Scams Prevention Framework Bill 2024

Submission to the Senate Economics Legislation Committee

Westpac Banking Corporation

9 January 2025

WE ARE GROUP

INTRODUCTION

Westpac thanks the Committee for the opportunity to provide a submission in response to the *Scams Prevention Framework* (**SPF**) *Bill* 2024. Importantly, the SPF has adopted a whole-of-ecosystem approach which is fundamental for any framework to effectively combat scams. Westpac also acknowledges the separate submission that has been made by the Australian Banking Association (**ABA**) which we have contributed to and fully endorse.

Australia is emerging as a global leader in scam prevention. Joint focus and collaboration from government, banks and telco providers brought Australian scam losses down for the first time since 2016, with data from the Australian Competition & Consumer Commission (**ACCC**) recording a 41 per cent reduction in reported losses[1]. At Westpac, investment of more than $100 million in scam prevention over the past two years has helped stop over $400 million being sent to scammers and in FY24[2] brought customer losses down by 29 per cent. New analysis[3] suggests this places Australia as one of the only countries in the western world where scam losses have reduced, not grown.

While these efforts show good progress we know there is still more to be done. Banks have successfully brought customer losses down, yet the prevalence of scams remains. Banks play an important role in stopping scams, but we cannot fight this fight alone. Scammers have no business operating in our economy and our collective goal should be nothing short of making Australia the hardest place for scams to operate in.

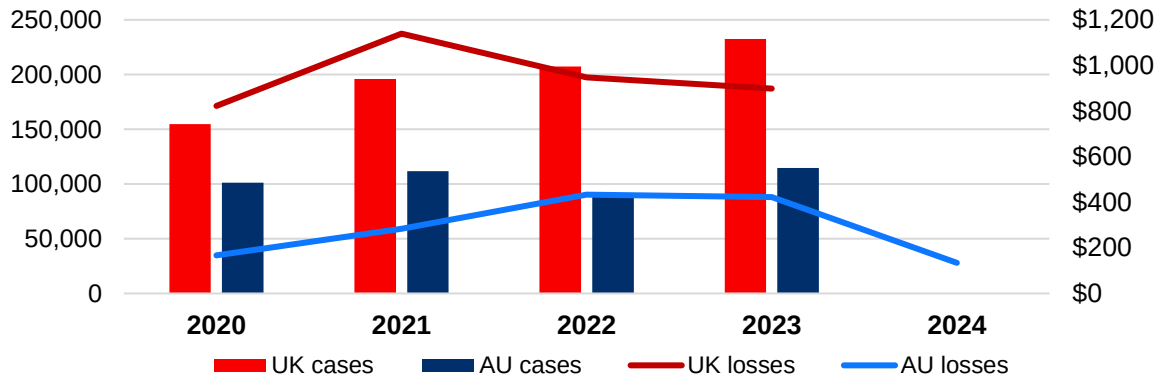
For these reasons, Westpac supports the intent of the SPF Bill and its approach to driving whole-of-ecosystem action on scams to protect Australians from this scourge. We believe this Bill is a 'national interest'-level piece of legislation and we ask the Committee to provide bipartisan support for it. We have provided some recommendations to improve elements of the Bill's application.

BDO ANALYSIS: AUSTRALIA A GLOBAL LEADER IN SCAM PREVENTION

In a comparative analysis of scam data by BDO spanning Australia, the United Kingdom (**UK**), Canada and the United States of America (**USA**), Australia is emerging as one of the most successful in reducing scams, concluding that:

- UK per capita scam losses are almost double Australian losses[4]
- Losses in the UK, USA and Canada have continued to increase since 2020, while Australian losses are down 52% in 2024[5]

Figure 1: Comparison of total scam cases and losses in Australia and the UK[6]



** Tracking YTD at time of reporting (January – June 2024)*

[1] Losses decreased from $559.9m in 2022−23 to $330m in 2023−24, National Anti-Scam Centre Quarterly Update, November 2024.
[2] Westpac FY24 period is October 2023 – September 2024.
[3] 'Scams Environment Data Analysis' Report conducted by BDO, December 2024.
[4] UK per capita reported scam losses of A$33.48 versus A$17.69 reported Australian losses in 2023.
[5] Losses decreased from $284m in 2023 to $137m in 2024 for the January – June comparable period, ACCC scam statistics.
[6] BDO 'Scams Environment Data Analysis' report, December 2024.

Further, as the effectiveness of the UK's Contingent Reimbursement Model (**CRM**)[7] has become a point of debate in Australia's policy discussions, BDO's analysis of the scheme has found that since its introduction:

- UK scam cases have grown at almost four times the rate of Australian cases with UK scam reports up by 90%; and
- the increase in UK cases and losses coincides with an increase in the reporting rate with minimal impact on losses.

The continued increase in UK scam cases suggests the scheme has failed to materially reduce the actual occurrence of scams as intended. That is, the enrichment of criminals through criminal activity simply continues. This growth in criminal enterprise is ultimately making its way to Australia's economy, with approximately 40 per cent of Westpac-detected scammers having some link to the UK.

Comparatively, Australia has been able to effectively reduce scam losses without such a scheme. In Westpac's view, the evidence shows that reimbursement schemes only serve to drive scam cases up further by encouraging scam activity and consumer complacency, so therefore should not be the focus of policy discussion.

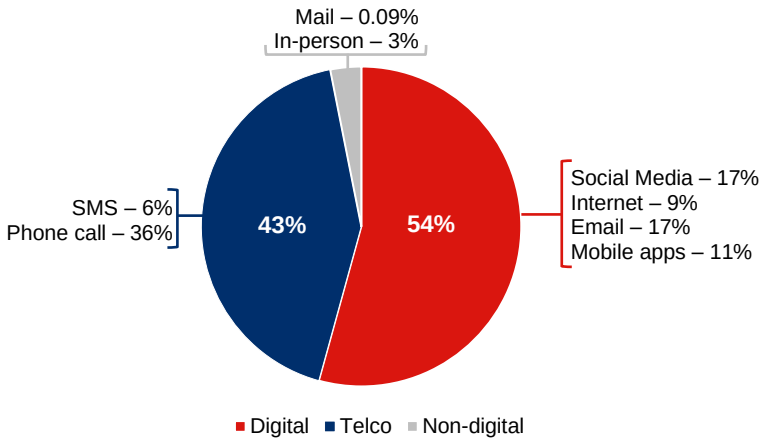
Having said the above, Westpac wants to be very clear that it strongly supports an Internal Dispute Resolution (**IDR**) mechanism that works as efficiently as possible for the benefit of consumers and meets the intention of the Bill to consider apportioned liability between the customer and regulated entities appropriately, if and/or when a regulated entity has failed to meet its Code obligations.

EQUAL ACTION FROM ALL ECOSYSTEM PARTICIPANTS IS CRITICAL

Westpac acknowledges digital and social media platforms have taken some initial steps in addressing scams, including collaboration with banks through new intelligence sharing arrangements. But the unfortunate reality is these platforms are avoiding responsibility by doing no more than the bare minimum of what their world-leading technology is capable of. The impact of applying such expertise to scam prevention could be profound.

As an example, Meta utilises some of the world's most sophisticated algorithms and AI to deliver hyper-targeted content and advertisements for specific user demographics. Yet it would only take the most basic algorithm for Meta to uncover any ads that have been purchased with credentials linked to a confirmed scam or fraud, thereby helping eradicate known scams quicker and preventing further loss.

Figure 2: Scams losses by origination channel[8]



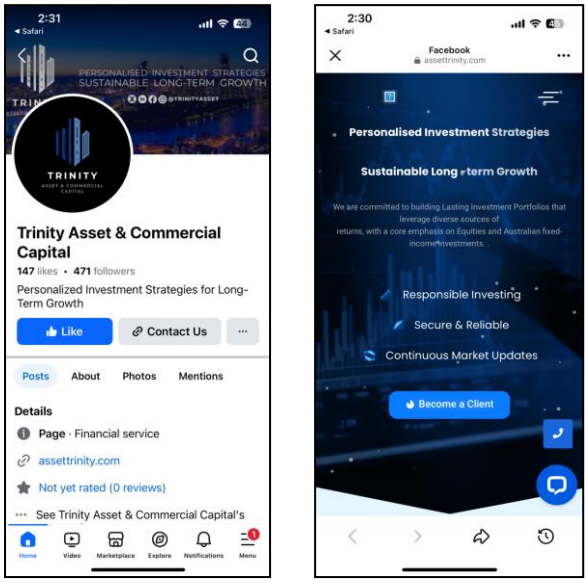
[7] The CRM was implemented in May 2019 as a voluntary Code to reduce the occurrence and impact of scams. It requires UK banks to reimburse some customers who fall victim to a scam. The scheme became mandatory in October 2024.
[8] National Anti-Scam Centre Quarterly Update, November 2024.

Scams on digital platforms are responsible for more than half of Australian scam losses (Figure 2)[9]. Furthermore, they continue to profit from these scams (via advertising revenue) all the while ignoring legitimate customer concerns when such activity is reported. Two examples of this are outlined below.

Example #1: Inaction when a scam is reported

On 2 October 2024 Westpac identified and informed Meta of a company that appeared to be a fake investment vehicle operating through a Facebook profile (Figure 3). At the time of writing this submission, approximately 14 weeks later, the profile is still live on its platform.

Figure 3: Reported scam profile that remains live on Facebook

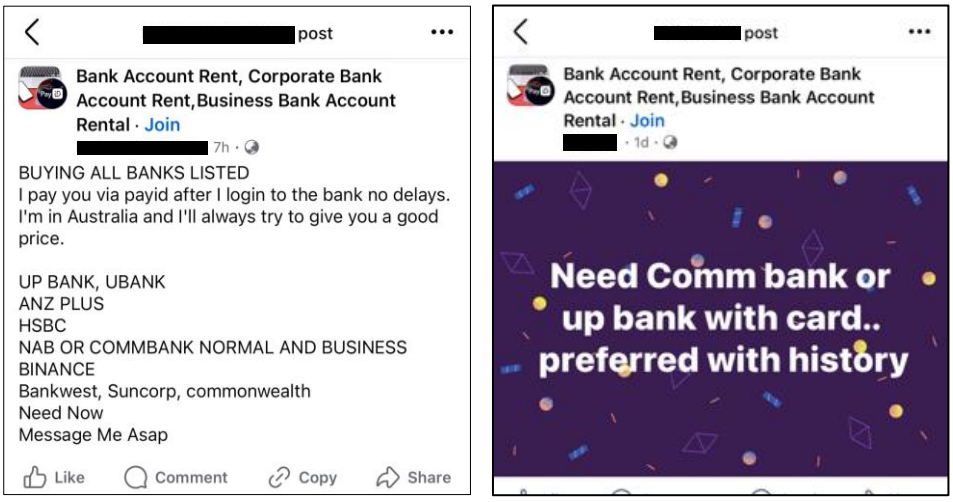


Example #2: Illegal bank account trading

Additionally, a simple search to “buy or sell bank accounts” on Facebook reveals the extent of fraudulent behaviour it allows to run rampant across its platform, with numerous community groups openly trading bank accounts for muling purposes (see Figure 4).

Considering these examples, Westpac would reinforce the important role of the SPF Bill in applying consistent and robust measures across all ecosystem participants to ensure a meaningful and effective framework that will adequately protect consumers.

Figure 4: Facebook users illegally trading bank accounts



[9] National Anti-Scam Centre Quarterly Update, November 2024.

RECOMMENDATIONS TO IMPROVE THE BILL'S APPLICATION

Westpac supports the passage of the Bill, however, also takes this opportunity to make the following four recommendations which we feel would further strengthen the Bill and its application.

Recommendation 1:

All SPF Codes should be reviewed and approved by the ACCC to ensure consistency and robustness

A whole-of-ecosystem approach, as is intended by the Bill, cannot be effective if the sector Codes don't require regulated entities across all Codes to meet the same standards.

Banks have helped establish Australia as an emerging global leader in scam prevention and one of the only jurisdictions globally to record a reduction in customer scam losses[10]. With 54 per cent of losses still originating from digital platforms[11], equal action and investment from other parts of the ecosystem are essential for stopping the occurrence of scams. To achieve the level of consumer protection the Bill seeks to deliver, it's imperative sector Codes have a consistent level of robustness.

In Westpac's view, the ACCC's cross-sector oversight and expertise developed through the establishment of the National Anti-Scam Centre (**NASC**) means it's best placed to oversee the development of sector Codes, rather than delegate this authority to SPF sector regulators which won't have the same system-wide view.

Suggested drafting is included at Appendix A.

Recommendation 2:

Clarify the scope of actionable scam intelligence, as well as what, when and how this intel should be reported

2.1 Refine actionable scam intelligence scope and reporting requirements

Westpac acknowledges the critical role of information-sharing in preventing scams. Through the Australian Financial Crimes Exchange (**AFCX**) and Fraud Reporting Exchange (**FRX**), banks have established real-time communication and data-sharing to identify and stop new scams, as well as stop and recover customer losses. Through these channels Westpac engages in over 3,000 interactions with its peers each week while our systems monitor over 30 million banking interactions each day to detect potential scams. This net is cast wide to maximise effectiveness but means not all alerted activity will be a scam.

The Bill requires entities to report and take steps in response to actionable scam intelligence. However, the proposed scope and reporting requirements in the Bill are extremely broad and would mean a significant amount of irrelevant information would need to be reported, including activity that isn't a scam. This would take considerable time and resources away from both the reporting entity and regulator that would otherwise be invested in stopping scams.

Refining the scope of actionable scam intelligence to information that will genuinely make an impact to stopping scams, as well as the subsequent reporting requirements, would help ensure a more efficient and effective approach.

Suggested drafting is included at Appendix B.

[10] BDO *'Scams Environment Data Analysis'* report, December 2024.
[11] National Anti-Scam Centre Quarterly Update, November 2024.

2.2 Scam warnings for SPF Consumers

Alerting customers to potential scams or new scam tactics is another important component of scam prevention and central to many of Westpac's own prevention features. For example, Westpac Verify alerts customers to a potential account name mismatch when a new payee is added in online or mobile banking.

Westpac acknowledges the framework's underlying intent in the Bill is to ensure all ecosystem participants are adequately alerting customers to scam activity. However, the significantly broad scope creates a risk this will generate an overwhelming volume of false positive alerts, including in instances where it may be irrelevant to customers, resulting in warning fatigue and complacency.

Additionally, there is a lack of clarity about what would constitute "reasonable steps", such as the channel, mode or frequency of such communication. While Westpac acknowledges the intent is to have this stipulated in the relevant sector Codes, we would reinforce the need for a single regulator through the ACCC to have oversight across the Codes to ensure a consistent approach is applied across sectors.

Suggested drafting is included at Appendix C.

Recommendation 3:

Extend the safe harbour for actions taken after an entity reasonably identifies activity to be a scam

The proposed safe harbour provisions in the Bill can apply where an entity has actionable scam intelligence, however this only applies where there are reasonable grounds to suspect the activity is a scam. This significantly limits the scope beyond what Westpac assumes is intended; that is, to provide safe harbour where entities are taking action to stop a scam.

Under the present drafting, safe harbour ends when an entity identifies an activity is a scam. In Westpac's view, safe harbour should be consistent with encouraging action after a scam has been identified to maximise prevention efforts and to protect customers.

In addition, the ability to apply a "reasonably proportionate" test is challenging given the need to balance obligations under similar consumer protection regimes, such as extra care requirements under the Banking Code of Practice (**BCoP**). As an example, the bank would have to consider if it is "proportionate" to block a detected mule account linked to a vulnerable customer who would subsequently be unable to receive pension payments.

Suggested drafting is included at Appendix D.

Recommendation 4:

Improve alignment between the SPF Principles and Codes and their associated penalties

As the Bill is drafted, entities can be compliant with Code obligations while concurrently in breach of the SPF Principles. This creates uncertainty, duplication and hinders the ability for entities to make investment decisions about appropriate scam prevention measures.

The Bill appropriately sets out obligations requiring entities to introduce robust systems and processes directed at combatting scams. Penalties should therefore similarly be designed to encourage the implementation and maintenance of those robust systems and processes.

Civil penalties should also reflect the materiality of any breach. As an example, Westpac has outlined the significant volume of information that's managed relating to potential scams and the speed at which banks must act to stop scam activity. This volume increases the risk of single breaches, even if the bank has implemented and maintained very robust systems and procedures

for stopping scams. It would therefore be disproportionate to expose entities to significant penalties for single isolated breaches.

Suggested drafting is included at Appendix E.

APPENDIX A

Recommendation 1:

All SPF Codes should be reviewed and approved by the ACCC to ensure consistency and robustness

SPF Codes need to be consistent and meet the same level of standard to ensure an effective whole-of-ecosystem approach to stopping scams. We think this could be achieved by amending the Minister's delegation making power in section **58CD** as follows:

The Minister may, in writing, delegate the Minister's power under section 58CB to make a code for a regulated sector to:

(a) another Minister; or

(b) the Commission; ~~or~~

~~(c) the entity that is, or is to be, the SPF sector regulator for the sector.~~

APPENDIX B

Recommendation 2:

Clarify the scope of actionable scam intelligence

Not all intelligence will be relevant or effective for stopping scams. Reporting should therefore be limited to information that will genuinely make an impact when it comes to scam prevention. To achieve this, we recommend amending section **58AI** as follows:

A regulated entity ~~identifies, or~~ has actionable scam intelligence if (and when):

(a) there are reasonable grounds for the entity to suspect that a communication, transaction or other activity relating to, connected with, or using a regulated service of any entity is a scam;

(b) it is a kind prescribed by the SPF rules; and

(c) the intelligence is reasonably able to serve as the basis for the regulated entity to decide to act on the suspected scam

APPENDIX C

Recommendation 2:
Clarify what, when and how actionable scam intelligence should be reported

A high frequency of alerts can breed complacency and warning fatigue among SPF Consumers, thereby rendering them ineffective. Westpac therefore suggests the following amendments:

Amend section **58BY** as follows:

(2) The entity contravenes this subsection if the entity fails to give a report about the actionable scam intelligence:

(a) to the SPF general regulator:

(i) before the end of the period prescribed by the SPF rules that starts at the end of the period referred to in paragraph 58BZA(2)(d) for that intelligence (unless by the end of the period, the entity has identified that the activity the subject of that intelligence is not a scam); and

(ii) in the manner and form prescribed by the SPF rules

Amend section **58BK(2)** as follows:

Further sector specific details can be set out in SPF codes

(2) For the purposes of ~~(but without limiting)~~ subsection 58CC(1), the SPF code for a regulated sector ~~may~~ must include sector specific provisions:

(a) describing what are reasonable steps for the purposes of this Subdivision (see also section 58BB); or

(b) requiring each regulated entity for the sector to:

(i) identify its SPF consumers who are at risk of being targeted by a scam; or

(ii) identify its SPF consumers who have a higher risk of being targeted by a scam; or

(c) requiring each regulated entity for the sector to provide information about such scams to an SPF consumer describe in subparagraph (b)(i) or (ii).

APPENDIX D

Recommendation 3:

Extend the safe harbour for actions taken after an entity reasonably identifies activity to be a scam

The Bill significantly limits the scope beyond what we assume is intended—that is—to provide safe harbour when entities are taking reasonably proportionate action to stop a scam.

We suggest amending section **58BZ** to:

(1) This section applies to a regulated entity if the entity ~~has~~ reasonably considers it may have actionable scam intelligence of the kind described in section 58AI about an activity relating to, connected with, or using a regulated service of ~~the~~ an entity.

(2) The regulated entity is not liable in a civil action or civil proceeding for taking action to disrupt the activity if the action

(a) is taken in good faith; and

(b) is taken in compliance with the SPF provisions; and

(c) is reasonably proportionate to the ~~activity~~ suspected scam, and to information that ~~would~~ is reasonably ~~be expected to be~~ available to the entity about the activity, having regard to the circumstances including the time available to take the action and the potential loss or damage if the action is not taken; and

(d) is taken:

(i) during the period:

(A) starting on the day that the intelligence becomes actionable scam intelligence for the entity; and

(B) ending when the entity reasonably believes that the activity is or is not a scam, or after 28 days, whichever is the earlier; or

(ii) after the entity identifies the activity is a scam; and

(e) is promptly reversed if:

(i) the entity identifies that the activity is not a scam; and

(ii) it is reasonably practicable to reverse the action

APPENDIX E

Recommendation 4:

Improve alignment between the SPF Principles and Codes and their associated penalties

Principles-based obligations alongside sector-specific obligations in the SPF Codes will create uncertainty, ambiguity and unnecessary duplication. We suggest redrafting the principles so that they are positive obligations that the SPF Code must reflect, for example by:

Replacing, where relevant, *"A regulated entity contravenes this subsection if the entity…"* with *"The SPF Code must set out obligations on regulated entities to…"*