notifications. These useful notifications can become burdensome for regulated entities and consumer alike, while the influx of information can reduce the impact of these warnings to customers. Instead, the Bill should contemplate other ways of dissipating scam information, such as through the SPF code regulators.

Bendigo and Adelaide Bank recommendation:

- Higher risk customers are defined in the SPF code for a regulated sector. This definition should be consistent across all codes.
- There is an explicit carve out to the notification requirements to contact people who are not customers of regulated entities.
- Threshold information relating to when scam warnings need to be provided to high-risk customers, also what information the warnings need to contain.

4. Interaction with existing legislation

We consider that the Bill and corresponding subordinate legislation should align terminology with existing legislation. For example, section 58AG of the Bill refers to “personal information”. For simplification and alignment with existing legislation, Treasury should amend this terminology to “personal data”. This would reflect the Privacy and Other Legislation Amendment Bill 2024 (Privacy and Other Legislation Amendment) and Australia’s alignment with terminology used in the European Union information privacy regulation General Data Protection Regulation (GDPR).

Bendigo and Adelaide Bank recommendation:

- Where possible, the Bill and corresponding subordinate legislation should align terminology with existing legislation.

Spam Act 2003

The Bill outlines that notifications need to be provided to direct customers of the regulated entity, but also to people who may be impacted, but are not direct customers of the regulated entity (an SPF customer).

Where customers have opted-out of communications from the regulated entity or a regulated entity does not have a direct relationship with the customer warning notifications could be a breach of the *Spam Act 2003* (Spam Act).

Bendigo and Adelaide Bank recommendation:

- The Bill specifies that the provision does not include contacting people who are not customers of the regulated entity. Also include, only new scam typologies are to be communicated, not each scam incident to reduce the number of notifications a customer may receive from a regulated entity.

Privacy Act 1988

Subsection 52BS(3) specifies information which regulators may require from regulated entities includes personal information, information regarding the person reasonably suspects of committing a scam and the SPF customer who was engaged as part of the scam. The personal information includes name, address, email, phone number, bank account details or credit card details. Under the current Australian Privacy Principles (APP), there is an exemption to share information relating to law enforcement investigations. We suggest that this is used and defined for the ACCC NASC.

Further, sharing this kind of information with the regulator could contravene the tipping off provisions.

Bendigo and Adelaide Bank recommendation:

- Specify that the ACCC NASC is a law enforcement agency for the purposes of the APP.
- These legislative changes should be dealt with in the Bill and not left to other ‘clean-up’ legislation which may delay effective implementation of the scheme.