

4 October 2024

Scams Taskforce
Market Conduct Division
Treasury
Langton Cres
Parkes ACT 2600



By email only: scampolicy@treasury.gov.au

Australian Payments Network (AusPayNet) welcomes the opportunity to respond to Treasury's consultation on the exposure draft legislation for establishing the Scams Prevention Framework (SPF).

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 provided in response to Treasury's earlier consultation on mandatory industry scam codes in January 2024. In developing this submission, interested members participated in a consultation process to discuss key issues and provide feedback to inform AusPayNet's response. References to 'AusPayNet's view' reflect the feedback agreed with these members, with the submission highlighting any key differences in views across our membership base.

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 Government's commitment to introducing a coordinated, cross-sectoral SPF that will 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, we are concerned that some elements of the draft legislation could have significant 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, the uncertainty around understanding and complying with all 'reasonable steps' obligations, the narrow safe harbour provisions, and the onerous liability regime. Our members have cautioned that this 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 fintechs to participate in the payments flow.

To enhance the effectiveness and minimise the potential unintended consequences of the SPF, we propose a number of recommendations for refining the enabling legislation. These include:

- limiting the scope of consumers that regulated entities are obliged to protect under the civil penalty provisions to a more practicable range;
- providing greater certainty to regulated entities about the scope of their obligations through the SPF sector codes and regulatory guidance;
- amending the liability regime to account for the distribution of responsibility across the scams lifecycle, and limiting severe penalties to systemic breaches of the SPF sector codes; and
- considering the impact of the SPF on non-bank payment service providers.

The rest of our submission will provide further detail on the concerns and recommendations noted above, as well as feedback on other key elements of the exposure draft legislation.

Scope of the SPF

Definition of Scams

Our earlier submission noted the importance of clearly distinguishing between scams and other types of cyber and economic crime activities, particularly those covered under other consumer protection laws and regulatory frameworks (such as the ePayments Code). This delineation will be vital for avoiding regulatory overlap and ensuring clear compliance pathways for regulated entities.

AusPayNet appreciates Treasury considering the feedback from the earlier consultation to update the definition of ‘scams’ under the SPF. We understand that the revised definition 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 expansion of the scam definition beyond obtaining only ‘personal information’ or ‘financial benefits’ is also a positive step that reflects the diverse nature and impacts of scam activities. We note that the updated definition relies on the concepts of *deceiving* a consumer into *performing* an action that would result in a loss or harm. While these concepts may be sufficient to distinguish ‘authorised’ fraud from other criminal activity, we welcome Treasury’s intention to provide greater legal certainty to regulated entities about the extent and scope of their SPF obligations by explicitly excluding certain activities (such as hacking, data breaches and unauthorised payments) through the SPF rules.

Relatedly, we are conscious that Treasury intends to carry out a comprehensive review of the ePayments Code as part of the second tranche of PSP licensing reforms. However, we understand that this review is unlikely to take place until at least 2026. Given the importance of clearly delineating between different regulatory frameworks and obligations, we ask Treasury to consider making minor definitional amendments to the ePayments Code in the interim, to ensure that scams – as defined under the SPF – are clearly excluded from the Code. These amendments should ideally coincide with the timing of the banking sector being designated under the SPF.

Definition of an SPF Consumer

While we support the intention to provide broad customer protections under the SPF, the current definition of an SPF Consumer raises significant concerns for our members. The inclusion of Australian residents located 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 (including those to whom the entity does not even know it owes an obligation) creates a vast scope of responsibilities that will be challenging to effectively fulfill in practice.

For example, the exposure draft currently requires regulated entities to take ‘reasonable steps’ to identify *each* SPF Consumer that is or could be impacted by a scam, based on actionable scam intelligence (s.58BO(1)), and provide warnings to *each* SPF Consumer that is at a ‘higher risk’ of being targeted by a scam (s.58BK(2)). It will be very difficult for entities to identify and communicate with individuals they have no formal relationship with (and indeed, many consumers may come to expect that communication from a service they have not engaged with directly may be a scam in itself, reducing the effectiveness of any such warnings).

We therefore ask that Treasury consider the practicality of the proposed definition, and ensure that the sectoral codes provide detailed guidance on what constitutes ‘reasonable’ actions for protecting any consumer groups that may ordinarily be outside the realistic scope of an entity’s purview. This guidance will be crucial for ensuring consistent and achievable compliance, as well as regulatory certainty, across the industry.

In line with our earlier submission, we welcome the inclusion of small businesses in the definition of an SPF Consumer. However, the current criteria of fewer than 100 employees is likely to be difficult for regulated entities to verify and monitor. It may also inadvertently capture entities that have a small number of employees but significant operations (such as ‘small’ fund management companies with large transaction values and volumes). We suggest aligning the definition of small businesses under the SPF with those used in other services regulations to ensure consistency and practicality.

Designated Sectors

As discussed in our previous submission, 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’.

This is incredibly important for the payments industry, which has become considerably more complex and interconnected over the past two decades, with an array of new payment methods and service providers. Non-bank payment service providers (PSPs) in particular now play a significant role in the payments ecosystem. This means that the payments value chain often includes banks and non-bank PSPs, so banks do not have end-to-end control or visibility over all the steps in that chain, and may sometimes 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. Our earlier submission 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.

Added to the other key concerns with the draft legislation noted above, many of our members have 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, until those PSPs can be captured under both the information- and liability-sharing arrangements under the SPF.

AusPayNet understands that Treasury is mindful of the critical role of PSPs and some of the potential risks from delaying their designation, and is therefore intending to capture them under the SPF in a second tranche of designations. Given the lead time that is likely to be required to designate a new sector, and consult on and implement a new sector-specific code, we ask that Treasury consider how to mitigate any potential unintended consequences on non-bank PSPs in the interim.

Overarching Legislative Framework

In line with our earlier submission, 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. The ability to designate new sectors over time, and the relative flexibility of sector codes compared to legislation, are crucial features that will help maintain the SPF's relevance and effectiveness into the future.
- The multi-regulator model, leveraging existing regulatory frameworks and expertise. This is a pragmatic approach that should facilitate efficient implementation, including by enabling more coordinated consideration of any legal or regulatory impediments that may need to be adjusted to support the SPF principles (such as the AML/CTF and privacy regimes), and by allowing the codes to reflect existing scam mitigation measures that the relevant industry already has in place.
- The set of proposed 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, the current drafting of several elements in the proposed legislation have raised some significant concerns for our members, as discussed further below. As noted earlier, these concerns could have severe unintended consequences for competition, efficiency, innovation and trust in the payments ecosystem. We therefore welcome further engagement with Treasury to consider how these concerns could be addressed within the enabling legislation, while maintaining the underlying policy intention and effectiveness of the SPF.

Compliance with SPF Principles

As detailed in AusPayNet's earlier submission, we generally support adopting a principles-based approach to the SPF, at both the overarching, cross-industry level, and the sectoral code level (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. 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.

However, a significant concern among our members is the potential for a regulated entity to be in breach of the SPF principles even while fully complying with their sectoral code. A considerable amount of detail necessary for interpreting the application of the SPF principles (particularly the meaning of 'reasonable', 'proportionate' and 'relevant' actions under each principle) will appear in the SPF rules and codes. However, the current drafting of the legislation suggests that even when the codes provide guidance in these areas, a regulator or external dispute resolution (EDR) scheme could ultimately decide that the necessary standard in a particular situation or for a particular entity had differed from that guidance. This ambiguity could create undue compliance burden and regulatory uncertainty for entities, particularly in relation to taking 'reasonable steps' to meeting the SPF principles, and lead to inconsistent enforcement. Combined with the proposed penalty regime (discussed below), regulated entities are likely to take overly risk-averse approaches to compliance which, in the payments ecosystem, could unwind many years of efficiency, innovation and competition gains. As detailed further below, overly cautious action in the payments ecosystem could have much more significant impacts on individuals and the real economy than in other sectors.

Members have urged Treasury to amend the framework so that the sector codes (and corresponding regulatory guidance) are structured to provide sufficient clarity to regulated entities about their obligations under the overarching SPF principles, to ensure that compliance with a sector code would provide a safe harbour from breaches of the SPF legislation. Noting that the codes themselves would still be expected to contain some principles-based obligations, this may include guidance on where certain entities within an industry may be expected to exceed the minimum standards set out in the code. Additional regulatory guidance should support the codes, including by informing regulated entities when certain developments might warrant a change in their approach to compliance with the SPF on a timelier basis. Close cooperation between the regulators and regulated entities would also help provide clarity around expectations for compliance with the various principles-based obligations on an ongoing basis. We also suggest committing to reviewing the codes on a periodic basis, to ensure that the guidance and minimum standards remain appropriate.

Penalty Regime

Members have also raised deep concerns about the proposed civil penalty regime. The current drafting of the legislation implies that the proposed penalties could be applied in response to individual scams. This creates a significant risk for regulated entities, given the high potential dollar amount of the proposed civil penalties, the considerable regulatory uncertainty that remains around some of the proposed provisions (as discussed above), and the significant volume of individual scam attempts occurring across the regulated sectors each day. We ask Treasury to consider amending the exposure draft such that only systemic or egregious breaches of the 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 suggest that some form of regulatory 'warning' be issued to non-compliant entities in the first instance of a breach, with guidance on how to uplift their practices and reasonable timeframes for actioning the direction. Civil penalties should then only apply in the event that the regulated entity does not comply with the regulatory direction 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. Members have also noted the important of establishing clear, cross-sector guidance on liability apportionment at both the internal dispute resolution (IDR) and EDR levels, to provide greater clarity for regulated entities and support, and support fair and consistent outcomes.

In line with our earlier submission, 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 create uncertainty for regulated entities attempting to prepare for and ensure ongoing compliance. We understand that it is Treasury's intention that the Minister or relevant regulator would consult with the affected industry prior to the establishment or amendment of any sector codes. To provide further certainty to regulated entities, we suggest that this consultation requirement be made explicit within the legislation.

- Given the volume and ever-changing nature of scams, we encourage ongoing assessment of regulatory 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 the industry, which will be important for providing regulated entities with clarity around their obligations, and informing regulators' understanding of best practices across sectors.
- We also expect that it is Treasury's intention that all sector codes would be reviewed by the Australian Competition and Consumer Commission (ACCC) and approved by the Minister, to ensure that they are designed consistently, accord with the SPF principles, and include robust, measurable and outcomes-based obligations for all sectors. However, we suggest that this expectation also be made explicit within the legislation.
- There are some concerns around relatively tight compliance timeframes for certain provisions. Members have suggested that the timeframes in the SPF better align with existing ASIC (or other sectoral regulator's) obligations, to reduce the compliance burden on regulated entities.
- We understand that Treasury intends to carry out further consultation on the transition arrangements for the SPF legislation and codes. As part of this, we note that the obligations under the SPF principles would currently be expected to apply to a sector once it has been designated, rather than after the relevant sector code has been established. Given our earlier comments about the potential unintended consequences of heavy penalties being coupled with uncertainty around how to comply with the cross-sectoral principles, we ask Treasury to consider the timing gap between designation and the establishment of a sector code as part of its consultation on transition arrangements.

SPF Principles

As noted earlier, a considerable amount of detail necessary for interpreting the application of the principles (particularly the meaning of 'reasonable', 'proportionate' and 'relevant' actions under each principle) will appear in the SPF rules and codes. We therefore reserve comment on the appropriateness of these obligations, as they apply to each sector, until the relevant rules and sectoral codes are developed. For the purposes of this consultation, this section outlines the key feedback and concerns that members have raised around certain aspects of the proposed overarching principles.

Prevent

The prevention principle, while crucial, presents some practical challenges in its current form. When combined with the very broad definition of SPF Consumers, the obligation to identify and warn consumers at higher risk of scams could lead to over-notification by regulated entities to minimise the risk of breaching the principle. This could result in consumer desensitisation to warnings, and reduce their vigilance to emerging threats. The sector codes will need to provide clear guidelines on appropriate risk assessment and communication strategies to ensure that compliant warnings remain impactful and actionable for consumers.

We also reiterate members' concerns about the potential unintended consequences of the prevention obligations for non-bank PSPs and similar businesses that rely on connections with regulated entities. Particularly in the payments ecosystem, the absence of clear guidelines could lead to the risk of banks

adopting overly cautious approaches that could stifle innovation or lead to unnecessary service restrictions (including debanking, blocking payment flows to and from non-bank PSPs, and restricting the use of fintech services for their consumers). Aside from the direct impact on the viability of non-bank PSPs' businesses, this could also dampen innovation and delay the adoption and growth of certain payment methods (particularly real-time payments).

Report

AusPayNet strongly supports the emphasis on information sharing as a key tool in combating scams. With the growing complexity and sophistication of scams, cross-sectoral collaboration to identify and disrupt such criminal activity is becoming critically important. However, the reporting obligations as currently drafted raise several practical concerns.

Given the large daily volume of scam attempts, the proposed reporting requirements will require significant operational resources and effort from both the regulated entities and the relevant regulators. We acknowledge that standardising SPF reporting requirements across all regulated sectors will help drive consistency and analytical efficiency. However, this does raise concerns for sectors 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 would be negatively impacted by the new reporting obligations, as regulated entities will prioritise reporting under the SPF to minimise the risk and consequences of non-compliance. We therefore ask that Treasury and the SPF general regulator work closely with affected sectors to streamline reporting processes, clarify reporting priorities, avoid duplication of effort (including by utilising existing sectoral reporting mechanisms wherever possible), and minimise any potential unintended consequences.

Relatedly, the broad powers granted to the SPF general regulator to share actionable scam intelligence are generally positive. However, the fast pace of most scam activity 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 SPF general regulator (or any other approved reporting and information sharing entity) has the necessary capabilities and resources to efficiently analyse any scams intelligence received and disseminate relevant insights to relevant stakeholders.

Finally, we appreciate the broad override of confidentiality obligations for SPF reporting purposes. Given the likelihood that regulated entities will need to disclose personal information under the SPF reporting obligations, we recommend including an explicit reference to the Australian Privacy Principles within the note to section 58BT (alongside the relief from the secrecy provisions in the *Telecommunications Act 1997*), to provide further certainty for regulated entities.

Disrupt

Similar to the prevention principle, members have noted that the proposed disruption principle is very broad and introduces considerable uncertainty for regulated entities. Given the 'evidential burden' placed on entities that take disruptive actions 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 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 scam activities and the requirement for entities to gather sufficient actionable intelligence to justify any disruption 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 also lead to an unwarranted 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, risk-based frictions being applied to all for real-time account-to-account transactions, regardless of the risk score.

Importantly, the real world impact of disruption activities across sectors will vary. For example, the impact on a business from having their social media advertisement being 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 be likely to particularly impact 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 thereby rely on the safe harbour provisions, such actions could have serious real-life implications such as downstream investment losses or the loss of a home purchase contract. Extensive consideration will therefore need to take place regarding the appropriate balance between risk-based frictions and false positives on genuine transactions, so as not to disproportionately impact the economy.

While the intention behind the safe harbour principle is welcome, members have noted that the currently drafted provisions are very narrow, and would not apply to all the potential disruption measures that an entity may need to take. The safe harbour provisions are vital for providing certainty to regulated entities about their protections while investigating and disrupting scams. Further clarity is therefore needed on the practical application of the proposed guardrails, particularly regarding the assessment of proportionality, the consequences of irreversible actions, and scenarios where a consumer insists on proceeding with their original actions despite warnings from the regulated entity. We also question whether the 28-day timeframe is reasonable and, if so, what actions a regulated entity should take after this time if it has not been able to confirm 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 Treasury to consider extending the relief from potential contraventions of other laws and contractual obligations in section 58BT (in relation to reporting

obligations) to reasonable disruption activities, 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 any banking and broader PSP sector codes, in close consultation with the relevant schemes.

Conclusion

AusPayNet welcomes Treasury's efforts in developing this comprehensive Scams Prevention Framework. We believe that with further refinement, particularly in the areas of scope, clarity of obligations, and liability apportionment, the SPF has the potential to significantly enhance Australia's defences against scams. Our members are eager to continue engaging with Treasury to ensure that the framework 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.

As the self-regulatory body for the payments industry, AusPayNet is ready to lead the development of any technical standards for the banking and broader payments industry, where the industry sees a need for such technical standards to effectively comply with any payments-related obligations under the relevant codes.

Separately, we encourage continued focus on improving Australian law enforcement's capacity and capabilities in identifying and stopping the criminals conducting scams, including through cross-jurisdictional collaboration. We also welcome the continued Government and regulatory focus on reviewing and revising other related legislative and regulatory frameworks, including the AML/CTF and Privacy regimes, to ensure alignment and the removal of impediments to effective cross-sectoral and public-private collaboration on reducing the prevalence and impact of economic crime in Australia. We also support the ongoing work by Treasury and the ACCC to improve consumer education and awareness of scams, given the importance of consumer vigilance and responsibility for scams prevention across the ecosystem.

AusPayNet looks forward to continued engagement with Treasury as this important work progresses. Please contact Kateryna Occhiutto, Head of Policy & Insights (kocchiutto@auspaynet.com.au) and Toby Evans, Head of Economic Crime (tevans@auspaynet.com.au) if you have any further questions.

Yours sincerely,



Andy White
Chief Executive Officer
Australian Payments Network