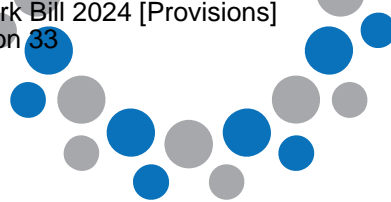




Australian Banking  
Association



# **Senate Economics Committee Inquiry into the Scams Prevention Framework Bill 2024**

**Submission of the Australian Banking Association**

9 January 2025





## Table of Contents

1.0	Overview .....	2
2.0	The need for a whole of ecosystem approach .....	3
2.1	Australian banks are acting to protect customers from scams .....	3
2.2	Scams do not originate in banks .....	4
2.3	Digital platforms must do more .....	5
3.0	Detailed recommendations .....	8
3.1	Streamline the interaction of the SPF Principles and Industry Codes to provide clear investment incentives .....	8
3.2	Ensure that “actionable scam intelligence” is actionable .....	10
3.3	Clarify the scope of the application of the SPF to retail and SME customers .....	10
3.3.1	Application to institutional or wholesale customers .....	11
3.3.2	Bank liability for actions of wholesale and institutional customers .....	12
3.4	Clarify some aspects of extraterritorial application .....	12
3.5	Further clarify the interaction with other obligations .....	13
3.6	Ensure appropriate transitional arrangements .....	14
	Appendix – Examples of bank account sales on digital platforms .....	15

### Policy Contact:

Nicholas Giurietto, Head of Future Policy



Merric Foley, Policy Director



### About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.



## 1.0 Overview

The Australian Banking Association (**ABA**) welcomes the opportunity to provide a submission to the Senate Standing Committee on Economics inquiry into the *Scam Prevention Framework Bill 2025* (**the SPF Bill**).

The ABA reiterates its support for the Government's whole-of-ecosystem approach to combatting scams, the introduction of sector-specific mandatory scams codes (**Industry Codes**), and the stated intention to establish a single external dispute resolution (**EDR**) scheme for scams.

The whole-of-ecosystem approach outlined in the SPF Bill will build on proactive measures being taken by the banking industry against scams. Banks continue to invest in measures to protect Australians from scams. The work undertaken by banks, on both an individual and collective basis through the ABA ScamSafe Accord, has already begun to pay dividends. Australia is one of the few countries in the world reporting declining scam losses with losses reported to ScamWatch falling from \$559million in 2023 to \$330million in 2024.<sup>1</sup>

However, scams do not originate with banks.

It is therefore essential that the design and implementation of the SPF appropriately and effectively incentivise all relevant sectors of the economy to contribute to the national anti-scams effort. Banks' efforts to strengthen the last line of defence against scams must be supplemented by measures to stop scams at the source, before they reach Australians. In particular, digital platforms must fully participate in a co-ordinated national anti-scam defence.

This submission highlights key opportunities to strengthen the SPF Bill to ensure that all relevant sectors of the economy have effective incentives to invest in strengthened scams defences, most importantly to provide clear investment incentives by streamlining the interaction of the SPF Principles and Industry Codes.

In addition, we recommend additional measures to strengthen the SPF Bill generally: to ensure that "actionable scams intelligence" is truly actionable, and to clarify the scope of application of the SPF to retail and SME customers.

The **ABA supports the passage of the SPF Bill** alongside implementation of the above recommendations to strengthen its impact and drive the most effective possible national anti-scams effort.

---

<sup>1</sup> National Anti-Scams Centre (Nov 2024) *National Anti-Scam Centre in Action: Quarterly Update* ([link](#)) page 1



## 2.0 The need for a whole of ecosystem approach

### 2.1 Australian banks are acting to protect customers from scams

Banks have always worked to protect their customers from fraud and crime. As scams have grown globally, banks have redoubled their efforts in this area. Over the past two years, Australian banks have acted on a collective and individual basis to introduce new systems and platforms to protect Australian consumers from scams. The actions taken by Australian banks have complemented the work of the Australian Government's innovative National Anti-Scams Centre (**NASC**), other regulatory organisations such as the Australian Securities and Investments Commission (**ASIC**) and the telecommunications sector in beginning to drive down scam losses in the Australian community, with losses reported to ScamWatch falling from \$559million in 2023 to \$330million in 2024.<sup>2</sup>

The Scam-Safe Accord represents the banking industry's commitment to protecting customers from scams.<sup>3</sup> Through this industry-wide collaboration, banks are adding greater friction to payments, enhancing detection systems and sharing intelligence to help protect customers. Key initiatives include:

- **Confirmation of payee (COP).** Australian banks are investing \$100 million in a new industry-wide system ensuring that people can confirm they are transferring money to the person they intend to. As of January 2025, Australian Payments Plus (**AP+**) has completed the design of the COP service and testing has commenced. Noting that some banks already have equivalent, bank-specific, mechanisms in place, financial institutions will progressively integrate the new service into their banking channels, commencing in 2025.
- **Intelligence sharing.** ABA members have joined the Australian Financial Crimes Exchange (**AFCX**) and its Fraud Reporting Exchange (**FRX**). These services help banks share verified scams intelligence at speed – helping to prevent more scams and recovering funds for customers faster. Beyond the Scam-Safe Accord, many ABA members are also participating in the AFCX Anti-Scams Intelligence Loop (**ASIL**), which enables near real-time data sharing between participants.
- **Biometric checks.** To help prevent the misuse of accounts, ABA members have committed to introducing further technology and controls, for when new individual customers open accounts online. ABA members have implemented biometric checks for new accounts or are on track to do so. This supplements the existing checks that banks undertake under existing anti-money laundering (**AML**) and know your customer (**KYC**) obligations.
- **Payment warnings.** Australian banks are implementing risk-based payment warnings to help introduce appropriate friction to payment transactions. This may include appropriate warnings such as adding a new payee, amending a payee, increasing payment limits, and using technology to introduce risk-based delays.

The Australian banking industry has also invested significantly in other initiatives. For example, over the past year, the ABA has run educational advertising campaigns directed at informing and educating

<sup>2</sup> National Anti-Scams Centre (Nov 2024) *National Anti-Scam Centre in Action: Quarterly Update* ([link](#)) page 1

<sup>3</sup> ABA (accessed Jan 2025) *Keeping Australia Scam Safe* ([link](#))



## Australian Banking Association

consumers.<sup>4</sup> The ABA's campaigns emphasise industry-wide themes, such as the importance of "alarm bells" or seasonal-specific topics such as Black Friday, Christmas and Boxing Day sales.

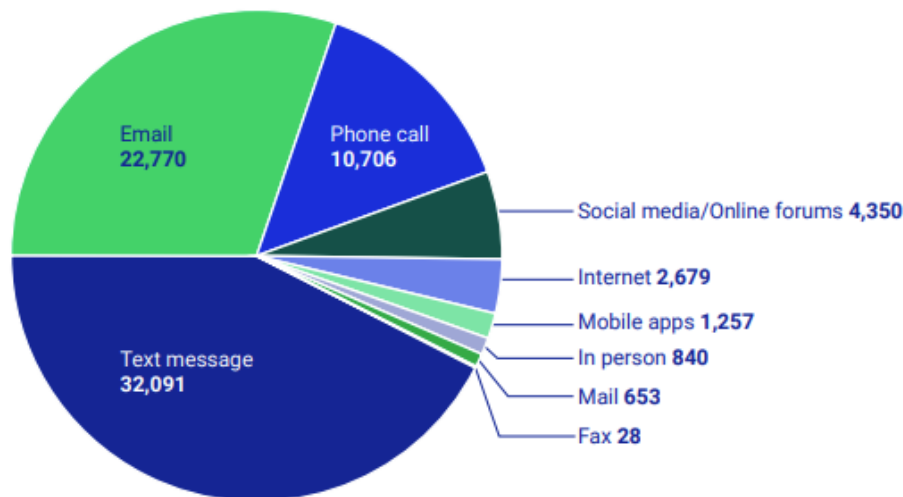
The banking sector recognises that further investment, continuous improvement and vigilance is necessary as scams continue to evolve. Australian banks have actively contributed to NASC fusion cells, invested in customer education campaigns, and continued to innovate on both an individual and collective basis. The submissions made by ABA member banks provide more detail on their own anti-scam actions.

## 2.2 Scams do not originate in banks

By the time a customer uses their banking service to make a payment to a scammer, they have **already** been scammed.

Banks have an essential role – for example, in detecting scams, warning customers of potential scam risks, and attempting to recover funds. However, this role is necessarily a last line of defence and must be complemented by efforts to stop scams at source before they reach Australians in the first place.

Scammers typically initiate contact with a potential victim through a social media post, messaging app, SMS or direct phone call. These avenues of first contact ultimately take place outside of the bank's visibility. While banks can and do take preventative safety education measures,<sup>5</sup> they ultimately have no direct influence over these points of first contact.



Number of reports by contact method, April-June 2024<sup>6</sup>

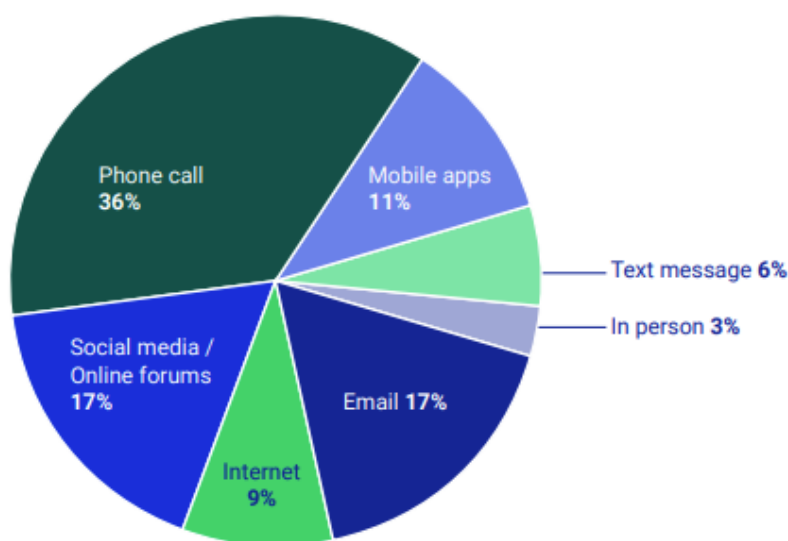
<sup>4</sup> See the 2023/2024 "Alarm Bells" campaign (<https://www.ausbanking.org.au/scams-hear-the-alarm-bells/>)

<sup>5</sup> For example, ABA campaigns have advised customers that banks will never ask customers to transfer funds to another account over the phone; ask for sensitive banking details like online banking passcodes or passwords; ask for remote access to a customer's devices; or threaten customers to take immediate action on an issue.

<sup>6</sup> National Anti-Scams Centre (Nov 2024) *National Anti-Scam Centre in Action: Quarterly Update* ([link](#)) page 6



Australian Banking  
Association



*Percentage of overall losses by contact method, April-June 2024<sup>7</sup>*

## 2.3 Digital platforms must do more

Complementary work across government and the banking sector has already led to a significant decline in scam losses. The introduction of the SPF and Industry Codes will continue this trend.

Unfortunately, experience to date shows that the digital platform sector has not matched the investments or ambition of the Australian banking sector. As the business model of these entities is based on advertising revenue (which unfortunately currently includes a great deal of scam advertising), it is unlikely that they will take significant anti-scams steps unless the SPF contains effective incentives to do so.

The screen shot below provides an example of a user of a digital platform messaging app soliciting the misuse of a bank account. Facilitating the sale of legitimately established Australian bank accounts undermines attempts by banks to combat mule accounts<sup>8</sup> and is an example of burden shifting by digital platforms that are failing to meet reasonable community expectations to help keep Australians safe from scams. When this was drawn to the attention of the platform, they declined to remove the ad as it did not “go against our Community Standards”.

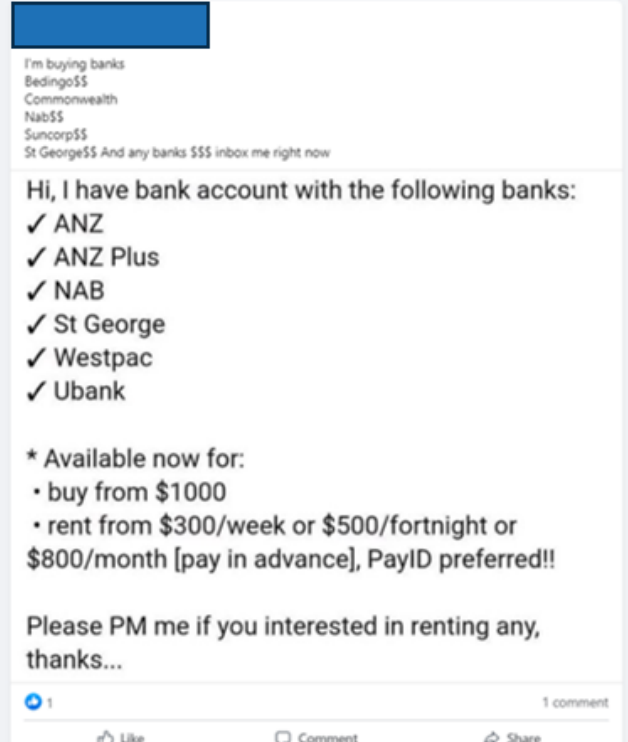
---

<sup>7</sup> National Anti-Scams Centre (Nov 2024) *National Anti-Scam Centre in Action: Quarterly Update* ([link](#)) page 7

<sup>8</sup> A mule account is operated by a scammer that is used to collect victim funds and transfer them to another account, or outside of Australia.



## Australian Banking Association

 <p>The screenshot shows a Facebook post from a group named "I'm buying banks". The post text reads: "Bedingo\$\$ Commonwealth Nab\$\$ Suncorp\$\$ St George\$\$ And any banks \$\$\$ inbox me right now". Below this, the post says: "Hi, I have bank account with the following banks: ✓ ANZ ✓ ANZ Plus ✓ NAB ✓ St George ✓ Westpac ✓ Ubank". It then lists terms: "* Available now for: • buy from \$1000 • rent from \$300/week or \$500/fortnight or \$800/month [pay in advance], PayID preferred!!". The post ends with "Please PM me if you interested in renting any, thanks...". At the bottom, there is a blue heart icon with the number "1", and icons for "Like", "Comment", and "Share".</p>	<p>Yesterday at 10:13 PM</p> <p><b>We didn't remove the group</b></p> <p>To keep our review process as fair as possible, we use the same set of Community Standards to review all reports.</p> <p>We've taken a look and found that the group doesn't go against our Community Standards.</p> <p>We understand that this might be upsetting so we recommend exploring the options available to control what you see.</p> <p>If you want us to review something specific within a group, be sure to report the content (example: photo), not the entire group.</p>
---	---

This is not an isolated incident. The **Appendix** to this document provides further screenshotted examples of groups on a digital platform soliciting the sale or rent of Australian bank accounts. These screenshots were taken following a short, ten-minute search of the platform in question with a simple search string "rent bank account". These examples were openly visible on the platform and the ease at which they were identified raises serious questions about the platform's commitment to fighting scams.

While banks have a range of measures to combat different types of mule accounts, one of the most effective points banks have at addressing identity takeover is at account opening, where KYC checks are undertaken to verify the individual's identity. Identifying a mule account via other measures becomes much more complex if an account is validly opened by a genuine customer and later rented or sold to a scam syndicate.

The selling of mule accounts is not the only form of scam activity being facilitated on digital platforms. Equally, if not more, concerning is their use as an initial point of contact between scammers and victims. As indicated above, NASC reports indicate that "social media/online forums" account for 17% of overall scam losses reported to ScamWatch. Regulators have continued to raise concerns about the level of scam activity on digital platforms. In early December 2024, ASIC warnings to consumers about suspect investment scams being advertised on digital platforms,<sup>9</sup> and a review of cryptocurrency advertisements by the ACCC indicated that 58% of the advertisements reviewed "violated Meta's Advertising Policies or, potentially, involved scams".<sup>10</sup>

<sup>9</sup> ASIC (Dec 2024) *Suspected scam alert; ASIC warns customers about unlicensed stock tip promoters through private chat apps* (link)

<sup>10</sup> <https://classic.austlii.edu.au/au/cases/cth/FCA/2024/890.html>



Finally, while welcoming the recent announcement by Meta that it will introduce identity verification for advertisers of financial products on its platforms,<sup>11</sup> we note that further actions are required to reduce buy/sell scams.

---

<sup>11</sup> <https://www.theguardian.com/technology/2024/dec/02/meta-to-force-financial-advertisers-to-be-verified-in-bid-to-prevent-celebrity-scam-ads-targeting-australians>





## 3.0 Detailed recommendations

The ABA supports passage of the SPF Bill. This is a critical measure to drive a whole-of-ecosystem approach to protect Australians from scams. Australia has made strong progress in reducing the value and volume of scams but losses, and their devastating impacts, remain too high. Further progress requires that all relevant sectors of the economy contribute appropriately to the battle against criminal scammers.

This submission makes several recommendations for Committee consideration that would further strengthen the impact of the proposed framework, most importantly to:

- Streamline the interaction of the SPF Principles and Industry Codes to provide clear investment incentives;
- Ensure that “actionable scams intelligence” is actionable and ensure that expectations on organisations are clear;
- Clarify the scope of application of the SPF to retail and SME customers;
- Clarify interactions with other laws.

Additionally, the ABA recognises that many aspects of the proposed regime will be further defined in the SPF Rules and Industry Codes. A clearly defined and robust dispute resolution mechanism will be critical to the SPF’s operation. The SPF Rules should provide clear liability rules, an apportionment mechanism to guide dispute resolution processes and ensure a consistent approach for customers to seek redress across all relevant sectors.

Banks accept that liability should apply to all relevant sectors on a proportional basis, including our own, where entities have failed to meet their obligations. While noting the challenges in developing and applying cross-sectoral liability rules, we view that passage of the SPF Bill will provide a clear “line in the sand” to all parties. We are committed to working constructively with the Government and other industries to develop a fair and evidence-based liability framework.

### 3.1 Streamline the interaction of the SPF Principles and Industry Codes to provide clear investment incentives

The ABA submission to the Treasury consultation on the SPF exposure draft (**ED**) legislation highlighted a significant concern with the interoperation of the SPF Principles and Industry Codes. An organisation can comply fully with its obligations under the relevant Industry Code but nevertheless be found responsible for compensation or regulatory sanction under an SPF Principle. This creates a double jeopardy challenge that is problematic in principle and undermines the clarity of communication of regulatory expectations essential to drive the necessary long-term investments in anti-scams measures. Effectively marshalling resources for anti-scams investment means it is essential that regulated organisations know the goals at which they are aiming.

In our submission to the ED consultation, we stated:

*An environment in which reasonableness is determined on a case-by-case basis will not provide sufficient certainty on which to base long-term investment decisions in anti-scams capability. The industry-led Scam-Safe Accord provides a strong example where clearly defined obligations have underpinned substantial ongoing investment in anti-scams measures*



*across the banking sector. Industry actions were possible because of the certainty provided by collaborative discussion and agreement on the key priorities for combatting scams.*

We acknowledge that changes following the ED consultation go some way to addressing this concern. In considering whether a regulated entity (**RE**) complied with an SPF Principle, the SPF Bill would require the decision maker to consider whether the RE complied with the relevant Industry Code.<sup>12</sup> However, this would still create an uncertain and ambiguous two-tier regulatory environment that risks diverting investment from actual anti-scams initiatives to administrative compliance tasks with nil-to-minimal real-world impact on scammers.

The ABA understands that the Government's reasoning for retaining concurrent application is twofold:

- It ensures that the SPF applies to a particular sector immediately on designation, noting that the development of an Industry Code for that sector may take several months or longer.
- The Codes are intended to contain more specific commitments and may not be able to properly capture the evolving scams environment. Applying the SPF Principles will ensure that REs are held accountable to take appropriate actions in response to emerging scams that are not contemplated under the relevant Industry Code.

While acknowledging the Government's viewpoint, the ABA respectfully views that there are more effective ways of accommodating these perspectives:

- Application of the SPF Principles by a decision-maker to an RE could be restricted to instances in which an Industry Code has not yet been applied to the relevant sector. This model would have the additional advantage of incentivising industry sectors to expedite development of Industry Codes as a pathway to regulatory certainty.
- The Codes themselves can and should be reviewed on a regular basis as the threat landscape evolves, using actual scams data and intelligence to determine what, if any, further steps should be taken to continue to drive down scams. This approach would combine regulatory certainty with a clear and data driven mechanism to update regulatory expectations.

Finally, the ABA reiterates our earlier view that the right to bring individual causes of action is inappropriate to include in the legislation. The principal intent of the regime is to encourage preventative action on a whole-of-ecosystem basis, and the legislation already provides for dispute mechanisms through IDR, EDR and civil penalties.

### Recommendation

The ABA recommends that:

- The legislation be amended such that, in a sector where a Code has been approved and issued, compliance with that Code is taken to be compliance with the SPF Principles.
- The legislation be amended to remove the right to bring individual causes of action against REs.
- Industry Codes be updated every two years to reflect the impact of existing measures and the evolving scams threat landscape.

<sup>12</sup> Section 58BB



### 3.2 Ensure that “actionable scam intelligence” is actionable

As identified in our earlier submission to Treasury on the ED consultation, the ABA holds concerns regarding the breadth of the definition of “actionable scams intelligence”, which currently reads:

*A regulated entity identifies or has actionable scam intelligence if (and when) 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 the entity is a scam.*

Our concern is that there is no element of the definition in the current Bill that means that “actionable scams intelligence” is truly “actionable” – in the sense of being capable of supporting a decision to act. Throughout the Bill, holding or possessing actionable scam intelligence frequently serves as the trigger point requiring an RE to take certain forms of action. For example, section 58BR would require the reporting of actionable scam intelligence to the regulator.<sup>13</sup>

On its own, a mere suspicion may not always be a sufficient basis on which to take effective action. We are concerned that the current definition may lead to a substantial increase in compliance, including substantially more reports to a regulator, rather than the creation of more information that can actually be used to inform decisions about combatting scams.

The ABA views that a more effective approach would be to allow for the SPF Rules to further define “actionable scam intelligence”. This would allow the Minister to work with expert anti-scam practitioners in industry to identify and define those data elements that are most useful in combatting scams without the risk of swamping the system with non-useable information. Importantly, this approach would strengthen the whole of ecosystem data sharing model that has already begun to pay dividends in Australia’s battle against scammers.

#### Recommendation

The ABA recommends that:

- That the legislation be amended to provide the Minister with the power to issue SPF Rules that more clearly define actionable scam intelligence.

### 3.3 Clarify the scope of the application of the SPF to retail and SME customers

Australian banks support the SPF Bill and accept our role in protecting Australian consumers from scams. We view that actions to combat scams across the ecosystem will be most effective if they can be directly targeted towards consumers. Below, the ABA has presented some examples where the current drafting of the SPF Bill may inadvertently capture entities that it was not designed to. Clarifying these areas would ensure that ecosystem wide efforts and resources remain directed towards the most promising areas.

---

<sup>13</sup> Also see, for example, sections 58BX and 58BY



## Australian Banking Association

### 3.3.1 Application to institutional or wholesale customers

The ABA views that the legislation should be clarified to specify that the framework does not apply to institutional or wholesale customers.<sup>14</sup> As outlined in the Explanatory Memorandum (**EM**), the legislation is designed to protect the Australian community and consumers.<sup>15</sup> It is not intended to capture large corporate clients. Capturing large corporate clients would increase the complexity of implementation and direct resources away from the intended beneficiaries – individual consumers and small businesses

Section 58AH(1) defines “SPF consumer” to include a natural person, or a small business operator, who is or may be provided or purportedly provided the service in Australia. Relevantly, the definition of “small business operator” means:<sup>16</sup>

*(a) in the case of the person being a body corporate:*

- i. the sum of the person’s employees, and the employees of any body corporate related to the person, is less than 100 employees; and*
- ii. the person’s annual turnover during the last financial year is less than \$10 million; and*

*(b) in the case of the person not being a body corporate:*

- i. the person has less than 100 employees; and*
- ii. the person’s annual turnover (worked out as if the person were a body corporate) during the last financial year is less than \$10 million; and*

*(c) in every case—the business has a principal place of business in Australia.*

The ABA notes that the “annual turnover” limbs have been incorporated since the ED consultation. While the ABA appreciates these clarifications, we view that additional amendments may be needed to exclude wholesale and institutional customers and ensure that scam prevention efforts are appropriately targeted.

We view that a combination of measures may be needed, including:

- Explicitly excluding wholesale and institutional customers from the operation of the legislation and exclude banks without a retail client base.<sup>17</sup> An example of how this could be achieved in the SPF Bill is provided by the no-action letter provided by ASIC<sup>18</sup> in relation to the Unfair Contract Terms (**UCT**) regime.<sup>19</sup>

<sup>14</sup> Save for individuals who have met the requirements of the ‘sophisticated investor test’ for the purposes of the *Corporations Act*

<sup>15</sup> See for example, paras 1.4 to 1.14 repeatedly discuss the protection of Australian consumers

<sup>16</sup> *Scam Prevention Framework Bill* 58AH(5) definition of **small business operator**

<sup>17</sup> The ABA notes that some banks hold AFSL exemptions (such as the “sufficient equivalence” relief) that restrict them to dealing with wholesale clients only. Given their client base, such banks are typically not required to maintain IDR arrangements or to join an EDR scheme.

<sup>18</sup> ASIC (Feb 2024) *Class no-action letter – s12BF(2A) and (2C) of the Australian Securities and Investments Commission Act 2001 and s912A(1)(c) and 912D(1) of the Corporations Act 2001* ([link](#))

<sup>19</sup> *Australian Securities and Investments Commission Act 2001 (ASIC Act)* as amended by the *Treasury Laws Amendment (More Competition, Better Prices) Act 2022 (Cth) (UCT Reforms)* (together the **amended UCT regime**).



## Australian Banking Association

- Measuring thresholds for small business at a group level, including the parent and related bodies corporate. This could be potentially accomplished by amending section 58AH(5)(a) as follows:
  - In 58AH(5)(a)(i), replacing the term “body corporate related to the person” with the term “person’s body corporate” in 58AH(5)(a)(i), and
  - In 58AH(5)(a)(ii), adding the wording “(together with any related body corporate’s annual turnover)”.

### 3.3.2 Bank liability for actions of wholesale and institutional customers

The ABA notes that Government has indicated that Third-Party Payment Providers (**TPPPs**) and/or Money Service Businesses (**MSBs**) will not be included within the SPF’s initial scope.<sup>20</sup> However, there remains a possibility that other parties within the ecosystem will be held responsible for losses incurred through them.

Consistent with the Australian Government’s ecosystem approach to fighting scams, the ABA views that entities best capable of dealing with scams should bear liability for any losses arising out of their failure to act. In this case, the TPPPs and MSBs themselves. The ABA suggests that the Australian Government include TPPPs and MSBs in a future SPF phase as a matter of priority and, in the interim, clearly demarcate areas of bank liability for these losses.

#### Recommendation

The ABA recommends that:

##### **Application to wholesale and institutional customers**

- The legislation be amended to:
  - Explicitly exclude wholesale and institutional customers from the operation of the SPF (noting the above caveat for sophisticated investors).
  - Clarify that thresholds for small business are measured at the group level including the parent and related bodies corporate.

##### **Bank liability for actions of wholesale and institutional customers**

- The Australian Government include TPPPs and MSBs in a future SPF phase as a matter of priority and, in the interim, amend the legislation to clearly demarcate areas of bank liability.

### 3.4 Clarify some aspects of extraterritorial application

The Framework applies “extraterritorially” to “acts, omissions, matters and things outside of Australia” meaning that the Framework will intersect with other jurisdictions’ scams frameworks (e.g. the United Kingdom and Singapore). We view that further clarity is needed on how this would work in practice.

<sup>20</sup> Explanatory Memoranda paragraph 1.8



For example, an individual who normally resides in Australia may leave for a period to work, study or travel in another jurisdiction. It is unclear whether SPF obligations would apply to that person were they to be based internationally. This has practical implications, as the RE may have limited ability to take action to protect that individual. A similar concern can be raised with respect to how REs would assist a business that has a principal place of business in Australia but operates offshore.

Likewise, the SPF applies to businesses with a “*principal place of business in Australia*” but by way of section 58AJ, applies “extraterritorially” to “acts, omissions, matters and things outside of Australia”. Again, RE may be limited in how they can protect these businesses in respect of their international activities to the same extent as their domestic activities.

#### Recommendation

The ABA recommends that:

- The SPF Rules and Industry Codes provide further guidance on application to Australians living and travelling abroad for extended periods of time, including which jurisdictions’ framework applies where there is intersection between two and how the location of a principal place of business should be determined.

### 3.5 Further clarify the interaction with other obligations

There is an opportunity to provide more clarity regarding the interaction of the SPF with other legislative obligations, particularly the *Anti-Money Laundering and Counter-Terrorist Financing Act (AML/CTF Act)* and the *Spam Act*. For example:

- A “safe harbour” provision in the SPF could allow REs to take an action to prevent a scam being perpetrated in circumstances where existing laws may prevent the action. This could include a disclosure that may otherwise be prohibited by the tipping off provisions of the AML/CTF Act or contacting a customer who has opted out of communications under the *Spam Act*.
- Many elements of actionable scams intelligence reporting will overlap with AUSTRAC’s Suspicious Matter Reporting (**SMR**) Regime. Once actionable scams intelligence is identified, a “suspicion” (for the purposes of the AML/CTF Act) is likely to have also been formed, which would require an entity to submit an SMR to AUSTRAC, potentially creating a duplicative reporting obligation. The full extent of overlap will be apparent after finalisation of the SPF Rules and Codes. The ABA views that the SPF Bill, SPF Rules and Industry Codes should be designed to minimise the level of duplication. This could also involve utilising the regulator information sharing provisions to ensure that if a case is reported to one regulator, it does not need to be shared to another regulator.
- Finally, we note that implementation of obligations under the SPF may increase the likelihood of false positives leading to payment blocks or delays. We note that 58BW(2) provides a safe harbour for REs taking such actions, and suggest that the SPF Rules could further define the safe harbour circumstances.





### 3.6 Ensure appropriate transitional arrangements

Recognising the need for rapid action, the ABA views that a staggered transitional approach is the best way to balance allowing time for system changes while also ensuring that the rollout of additional protections for Australian consumers are not delayed. Introduction of the Industry Codes will create new obligations on all REs, which will take different timeframes to implement:

- Some obligations will require additional investment in complex technology builds and implementation, and internal process change. These will have to be incorporated into existing roadmaps, and smaller members may require additional time to marshal resources. For example, the timeframe for an industry-wide COP (including technical build by AP+ and integration into core banking systems) has allowed for over twelve months.
- Equally, some obligations may not require significant timelines for implementation and rollout and may be capable of applying shortly after the introduction of the Industry Codes. For example, the Industry Codes may reflect some obligations under existing industry agreements that members of that sector should have already implemented.

As a baseline, the ABA views that all obligations should enter into force 12 months from agreement of the Industry Codes that will contain the industry-specific obligations. Consistent with the staggered implementation approach outlined above, some obligations could be brought forward (where they can be easily met or should already be met) or moved backwards (to allow entities of all sizes time to implement any particularly complex technical builds).

Finally, the SPF will cover multiple sectors and the obligations on different sectors will be mutually reinforcing. As such, the ABA views that the development and implementation of Industry Codes should be aligned, with designation occurring simultaneously for all sectors within the first tranche.

#### **Recommendation**

The ABA recommends that:

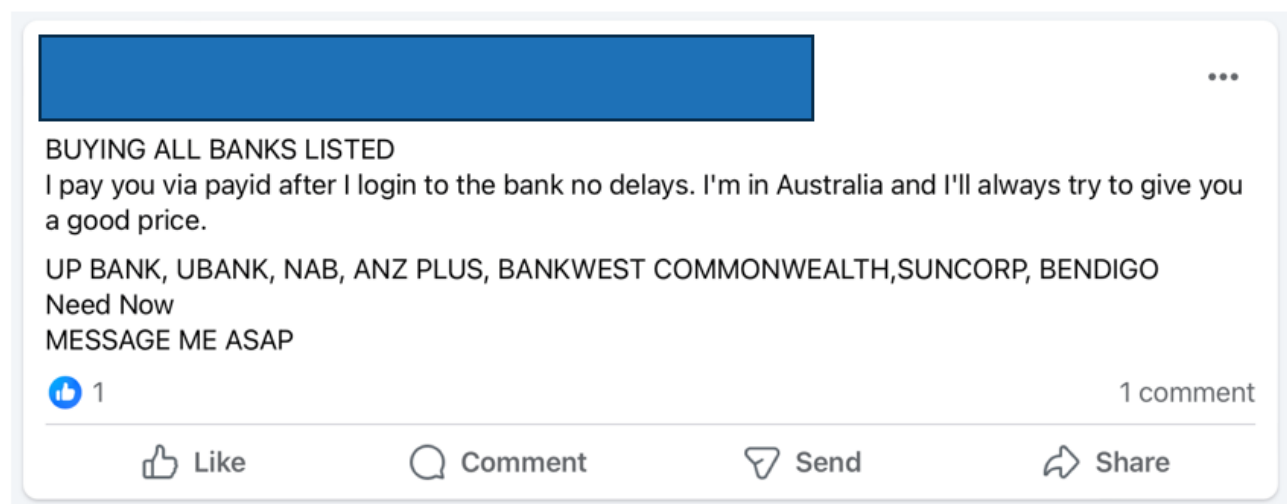
- The legislation be amended to provide a flexible transition timeframe, including:
  - As a baseline, all obligations entering into force 12 months from agreement of the Industry Codes
  - A Ministerial power to move certain obligations forward or backwards depending on complexity of implementation.
- Industry Codes for all sectors within the first tranche be developed concurrently, and all sectors in the first tranche should be designated simultaneously.



## Appendix – Examples of bank account sales on digital platforms

The screenshots below are examples of advertising and soliciting the sale or rental of bank accounts, occurring openly on digital platforms. These screenshots were taken following a short, ten-minute search with a simple search string “rent bank account”. These represent only a small fraction of the Australian bank accounts listed on the platform. Many of the groups in which these advertisements were posted have been allowed to continue by the platform for many months.

At time of writing, one popular group “Gameing rent bank account” had been live since May 2024, and another group “AUSTRALIAN BANK ACC RENTING” had been live since September 2024.







## Australian Banking Association

I Buyer Need new Acc or old account prefer CommBank, Ubank, Up bank, ANZ plus Nab, Bankwest, Suncorp, Bendigo Bank, ING, Please send me a message if you have Payment via payment id. And I'll pay for it quickly Send me a message now

1

9 comments

Like

Comment

Send

Share

Anyone have a U bank for rent message me asap

1

4 comments

Like

Comment

Send

Share

I need a bank account  
Australia bank  
Nab, UBANK, UPBANK, COMMBANK, ANZ PLUS \$1200  
Any bank Australia  
Message me

1 comment

Like

Comment

Send

Share



## Australian Banking Association



...

Hey there, looking to earn some extra income with your bank accounts?  
The first payment will be paid upfront upon checking your bank account login details and usage (and no, you don't have to change your mobile number or any other stuff, just make sure that your acc has a payid linked) and the 2nd payment will be paid monthly, vice versa. No bullshit like downloading or links, you're collaborating with a legit business team!

Banks list that we are looking for:

UpBank  
Auswide  
Mego  
Boq  
Virgin  
Heritage  
Qudos  
Bankwest  
Suncorp  
Bendigo  
NAB  
CommBank  
ANZ  
haybank  
Macquarie Bank  
GS Bank  
ING

If you're interested, please add: Jessy2103\_ on WeChat, 100% legit and thanks for reading, hope to do business with y'all soon!

1

4 comments

Like

Comment

Send

Share



...

I have a ING account prefer to sell or can rent out at weekly rate  
Make an offer to buy upfront or rent  
Serious buyers plz

1

Like

Comment

Send

Share



Australian Banking  
Association



I need a bank account

Australia bank

Nab, UBANK, UPBANK, COMMBANK, ANZ PLUS, SUNCORP, COMMONWEALTH \$1200

Any bank Australia

Need Now

Message me



1

4 comments



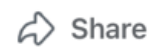
Like



Comment



Send



Share



I need a bank account

Australia bank

Nab, UBANK, UPBANK, COMMBANK, ANZ PLUS , BANKWEST, BINANCE, SUNCORP, \$1200

Any bank Australia

Need Now

Message me Asap



1

2 comments



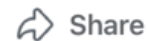
Like



Comment



Send



Share



I need a bank account

Australia bank

Nab, UBANK, UPBANK, COMMBANK, ANZ PLUS, BANKWEST, COMMBANK, BINANCE \$1200

Any bank Australia

Need Now

Message me



3

5 comments



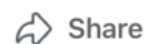
Like



Comment



Send



Share



Australian Banking  
Association



Looking for people who've never sold banks before. Offering good rent\$\$

Westpac-250pw

Nab-250pw

Beyond-1800pw

Bendigo-300pw

Upbank-350pw



3

31 comments 60 shares



Need upbank 300 per bank per week



7

24 

- ENDS -