

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

04/10/2024

Via email: scampolicy@treasury.gov.au

Treasury Laws Amendment Bill 2024: Scams Prevention Framework

Dear Treasury Scams Taskforce,

Thank you for the opportunity to comment on the draft legislation which implements the Scams Prevention Framework (**SPF**). Australian Payments Plus (**AP+**) welcomes this next step in the Government's commitment to fight scammers and organised crime and supports the world-leading, whole of ecosystem approach that the Government is taking.

AP+ brings together Australia's three domestic payment organisations, BPAY Group, eftpos and the New Payments Platform (**NPP**) into one entity. Our payment schemes are subject to Reserve Bank of Australia (**RBA**) oversight under the *Payments Systems (Regulation) Act*.

AP+, alongside our NPP Participating Institutions, is currently building and testing the Confirmation of Payee (**CoP**) solution, which will be a valuable tool in the financial sectors efforts to combat scams and frauds. Financial institutions will integrate the CoP service into their banking channels starting in early 2025.

As the operator of Australia's domestic payment infrastructure, we frequently uplift the rules and fraud controls of our various products and schemes to build greater resilience in the payment ecosystem and to respond to new scam and fraud vectors. **ConnectID**, is our national digital identity exchange which will help prevent identity theft by making Australian's identities harder to steal. AP+ is also an active member of the Australian Financial Crimes Exchange (AFCX) and the ACCC National Anti-Scam Centre (NASC).

The Australian payment system

Our regulator, the RBA, is responsible for promoting the stability, efficiency and competitiveness of the payments system through the Payments System Board (**PSB**). The PSB has five strategic priorities which includes the promotion of competitive, cost-effective and accessible electronic payments. In their 2024 Annual Report¹, the PSB notes the RBA is actively encouraging the banking industry to deliver and promote additional fast payment capabilities to end users, whilst also controlling risk in the financial system and promoting the efficiency of the payments system.

In 2022/23², Australians made on average, 730 electronic transactions per person. We estimate, across all the different account-to-account (**A2A**) payment mechanisms in the Australian payment system, that \$18.5 Trillion A2A payments were made by financial institutions, government users, businesses, and consumers in 2023/24. Thus, the RBA has a close interest in the capability of the NPP, especially the uptake of new functionality to meet the evolving needs of end users in the Australian economy.

¹ The RBA Payments System Board (PSB) Annual Report 2024 ([link](#))

² The RBA Payments System Board (PSB) Annual Report 2023 ([link](#))



Launched in 2018, the NPP is now available to the retail and business customers of more than 110 financial institutions and is currently used to make almost one-third of all account-to-account payments. In 2023/24 the NPP processed over 1.5 billion transactions worth more than \$1.8 trillion, and usage continues to grow due to the functionality the NPP, and the 2030 closure of Bulk Electronic Clearing System (BECS).

The Scam Prevention Framework

AP+ understands the importance of safe, secure and resilient domestic payment infrastructure. As the operator of Australia's domestic payment infrastructure, we offer one recommendation that preserves the effectiveness of the SPF and avoids disruption to the orderly operation of Australia's systemically important payment infrastructure³ and avoids unduly impacting the real-economy where financial institutions, government users, businesses and consumers require certainty across many different payment use-cases (**payment certainty**).

The Government is one of the largest users of the domestic payment system. In 2022/23 Services Australia⁴ made payments worth \$219.5 Billion, which includes \$1.8 Billion in disaster and emergency payments. Services Australia relies on the orderly operation of Australia's payment system to quickly deliver disaster and rapid response payments to support those Australian's severely impacted by floods, bushfires and other natural disasters. Services Australia managed 977,000 of these emergency calls in 2022/23.

We highlight this example of Services Australia emergency relief payments, as it goes to our recommendation. It is one example of a substantial number of payments that need to be made quickly, and often go to a citizen or business that has never before received a payment from Services Australia. It is an example of when both the government-user and the recipient need speed and payment certainty from the Australian payment system.

We would strongly encourage Treasury to discuss our recommendation with the RBA who regulates the Australian payment system.

The AP+ recommendation

Section 58BW Taking reasonable steps to disrupt scams - Treasury Laws Amendment Bill 2024: Scams Prevention Framework

Paragraphs 1.174, 1.175, 1.179 and page 44: Application of SPF principles, in the Draft Explanatory Materials

Our recommendation arises from the fact that there are multiple different mechanisms and methods⁵ for payments across the different payment rails operating in Australia – each method has different rules (**Scheme Rules**) which ensures that when a customer (government agency, individual or businesses) uses a payment method best suited for that particular transaction – that they have the expected outcome, namely, payment-certainty. For example, real-time payments on the NPP can be made via OSKO, PayID or PayTo. Each of these products operate differently and have different Scheme Rules to ensure the different payment methods run smoothly across the economy and between counterparties. Different payment methods are an encouraged⁶ feature of a competitive, cost-effective and accessible electronic payments system.

³ In 2023, the RBA extended its oversight of the safety and resilience of payment systems from systemically important payment systems to include 'prominent' payment systems. Prominent payment systems are defined as systems where an outage could cause significant economic disruption and damage confidence in the financial system (even when this damage might not result in a threat to financial stability). Currently, the PSB has determined that the NPP, eftpos, Mastercard, Visa and the BECS meet these criteria, (RBA (2024), PSB Annual Report).

⁴ Services Australia Annual Report 2022-23 ([Link](#))

⁵ RBA Speech: *Online Retail Payments – Some Policy Issues*, 18 June 2024, ([Link](#))

⁶ The Payments System Board focuses on fostering competition and innovation in a regulatory environment that supports the safety and security of the Australian payments system.



Scheme Rules for these different payment methods are critical to the trust, stability and orderly operation of the Australian payment system. Counterparties (banks, payment processors, merchants and consumers) rely on the agreed steps and behaviours (as dictated by the Scheme Rules) as much as government-users, businesses or individuals in the economy require the payment certainty.

Therefore, we strongly recommend Treasury remove specific references to 'holds' on payments in the SPF. While we fully support the intent, requiring a bank to specifically place 'a hold' on a payment does not accurately reflect the function and operation of all the different real-time payment methods available in Australia. We seek to avoid the negative economic impact the widespread application of 'holds' across all payment methods will cause. We consider that the SPF legislation over-riding established Scheme Rules will have an unacceptable impact on users, businesses and citizens who require the expected certainty that comes with their decision to use a payment method best suited for that particular transaction.

An SPF obligation on a bank to now place a hold on a payment conflicts with the Rules of certain real-time payment methods (e.g. PayTo). PayTo rules explicitly require payment-certainty and therefore require⁷ the bank to **accept** or **reject** the payment and to inform the counterparties (e.g. the user, merchant, customer) of that outcome. More nuance is needed in the SPF to take into account the diversity in the operation of different payment methods and the fraud controls that AP+, banks and merchants have in place for each payment mechanism. Our recommendation seeks to minimise the disruption and protect third parties, in this case businesses and individuals (See objective in paragraph 1.179 of EM). The proposed principles must allow banks to utilise their real-time fraud monitoring controls and capability to formulate the right response for each payment mechanism to detect, deter and prevent scams across different payment methods, whilst also adhering with their obligations in Scheme Rules, which are critical for the orderly operation of the Australian payment system.

Our recommendation in detail

That the Explanatory Materials (**EM**) be amended to reflect that different payment methods (in our case OSKO, PayID, PayTo, eftpos and BPAY) operate differently, have different Scheme Rules, and each come with different fraud and scam prevention controls and obligations for the scheme members. This is also true for our competitors who also operate card schemes.

AP+ strongly recommend Treasury remove specific references to 'holds' on payments in the SPF and amend the wording to reflect that the regulated entity should in some cases (using PayTo as an example) accept or reject the payment immediately such that the action is always in accordance with the Scheme Rules of the payment method. This is possible as AP+ and banks have real-time fraud monitoring and OSKO, PayID, PayTo, eftpos and BPAY have a liability framework within each scheme. Nuance in the language of the obligation will avoid the SPF disrupting a significant amount of the billions of legitimate payment transactions in the economy or disrupting the orderly and regulated operation of Australia's payment system.

Further, in amending specific references to 'holds', we note that paragraphs 1.174, 1.175, 1.179 and page 44: Application of SPF principles, in the Draft EM, uses language that is too definitive and will likely result in the unnecessary disruption of a significant amount of legitimate payment transactions in the real-economy if adopted literally by the SPF regulated entities who process payments.

The legislation should allow the ability of regulated entities who process payments to use their real-time fraud monitoring controls and capability to detect, deter and prevent scams, while minimising the disruption and protecting third parties who need certainty in the outcome of a payment.

⁷ The PayTo rules states: 'MPS Users need to ensure they have processes in place to accommodate the "fast fail" nature of MPS payment processing. (Rule 3.5.2)'. The AP+ guidance to members is that they should screen the mandate and fast fail (reject/cancel) or accept this. This allow the payment to be real-time. They can also reject the mandate and apply a code that allows them to investigate for fraud and the payment initiator can retry to create the mandate again.



We therefore recommend Treasury consider amending the draft legislation as follows:

Section 58BW - Taking reasonable steps to disrupt scams—civil penalty provision.

The current drafting in Note 1, states: “For example, if a bank has received a substantial number of similar reports of suspected scams, it may be appropriate to pause or delay authorised push payments while the bank investigates the suspected scams.”

Propose to amend to: For example, if a bank has received a substantial number of similar reports of suspected scams, it may be appropriate to introduce appropriate frictions ahead of the final leg/step of a specific payment transaction such that the disruptive actions protect consumers and are also accordance with the scheme rules of the payment mechanism. In some instances, **and dependant on the payment mechanism**, it may, in some circumstances, also be appropriate to pause, ~~or~~ delay, **or reject that an authorised push payments or instruction in accordance with the scheme rules of that particular payment mechanism**, while the bank investigates and actions the suspected scams intelligence.

Context for the proposed amendment: For example, in the case of the PayID Scheme, it is appropriate (in addition to CoP) for a bank to apply warnings and/or frictions as a first-time payment is being set up using PayID. It may also be appropriate, in some circumstances, for the bank to temporarily pause (and the user should typically be made aware of this) the final leg of a small number of new PayID payments because of alerts in their real-time fraud monitoring and controls. That short pause allows a bank to investigate and action any intelligence or satisfy their fraud controls before releasing that payment to the new recipient.

Using the PayTo Scheme as another example, it is appropriate to introduce appropriate frictions (in addition to CoP) well ahead of the final leg of the PayTo payment transaction. In the case of PayTo, this is when the merchant or consumer is setting up the Payment Agreement (the payment mandate) - if the bank has received intelligence related to this merchant and/or their own real-time fraud monitoring alerts them to an issue – the appropriate action, in accordance with the PayTo scheme rules, is to *reject* the mandate (Payment Agreement) and to inform the counterparty of the rejection and that the merchant can try again after a specified time (typically 4 hours), which allows the bank to investigate and action the intelligence. This proactively preserves payment certainty for the consumer, protects against scams and is critical for the orderly operation of Australia’s payment system, where counterparties (banks/users/payment processors/merchants, consumers) each rely on agreed steps and behaviours dictated by the Scheme Rules.

We also recommend that Treasury consider amending the EM:

EM Paragraph 1.174: “introduce holds”

The current drafting of Paragraph 1.174 states “introduce holds”

Propose to amend to: “introduce appropriate friction(s) ideally ahead of the final leg of the payment transaction such that the disruptive action is also accordance with the scheme rules of the payment mechanism and does not unduly disrupt businesses and individuals in the real-economy who need certainty in payments to complete legitimate business transactions, contracts or purchases”.

Context for the proposed amendment: For example, in the case of the PayTo Rules, which seeks to preserve payment-certainty in the Australian economy, a hold is not an appropriate action where a scam is suspected. As per our commentary on Section 58BW, the appropriate action, in accordance with the PayTo scheme rules, is to reject the payment instruction and to



inform the counterparty of the rejection and that the merchant can try again after a specified time (typically 4 hours), which allows the bank to investigate and action the scam intelligence.

We accept a brief 'hold might, on occasions, be appropriate in other payment methods, however in the case of PayTo it is appropriate to reject the payment while the bank investigates. The legislation needs to cover the diversity of payment methods in a modern payment ecosystem, as each operate differently. Different payment methods are a key feature of a competitive, cost-effective and accessible electronic payments system.

EM Paragraph 1.175: “the disruptive action is reasonable and proportionate to the suspected scam”.

Propose to amend to: “the disruptive action is reasonable and proportionate to the suspected scam, in the case of a payment processing that the action is accordance with the scheme rules of the payment type, and does not unduly disrupt the orderly and regulated operation of Australia’s payment system, or unduly disrupt counterparties in that payment system, or disrupt the end-users, businesses and consumers who need certainty in payments to complete a business transaction or purchase ”.

EM: Page 44: Application of SPF principles, Example 1.8 A scam in the banking sector

“Disrupt: ABC bank temporarily adds friction to a high value transfers, including introducing a 24-hour hold of funds.”

For the reasons outlined above, we strongly recommend Treasury remove all the definitive language in this example. The legislation should allow the ability of regulated entities who process payment to use their real-time fraud monitoring controls and capability to minimise the disruption and protect third parties. The language in the example is just too narrow and may result in banks applying a standard 24-hour hold to all transactions across all payment types they deem ‘high risk’ in order to protect themselves from significant liability.

As per our commentary on Section 58BW and paragraphs 1.174 & 1.175 of the EM, this runs counter to the Scheme Rules of different payment methods which are critical to the systemic stability and operation of a modern Australian payment ecosystem, where counterparties (banks/payment processors/merchants) rely on agreed steps and behaviours (as dictated by the Scheme Rules) as much as businesses and individuals in the economy require certainty-in-payments.

Payment industry submissions

AP+ note the submissions of AusPayNet (APN) and the Australian Banking Association (ABA) and are supportive of their proposals and recommendations.

As per those industry submissions, we strongly urge Treasury to re-consider the approach that allows civil penalties to be imposed for a single scam incident, a better approach would be to apply the civil penalty provisions to systemic breaches of a Code or egregious patterns of behaviour. Without change, a likely consequence is that banks will feel compelled to apply broad based frictions to a large number of payments across the economy rather than risk the substantial penalties.

Clarity in the civil penalty regime is necessary to avoid overly conservative responses that risks disrupting the flow of payments in the economy and to avoid disrupting the orderly operation of the Australian payment system. Using PayTo as an example, banks currently monitor trends and if a pattern of scam indicators emerge then the bank typically can take steps to block a particular merchant. Without change to how the civil liability framework operates, this could result in banks blocking a merchant if there was one verified scam incident (which may involve but not be the fault of the merchant who is unaware), rather than following the agreed steps and behaviours (as dictated by the different Scheme Rules) to detect, deter and prevent scams



while minimising the disruption to the orderly flow of digital payments in the economy which the RBA considers critical.

Further, without change, the civil penalty provisions as they stand, are likely to have a chilling impact on the entry of new payment service providers (PSPs), and their ability to partner and compete, which is essential to a modern, efficient and competitive payment system in Australia; as new PSPs (yet to be licenced or subject to the SPF), would introduce new risks to the regulated entities captured in the SPF and expose those regulated entities to substantial pecuniary penalties for a single breach of a civil penalty provision.

Finally, we strongly urge Treasury to progress the finalisation of the payments licensing framework for PSPs, alongside ASIC making minor amendments to the current ePayment Code to carve out scams in line with SPF coming into effect to avoid overlap. The new PSP licensing framework will involve the setting of regulatory obligations for the purpose of managing risks to payments users. These two changes will uplift the obligations on non-bank PSPs who play a significant role in preventing scams. Implementation of the payments licensing framework will provide greater regulatory certainty and address some of the challenges faced by PSPs seeking partners to operate in Australia, thereby supporting competition, innovation, and greater scam protections to consumers.

This Government's coordinated public-private sector approach to scam detection and prevention is most welcome. The data and lessons from overseas show that this 'Australian approach' of early-intervention, information-sharing, and public-private partnerships is the right approach to harden our country against criminals who seek to scam Australians. AP+ fully supports what Treasury is trying to achieve with the SPF, however more nuance is needed to take into account the diversity of regulated payment methods, and to minimise potential disruptions to the economy and the Australian payment system. Thank you for your consideration of our views, we are available should Treasury have questions.

Yours sincerely,

Aidan O'Shaughnessy
Public Policy, Government & Regulatory Affairs.
Australian Payments Plus (AP+)



Australian
Payments
Plus



Australian Payments Plus brings together Australia's three domestic payment organisations, BPAY Group, eftpos and NPP Australia into one entity. Australian Payments Plus which strives to deliver world-leading innovation, excellence in delivery, and customer experiences that delight and inspire us to build a better, stronger and more prosperous Australia. The consolidation of Australia's domestic payments organisations was authorised by the ACCC on 9 September 2021, subject to undertakings, with the transaction completed in early 2022. AP+ shareholders include Adyen Australia Pty Limited, ANZ, ASL, Bank of Queensland Limited, Bendigo and Adelaide Bank Limited, CBA, Citigroup Pty Limited, Coles Group Limited, Cuscal Limited, EFTEX Pty Limited, First Data Network Australia Limited trading as Fiserv, HSBC Bank Australia Limited, ING Bank (Australia) Limited, Indue Limited, Macquarie Bank Limited, NAB, PayPal, Suncorp Metway Limited, Tyro Payments Limited, WBC, Windcave Pty Limited, Wise Australia Pty Limited, Woolworths Group Limited and WorldPay