

9 January 2025

Senate Standing Committees on Economics  
PO Box 6100  
Parliament House  
Canberra ACT 2600



By email only: [economics.sen@aph.gov.au](mailto:economics.sen@aph.gov.au)

Australian Payments Network (AusPayNet) welcomes the opportunity to make a submission to the Senate Economics Legislation Committee's inquiry (the Inquiry) into the provisions of the *Scams Prevention Framework (SPF) Bill 2024* (the Bill).

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. We manage and develop standards and guidelines governing payments in Australia. AusPayNet currently has more than 150 members including financial institutions, payment system operators, major retailers and financial technology companies. Our purpose is to create confidence in payments by: setting enforceable industry standards for a safe, reliable and effective payments system; leading transformation in payments to drive efficiency, innovation and choice; and being the home for ecosystem collaboration and strategic insight.

This submission builds on the feedback that AusPayNet provided in response to Treasury's consultations on mandatory industry scam codes in January 2024, and the SPF exposure draft legislation in October 2024. Those earlier submissions reflected the views of our members, who participated in a consultation process to discuss key issues and provide feedback to inform AusPayNet's responses. While the timing of this Inquiry did not allow us to conduct a new round of consultation with our members, the following response similarly reflects the member views presented in our earlier submissions on the SPF.

## Executive Summary

The proliferation of scams in Australia poses a significant threat to our society, economy, and digital ecosystem. As part of our strategic priorities, AusPayNet is committed to working with members, government, and other stakeholders to help defend the payments system and its users against economic crime. **We therefore welcome the introduction of the SPF Bill and the Government's commitment to establishing a coordinated, cross-sectoral SPF that would help ensure that key sectors in the scams lifecycle have appropriate measures in place to prevent, detect, disrupt, and respond to scams.** This is a crucial step towards protecting Australian consumers and businesses, and creating a more resilient digital economy.

**However, while we generally support the policy intentions underpinning the proposed framework, our members have expressed concerns that some elements of the legislation could have negative implications for competition, efficiency, innovation, and trust in the payments ecosystem.** These unintended consequences would be driven by the combination of several key provisions in the current draft, including:

- the breadth of the SPF Consumer definition;
- uncertainty around understanding and effectively complying with all ‘reasonable steps’ obligations under the SPF principles;
- the narrow safe harbour provisions;
- an onerous liability regime; and
- the intention to designate the banking sector without concurrently designating non-bank payment service providers (PSPs).

Our members have cautioned that these elements of the framework could lead to regulated entities in the payments ecosystem taking overly cautious approaches to their compliance with the SPF, which could affect payment certainty in the real economy, the uptake of real-time payments, and the ability of non-bank PSPs to participate in the payments flow.

While we appreciate that some of our recommendations have been adopted following the consultation on the SPF exposure draft, many of our members’ concerns have not been sufficiently addressed in the current Bill. AusPayNet understands that further detail on some of the obligations under the SPF will be provided in the forthcoming SPF rules and sectoral codes. We look forward to the industry consultations on the rules and codes, and will encourage the inclusion of sufficient detail in these instruments to alleviate some of concerns highlighted in this submission. **In terms of the enabling legislation, we ask the Committee to note the feedback and recommendations in the submission below, and consider whether further refinements should be made to the Bill to enhance the effectiveness and minimise the potential unintended consequences of the SPF.**

## Scope of the SPF

### *Definition of Scams*

AusPayNet understands that the definition of ‘scams’ under the SPF has been made intentionally broad to capture ‘the wide range of activities scammers engage in and their ability to adapt and to adopt evolving behaviours over time’ and across the entire scams lifecycle. The definition’s acknowledgement that scams could lead to a wide range of potential harms and losses (beyond simply financial losses) is also welcome, given the diverse nature and impact of scam activities.

At the same time, our earlier submissions had noted the importance of clearly distinguishing between scams and other types of cyber and economic crime activities, particularly those already covered under other consumer protection laws and regulatory frameworks (including the ePayments Code). This delineation is vital for avoiding regulatory overlap and ensuring clear compliance pathways for regulated entities. **To minimise the potential for regulatory overlap and provide greater legal certainty to regulated entities about the extent and scope of their SPF obligations, we therefore welcome the flexibility provided by the Bill to explicitly exclude certain activities through the SPF rules.** We encourage Treasury to exercise this power to exclude the activities and conduct listed as examples in the Explanatory Memorandum (EM), including hacking, data breaches, and fraud that did not involve any action from the consumer (EM 1.81).

However, we also note that the EM sets a clear intention that *‘The conduct covered within the meaning of scam may interact with other regulatory frameworks, such as the ePayments Code’* (EM 1.46). The EM does further state that *‘The intention is that where there are interactions with other regulatory*

*frameworks, a regulated entity should not be required to compensate for the same loss or damage twice, under two different regimes’.* While this clarification is welcome, the duplication of compensation is not the only issue that should be considered. Where entities face differing obligations under separate regulatory regimes, this could lead to increased complexity and inconsistencies in compliance and enforcement for both regulated entities and consumers. If the potential regulatory scope overlaps continue to be permitted under the SPF, **it will be critical to provide clarity and certainty to regulated entities through the Bill, SPF rules or SPF codes about which obligations under which regulatory regimes should take precedence.**

### *Definition of an SPF Consumer*

**While we support the intention to provide broad customer and small business protections under the SPF, the breadth of the ‘SPF consumer’ definition had raised significant concerns for our members.** The inclusion of Australian residents travelling anywhere in the world, temporary visitors to Australia (including tourists who may only be in the country for a few days), and individuals and businesses with no direct relationship to the regulated entity creates a vast scope of responsibilities that could be challenging to effectively fulfill in practice. It will be particularly difficult for entities to identify and effectively communicate with individuals or businesses they have no formal relationship with, or identify all persons who were SPF consumers that *may have been* impacted by a scam activity (s.58BO(1)). Indeed, many SPF consumers may come to expect that messages from a service they have not engaged with directly may be a scam in itself, reducing the effectiveness of any such communications.

**We therefore welcome the provision in the Bill that will allow the SPF rules to limit the scope of SPF consumers for certain regulated services (s.58AH(4)), and the intention stated in the EM that the SPF Codes could set out more specific obligations that relate to specific classes of SPF consumers as ‘it may not be appropriate or practical to extend certain obligations beyond SPF consumers with a direct customer relationship with the regulated entity’ (EM 1.97).** If the current breadth of the SPF consumer definition is maintained, it will be important to ensure that the sectoral codes circumscribe the obligations on regulated entities and provide detailed guidance on what constitutes ‘reasonable’ actions for protecting any SPF consumer groups that may ordinarily be outside the realistic scope of an entity’s purview. This curtailment and guidance will be crucial for ensuring consistent and achievable compliance, as well as regulatory certainty, across the industry.

### *Designated Sectors*

We understand that the initial sectors proposed to be covered by the framework – banks, telecommunications providers and digital communications platforms – are those that currently see the highest volume of scam activity. However, as acknowledged in the first consultation paper on mandatory industry scam codes, ‘scammers quickly adapt and are likely to shift their focus and activity to less regulated parts of the scams ecosystem’. We therefore welcome the flexibility built into the SPF to enable other sectors to be brought under the framework at a later date.

**We also welcome the provisions that require the Minister to consider and consult on a range of matters prior to designating a sector of the economy to be subject to the SPF (s.58AE). However, we ask that these provisions in the Bill be extended to include consideration of any businesses or services outside the scope of the sector being designated, but associated with or related to that sector.** This should include:

- consideration of the likely benefits and risks to those businesses or services;
- where potential risks are identified, consideration of how these could be mitigated; and
- due consultation with such businesses or services.

This is critically important for the payments industry, which has become considerably more varied, complex and interconnected over the past two decades. In particular, non-bank PSPs now play a significant role in the payments ecosystem, and the payments value chain often includes services provided by both banks and non-bank PSPs. As a result, banks are unlikely to have end-to-end control or visibility over all the steps in the payments value chain, and could be constrained in their ability to mitigate risks to customers (for example, in the case of payments initiated by a third party). This could challenge their ability to effectively comply with certain obligations under the prevent, detect and disrupt principles of the SPF.

AusPayNet understands that Treasury is mindful of the critical role of non-bank PSPs and some of the potential risks of delaying their designation, and therefore intends to capture them under the SPF in a later tranche of designations. However, many of our members had previously expressed concerns that even the temporary exclusion of non-bank PSPs from the SPF could lead to a corresponding 'exclusion' of those PSPs from the payments ecosystem, as a result of banks becoming significantly more risk-averse in their willingness to provide services to and from those PSPs. The voluntary work that many of these PSPs are already doing to help mitigate scams is unlikely to affect this outcome. It is only when non-bank PSPs are captured under both the information- and liability-sharing arrangements under the SPF that this risk will be ameliorated. In our earlier submissions, AusPayNet had therefore noted that designating non-bank PSPs concurrently with banks could help:

- ensure that customers are protected regardless of the payment method or service provider used;
- enable enhanced collaboration on disrupting scams across the entire payments ecosystem, including through the inclusion of all PSPs in information-sharing arrangements;
- prevent a material shift in scam activity to the non-bank segment of the payments industry; and
- ensure that the liability framework recognises that there are many entities that may have obligations to address scam risks within a single transaction flow.

## Overarching Legislative Framework

**AusPayNet broadly supports the overall structure of the proposed SPF.** This includes:

- An overarching legislative framework that sets out the roles and responsibilities of regulators and regulated entities in addressing scams across the scams lifecycle, supported by sector-specific codes that apply tailored obligations and minimum standards for each designated sector. This approach strikes a balance between establishing consistent, economy-wide principles and allowing for practical implementation across diverse industries.
- The framework's built-in flexibility, which should enable it to evolve in response to the ever-changing nature of scam activities. In particular, the ability to designate new sectors and adjust the scope of obligations for certain regulated entities or services, and the relative flexibility of the SPF rules and sectoral codes, are crucial features that will help maintain the SPF's relevance and effectiveness over time.

- The multi-regulator model, leveraging existing regulatory frameworks and expertise. This is a pragmatic approach that should facilitate efficient implementation of the SPF, including through more effective consideration of any existing scam mitigation measures that designated sectors already have in place, as well as any legal or regulatory impediments that may need to be adjusted to support the SPF principles (such as the AML/CTF and privacy regimes).
- The list of SPF principles, which will be critical to ensuring that all regulated entities have appropriate measures for preventing, detecting, disrupting and responding to scams, underpinned by effective governance and information-sharing arrangements.

**However, many of our members had expressed concerns that some elements of the exposure draft legislation could have severe unintended consequences for competition, efficiency, innovation and trust in the payments ecosystem.** Our earlier submissions had asked for consideration of how these concerns could be addressed within the enabling legislation, while maintaining the underlying policy intention and effectiveness of the SPF. While some of the recommendations we provided have been adopted, the comments below reiterate the member concerns that have not been sufficiently addressed in the current Bill.

### *Compliance with SPF Principles*

In line with our earlier submissions, **AusPayNet generally supports adopting a principles-based approach to the SPF at both the overarching and the sectoral levels, supported by appropriate guidance and minimum standards.** We understand that setting detailed requirements on how every entity within the scams lifecycle should address evolving scam risks is unlikely to be effective, and would impose unnecessary regulatory burden on some businesses – or not go far enough for others. It could also limit the scope for entities to develop better practices and be flexible in adjusting their anti-scam measures in response to developments in scam threat vectors, technology, and their business risk profile. We also understand that a flexible, principles-based approach must necessarily involve some level of ambiguity.

**However, the potential for a regulated entity to be in breach of the SPF principles even while fully complying with their sectoral code (EM 1.125) is a significant concern among our members.** Much of the detail necessary for interpreting the application of the SPF principles (particularly the meaning of ‘reasonable’, ‘proportionate’ and ‘relevant’ actions under each principle) is expected to be set out in the SPF rules and codes. However, the drafting of the legislation suggests that even when the codes provide guidance in these areas, a regulator or external dispute resolution (EDR) scheme could determine that the necessary standard required under the SPF principles in a particular situation or for a particular entity differed from the guidance in the code.

This ambiguity creates regulatory uncertainty and will potentially lead to inconsistent enforcement. When coupled with the onerous penalty regime (discussed below), our members warned that regulated entities would be likely to take overly risk-averse approaches to compliance. In the payments ecosystem, this could unwind many years of efficiency and competition gains, dampen innovation, and delay the adoption and growth of certain payment methods (particularly real-time payments). As noted above, such risk aversion could also have an impact on the viability of non-bank PSPs, including through unwarranted service restrictions by banks (such as debanking, blocking payment flows to and from non-bank PSPs, and restricting the use of fintech services for their consumers). More broadly, overly cautious action in the payments ecosystem could have much more significant implications for individuals and the real economy than in other sectors (as detailed below).

Our submission to the exposure draft consultation had therefore urged amendment of the framework so that the sector codes would provide clarity to regulated entities about their obligations under the SPF principles, and thereby provide a 'safe harbour' from breaches of the legislation.

We note that this recommendation has not been adopted, and therefore expect that this will remain a key concern for our members. **While we welcome the addition of the provision detailing matters relevant to an assessment of 'reasonable steps' to comply with the SPF principles (s.58BB), we note that an entity's compliance with the SPF code obligations would be *relevant* to that assessment (s.58BB(e)). This underscores our members' concern. We urge an amendment to the framework acknowledging that compliance with SPF code obligations constitutes 'reasonable steps' in relation to those SPF principles addressed in the code.** We also reiterate our earlier submission that the principles and code should be supported by additional regulatory guidance wherever possible. This could include timely communication from regulators when certain developments (including changes in the scams landscape and/or available technology) might warrant a change in entities' approaches to compliance with the SPF principles and codes. Close cooperation between the regulators and regulated entities will be critical to help provide clarity around expectations for compliance with the various principles-based obligations on an ongoing basis.

**Relatedly, we welcome the commitment in the Bill to reviewing the operation of the SPF after 3 years (s.58GF).** To ensure that the SPF rules and codes remain relevant over time – which is critical to providing at least a minimum level of regulatory certainty to regulated entities – **we encourage this provision to be extended to ensure that all SPF rules and codes would continue to be reviewed on a periodic basis** (at least every 3 years, or as required due to significant changes).

### *Penalty Regime*

During the consultation on the exposure draft, our members had raised strong concerns about the proposed civil penalty regime. Despite the feedback we had provided, the drafting of the legislation continues to enable the proposed civil penalties to be applied in response to individual scams. This creates a significant concern for regulated entities, given the considerable uncertainty that remains around how to achieve full compliance with some of the SPF provisions (as discussed above), the significant volume of individual scam attempts occurring across the regulated sectors each day, and the high maximum dollar amount of the proposed penalties.

We understand that the high maximum penalties are intended to provide a '*meaningful level of deterrence from breaching the relevant SPF principles*' (EM 1.459). However, **we ask that further clarity be provided in the legislation or supporting rules to ensure that only systemic or egregious breaches of the SPF principles and codes would attract civil penalties.** This would be similar to the penalty regime under s. 1317G of the *Corporations Act 2001 (Cth)*.

Reflecting the principles-based nature of the regime, we also recommend that a form of regulatory 'warning' be required to be issued to non-compliant entities prior to seeking a civil penalty order, with guidance on how to uplift their practices and reasonable timeframes for actioning. This approach would be in addition to the alternative enforcement tools provided for in the Bill. Civil penalties should then only be applied in the event that the regulated entity does not heed the guidance within a reasonable timeframe and continues to breach the relevant principle.

## Dispute Resolution

Further to the comments above, fair apportionment of responsibility across the scams lifecycle – and any corresponding civil penalties – will be crucial. **We therefore welcome the addition of provisions in the Bill that will help ensure fair apportionment of liability for any losses or damages across regulated entities (s.58FZF), as well as the intention that the SPF rules will set out guidance for apportioning liability at the internal dispute resolution (IDR) stage (EM 1.262-1.269).**

In line with our earlier submissions, we generally support the intention to authorise a single EDR mechanism across multiple regulated sectors, to help reduce complexity and promote consistency and efficiency in dispute resolution. Close collaboration between the EDR scheme operator and SPF regulators – as envisaged under the proposed information sharing provisions – will be crucial for fair and consistent interpretation and application of the framework across sectors. We note that if the Australian Financial Complaints Authority (AFCA) is authorised as the primary EDR scheme operator, a substantial review of its existing rules will be required to align with the SPF legislation and rules. Due to the significance and scale of these changes, we ask that consideration be given to requiring stakeholder consultation as part of this process.

## Other Provisions

Members have also provided the following feedback on the current draft of the enabling legislation:

- While appreciating the need for regulatory adaptability in the area of scams, too much flexibility can also create uncertainty for regulated entities attempting to prepare for and ensure ongoing compliance. We understand that there is an implicit intention that the Minister or relevant regulator would consider appropriate consultation with the affected industry prior to the establishment or amendment of any SPF codes. To provide further certainty to regulated entities, **we suggest that consultation requirements for sectoral codes be made explicit within the legislation** (similar to the existing provisions requiring consultation on sectoral designation instruments and the SPF rules).
- Given the volume and ever-changing nature of scams, **we encourage ongoing assessment of regulators' capacity and expertise in carrying out their roles under the SPF**, particularly as the framework expands to cover new sectors. As noted above, we also urge close ongoing collaboration between SPF regulators and designated sectors, which will be important for providing regulated entities with clarity around their obligations, and informing regulators' understanding of best practices across industries.
- The obligations under the SPF principles are expected to apply to a sector as soon as it has been designated (and any transitional arrangements are taken into account), rather than after the relevant sector code has been established (EM 1.25). Given our earlier comments about the heightened uncertainty for regulated entities around how to comply with the SPF principles in the absence of a sector code, coupled with the potential consequences of heavy penalties, **we ask that it be mandatory for the Minister to consider the timing gap between designation and the establishment of a sector code when determining any transitional arrangements.**

## SPF Principles

A considerable amount of the detail necessary for interpreting the application of the SPF principles in the Bill (particularly the meaning of 'reasonable', 'proportionate' and 'relevant' actions under each principle) is expected to be set out in the SPF rules and codes. We therefore reserve comment on the appropriateness of these obligations, as they apply to each sector specifically, until the relevant rules and sectoral codes are developed. For the purposes of this Inquiry, this section outlines the key feedback and concerns that members had previously raised about the overarching SPF principles.

### Report

**AusPayNet strongly supports the emphasis on information sharing as a critical tool in combatting scams.** With the growing complexity and sophistication of scams, cross-sectoral and cross-border collaboration and information sharing to identify and disrupt such criminal activity is becoming critically important. We therefore welcome the provisions in the Bill that will enable such information sharing to take place.

AusPayNet acknowledges that standardising SPF reporting requirements across all regulated sectors will help drive consistency and analytical efficiency. We also generally support the approach of prescribing the information that should be provided in scam intelligence reports through the SPF rules (following consultation with designated sectors), *'to ensure the reporting requirements can be quickly adapted as new scam trends emerge'* and *'provide flexibility to adjust reporting requirements as data sharing capabilities mature across different sectors'* (EM 1.184).

However, we do note that the proposed reporting requirements are expected to require significant operational resources and effort from both the regulated entities and the relevant regulators, particularly in light of the large daily volume of scam attempts. This has raised concerns among entities that already have existing scam-related reporting obligations and mechanisms in place, including obligations under anti-money laundering and counter-terrorism financing (AML/CTF) legislation, and industry-specific schemes such as the Australian Financial Crimes Exchange (AFCX). We expect that the effectiveness of existing sectoral intelligence sharing mechanisms like the AFCX could be negatively impacted, as entities would prioritise reporting under the SPF to minimise the risk and consequences of non-compliance with the civil penalty provisions. **We therefore welcome the new provisions in the Bill that would allow the use of authorised third-party gateways, portals or websites for reporting scam intelligence to SPF regulators (s.58BT).** This could help significantly reduce the operational burden for entities of setting up new reporting channels and processes. To further build on this, we ask that the Minister and SPF general regulator continue to consult and work closely with designated sectors to clarify reporting priorities across different regimes, and streamline not just reporting processes but also the information requirements. Frequent changes to the reporting requirements through the SPF rules should also be avoided to the extent possible, as every change generates a significant amount of operational effort for regulated entities.

Relatedly, **the broad powers granted to the SPF general regulator in the Bill to share actionable scam intelligence are generally positive.** However, the fast pace of most scam activities means that the effectiveness of these powers and the broader reporting obligations will depend on the regulator's capacity and capabilities in assessing, investigating and disseminating any intelligence in a timely manner. In AusPayNet's recent submission to the Government's consultation on AML/CTF reforms, we had highlighted that the significant volume of suspicious matter reports (SMRs) that entities are required to submit under the regime has led to many – if not most – of these reports not being



investigated or acted upon. As a result, the SMR process is at risk of becoming merely a costly compliance exercise that provides few actionable insights in the fight against economic crime. To avoid a similar outcome under the SPF, it will be important to ensure that the relevant regulators (or any approved reporting and information-sharing entities) have the necessary capabilities and resources to efficiently analyse the potentially large volume of scams intelligence received and disseminate insights to relevant stakeholders.

### *Disrupt*

**Our members have raised concerns that the Disrupt principle in particular is very broad and introduces considerable uncertainty and risk for regulated entities.** Given the evidential burden placed on entities that take disruption action in response to a suspected scam – and the potential civil penalties faced by entities that do not – it will be important for the sectoral codes to provide sufficient detailed guidance on what may constitute ‘reasonable’, ‘appropriate’ and ‘proportionate’ actions in various scenarios. This guidance should also include consideration of the speed at which regulated entities are expected to act, recognising the trade-off between the rapid nature of some scam activities (particularly at the point of making a payment) and the requirement for entities to gather sufficient actionable intelligence to justify any disruptive actions. Having to carefully assess the balance of probabilities for the numerous scam attempts occurring on (or related to) their service each day will place a significant burden on regulated entities. In line with our earlier comments, this may lead to a precautionary reduction in the efficiency and quality of digital services provided to all customers, in an attempt to minimise the risk of non-compliance with the SPF. This could include, for example, frictions being applied to a much larger volume of real-time account-to-account transactions than would occur otherwise, as a result of banks lowering the threshold risk scores for suspicious transactions.

**While the intention behind the safe harbour principle is welcome, our members are concerned that the provisions in the Bill are very narrow.** The safe harbour protections are vital for providing certainty to regulated entities about their protections while investigating and disrupting scams. However, further clarity is needed on the practical application of the provisions, particularly regarding the assessment of proportionality and scenarios where a consumer insists on proceeding with their original actions (such as making a payment) despite warnings from the regulated entity. **We also question whether the 28-day timeframe is reasonable, and how a regulated entity should balance the requirement to ‘continue to take steps to act on the actionable scam intelligence’ with the absence of any safe-harbour protections after this time (EM 1.170),** if it has not been able to determine whether a scam is being attempted.

Members have also highlighted that some of the disruption obligations may conflict with other consumer protection regimes. This will be particularly relevant for assessing reasonableness and proportionality. For example, the Banking Code of Practice require banks to take extra care of customers experiencing vulnerability; under this Code, the proportionality of blocking a ‘regular’ customer’s mule account on the basis of actionable intelligence may differ to that of blocking the account of a vulnerable customer who would no longer be able to receive government benefit payments as a result. **We therefore encourage introducing relief from potential contraventions of other laws and contractual obligations for reasonable disruption activities (as is provided for reporting activities under s.58BU), or provide additional guidance on how such conflicts should be addressed.**

Relatedly, members have also noted that banks' ability to comply with some of the proposed SPF obligations could be challenged, if doing so would contravene the scheme rules of the various payment systems in Australia. This interaction will need to be considered in the development of the banking sector code and any broader PSP sector codes, in close consultation with the relevant schemes.

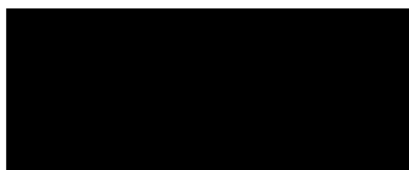
More broadly, it is important to recognise that the real world impact of disruption activities across designated sectors will vary. For example, the impact on a business of having their social media advertisement removed for two weeks while the digital platform investigates its legitimacy would be vastly different to the impact of that business not being able to send or receive a critical supplier payment for two weeks. Blocking or holding payments would have particularly significant implications for transactions such as supply chain payments, investments, and home purchases. Even if a bank is found to have acted reasonably and proportionately in blocking such a transaction, and can therefore rely on the safe harbour provisions (provided within the 28 day timeframe), such actions could have serious real-life implications for the individuals and businesses involved, such as downstream investment losses or the loss of a home purchase contract. SPF regulators will need to give careful consideration to the appropriate balance between risk-based frictions and false positives on genuine transactions, so as not to disproportionately impact the economy.

## Conclusion

AusPayNet welcomes the Government's efforts in developing this comprehensive Scams Prevention Framework. We believe that with further refinement through both the Bill and the supporting SPF rules and codes, the framework has the potential to significantly enhance Australia's defences against scams. We are eager to continue engaging on this issue to ensure that the SPF Bill achieves its policy objectives, while remaining practically implementable across all of the key sectors in the scams lifecycle, and minimising any unintended consequences on those sectors and the real economy.

Please contact Jennifer Le, Head of Government and Regulatory Relations [REDACTED] if you have any questions on this submission.

Yours sincerely,

A large black rectangular redaction box covering the signature area.

Andy White  
Chief Executive Officer  
Australian Payments Network