



Scams Prevention Framework – exposure draft legislation

Submission
October 2024

fintechaustralia.org.au

About this Submission

This document was created by FinTech Australia in consultation with its members. In developing this submission, interested members participated in roundtables to discuss key issues and provided feedback to inform our response to the consultation paper.

FinTech Australia and its members particularly acknowledge the support and contribution of our Policy Partner, DLA Piper, to the development of this submission.

About FinTech Australia

FinTech Australia is the peak industry body for the Australian fintech sector, representing more than 420 fintech companies and startups across Australia. As part of this, we work with a range of businesses in Australia's fintech ecosystem, including fintechs engaging in payments, consumer and SME lending, wealthtech and neobanking, the consumer data right and the crypto, blockchain and Web3 space.

Our vision is to make Australia one of the world's leading markets for fintech innovation and investment. This submission has been compiled by FinTech Australia and its members in an effort to advance public debate and drive cultural, policy and regulatory change toward realising this vision, for the benefit of the Australian public.

FinTech Australia would like to recognise the support of our Policy Partners, who assist in the development of our submissions:

- Allens;
- Cornwalls;
- DLA Piper;
- Hamilton Locke;
- King & Wood Mallesons; and
- K&L Gates.

Introduction

FinTech Australia and its members support the Australian Government's proposal to introduce a scams prevention framework (**SPF**) and are committed to helping protect the Australian community and economy from financial crime. We set out below our comments on the draft bill and explanatory memorandum (**Legislative Package**), noting the overarching Act is intended to be supported by rules and mandatory sector-specific codes.

Executive Summary

FinTech Australia and its members support the need to take meaningful, preventative action to address the significant impacts that scams have on the Australian community and economy. We stand behind the SPF's policy aims of introducing a whole-of-ecosystem approach to protect consumers, prevent harm and restore trust in digital services. We also recognise the leading contributions many fintechs have made in detecting and disrupting scam activities, further supporting the effectiveness of these efforts.

However, these aims cannot be achieved by the proposed SPF alone. The SPF needs to be supported by a holistic package of reforms aimed at strengthening the National Anti-Scam Centre, targeted enforcement activity against scammers, enhancing consumer awareness, and encouraging voluntary information sharing both across and within sectors. These reforms should also seek to establish standards and certifications that entities can undertake or obtain to demonstrate their ability and willingness to comply.

To help ensure the effectiveness of the SPF in protecting consumers while minimising unintended negative consequences, FinTech Australia recommends consideration be given to:

- ensuring the SPF accounts for scalable, evidence-based approaches to addressing scams, including the use of regulatory sandboxes to test the impact and effectiveness of the proposed SPF on specific sectors and the overarching aim of consumer protection;
- ensuring obligations on regulated entities are practical, proportionate to the consumer risk, and do not unintentionally hamper competition;
- implementing appropriate guardrails to ensure a consistent approach to interpretation and enforcement of the SPF across sectors, led by regulators who are sufficiently resourced and motivated to action the considerable intelligence that will result from the SPF;
- engaging in a formal consultation pipeline with industry before designating additional sectors and developing sector-specific codes;

- introduction of a more precise definition of "scams", further clarity regarding the extraterritorial application of the SPF and improvements to the practical application of the safe harbour;
- greater clarity on how the anti-scam obligations interact with other laws, such as AML anti-tipping off rules, privacy laws, consumer guarantees and unfair contract terms;
- an in-depth comparative review of equivalent scam prevention regimes and international best practice to inform Australia's approach; and
- thorough consultation with industry as to the appropriate settings for mandatory internal dispute resolution (IDR) and external dispute resolution (EDR) schemes.

FinTech Australia looks forward to continuing to engage with the Minister as the new regulatory framework develops.

Detailed response

1. General considerations

1.1 Achievement of policy objectives

FinTech Australia supports a whole-of-ecosystem approach to combat the significant risk scams pose to the Australian community and economy. At the same time, careful consideration needs to be given to the design of the proposed SPF, as well as other potential complementary reforms. The question of whether consumers will be best served by regulating industry in the manner and to the extent proposed by the Legislative Package is, in FinTech Australia's view, unanswered. However, with some changes to the SPF as proposed in this Submission, together with additional action outlined below, we believe Australia could be well-positioned to take a leading role in effective scam prevention.

There is a critical role to be played by voluntary information sharing (both within and across key sectors), stronger detection and enforcement in respect of known scammers and consumer education¹. A well-resourced and efficient National Anti-Scam Centre is vital to coordinate and manage these initiatives, and to provide consumers with visibility of the steps being taken to protect them from scammers.

Looking at the broader digital environment, a stronger approach is needed upstream to detect and penalise threat actors perpetrating cyber incidents, as well as entities which fail to take basic steps to protect themselves against such incidents. Cyber incidents which result in the exposure of personal information (including phone numbers and email addresses) lay the groundwork for scammers to exploit the Australian community, so mitigating this upstream risk is essential.

¹ One of our members has proposed that the Ministry could take an active role in raising public awareness on scam prevention via a well-resourced, multi-platform public education campaign.

Accordingly, FinTech Australia's members believe the SPF should not be viewed as the sole, or even primary, way of achieving its stated policy objectives. Instead, the SPF needs to form part of a coordinated package of reforms designed to address the confluence of factors that contribute to the prevalence of scams.

1.2 Scalable, evidence-based approaches to addressing scams

FinTech Australia members encourage the use of regulatory sandboxes to test proposed approaches to detection and prevention of scams and the impact of the proposed SPF. This would provide an evidence base to ensure the proposed SPF is effective against its objectives in preventing and mitigating consumer harm, and practically implementable.

For example, a government-funded pilot program or sandbox could be aimed at testing the impact of real-time versus batch reporting for scam detection and could be tested by entities of different sizes and resources. Such initiatives would provide concrete data to shape effective regulation and ensure good consumer outcomes without imposing unnecessary burdens on emerging businesses.

1.3 Consumer protection and innovation

FinTech Australia's members are deeply committed to detecting, remediating and preventing scams. Many members already have dedicated resources in place for these purposes and some are at the forefront of developing the technology to detect and prevent scams. It is therefore critical that the compliance burden of the proposed SPF does not inadvertently hinder the very innovation that the government seeks to leverage in fighting scams.

Australia's fintech community has for many years enabled traditional financial services providers and Australian consumers access to cutting-edge technologies, and can continue to meaningfully contribute to the development of transformational tools for scam detection and prevention if given the opportunity to operate effectively. In paragraph 2.1 of the Submission below, we suggest improvements to the proposed principles-based obligations so that the SPF is effective in protecting consumers and restoring trust, while at the same time ensuring that entities involved in addressing scams can continue to innovate and fairly compete.

1.4 Multi-regulator approach

FinTech Australia broadly supports the proposed approach to enforcement of the SPF. The appointment of sector-specific regulators, who understand the opportunities and challenges within each sector, is preferable to a "one size fits all" model to enforcement. However, careful guardrails need to be established to ensure that this results in an efficient, and fair, regulatory framework.

The appointment of ASIC, ACMA and the ACCC as the proposed regulators for the initial designated sectors is appropriate. However, significant consideration would need to be given to the appointment of sector-specific regulators for any further sector designations. This is particularly relevant should industries such as cryptocurrency fall within future sectoral designations, as it currently lacks centralised oversight by a regulator with knowledge of the sector and its particular challenges and drivers.

All regulators need to be adequately funded, resourced and empowered to undertake their roles, including to effectively action the considerable intelligence which will result from operation of the SPF. In some cases, a differential approach to enforcement across sectors may be justified, based proportionately on the risks to consumers arising within each sector. However, the underlying approach to enforcement and interpretation of the SPF should be consistent across all regulators.

Enabling direct remedies for consumers also raises the potential for courts and EDR schemes in individual disputes and class actions to take different views from those of the regulator which industry will have reasonably relied on in implementing their compliance programs. This needs to be addressed so that compliance measures that are accepted by regulators are not then overturned in the courts or EDR schemes.

2. Specific concerns

2.1 Principles-based obligations

While FinTech Australia broadly supports a principles-based approach to obligations under the SPF, these principles should take into account considerations of proportionality, practicality and should be evidence-driven so that they have the best chance of delivering on their objectives of protecting Australian consumers from scams and mitigating their impact.

Report and Governance obligations

Although reporting and governance obligations have an important place as part of broader oversight of the framework, they should not detract from the critical work of identifying and mitigating scam activity (for example, root cause analysis and remediation). For this reason, reporting obligations should be commensurate with scam activity and consumer risk and have regard to existing compliance measures and systems that are required to be implemented by regulated entities under separate regimes. Otherwise, the reporting obligations risk creating a 'box-ticking' culture rather than encouraging higher-quality, actionable disclosures to regulators.

Accordingly, FinTech Australia recommends that, at a minimum, the SPF provides flexibility for periodic batch reporting of scam-related data, rather than requiring real-time reporting. This would align with how ASIC currently receives complaints data through the six-monthly IDR reporting obligation and ease the compliance burden on entities, while ensuring regulators have

sufficient oversight of scam activity. As mentioned above under paragraph 1.2 of this Submission, testing approaches to reporting and other obligations via sandboxes or pilot programs would help ensure these obligations are evidence-driven, proportionate and more likely to be effective in achieving their aims.

An additional option would be for the framework to clearly define the types of relevant information that regulated services of the entity are required to collect and share - including an explicit meaning of "actionable scam intelligence" under s 58AI of the draft bill.

Prevent and Disrupt obligations

FinTech Australia supports the need for 'Prevent' and 'Disrupt' obligations as part of an effective, coordinated response to scams. However, as currently drafted, they are likely to present some significant unintended consequences. Under the 'Prevent' and 'Disrupt' principles in the draft bill, regulated entities are obliged to, among other things, take reasonable steps to prevent and disrupt scams on or relating to their service. While the relevant sector-specific code may set out what reasonable steps require for that sector, entities may be required (or choose) to go beyond the code to meet this test. FinTech Australia members are concerned that these obligations do not require regulated entities to consider, in determining what constitutes 'reasonable steps', the impact on other parties and specifically the impact on competition. As a result, regulated entities may take unnecessary, overbroad action to restrict services to third parties even where those parties exhibit no particular or proven risk of scam activity. These restrictions could include, for example, debanking fintech businesses, denying consumers access to fintech services, or 'softer' forms of exclusion such as delays on payment transfers, account transaction limits, customer number limits or ad-hoc audit and review frequency and costs. This significantly increases the risk of excluding newer or competitive businesses from designated sectors, without recourse.

FinTech Australia therefore recommends that the proportionality test in s 58BW(3) of the draft bill require regulated entities to consider the impact of "reasonable steps" on third parties that (now or in the future) rely on their services. Steps taken to prevent or disrupt scams must be proportionate to the risk and should not extend further than necessary to address the specific scam threat. This should also be extended to the safe harbour provisions (s 58BZ of the bill).

There also appears no requirement for a regulated entity to be transparent in its determination of what is a "reasonable step" nor does there appear a way for affected customers or financial industry participants to appeal any "reasonable steps" that would adversely affect them. There needs to be a clear, transparent and procedural process which regulated entities can take in relation to addressing scams which does not cause unnecessary harm, loss or damage to another involved entity not at fault.

In this vein, some Fintech Australia members have proposed that the bill provide for a dispute mechanism in which an affected third party can seek to have a regulated entity explain the

rationale for a reasonable step that adversely affects a third party and then if unreasonable or overly broad, have that determination challenged.

Without clear provisions addressing this, there is a risk that obligations in the SPF could unintentionally hamper competition in the sector which would ultimately be to the detriment of both consumers and entities that seek to play their part in tackling scams.

Respond obligations

Mandating the use of IDR and EDR schemes is, in FinTech Australia's view, unlikely to meaningfully contribute to achievement of the Minister's stated policy aims without more detailed consultation with industry. A detailed background understanding of the number and scope of IDR schemes which are currently in place across the proposed designated sectors is key, so that the legislative minimum standard can be fixed accordingly. Many of FinTech Australia's members have robust IDR schemes in place and the proposed requirements may not move the needle for these entities.

Care needs to be taken regarding the designation of an industry-wide EDR. The chosen EDR scheme(s) must be able to sufficiently adjudicate the operations of all entities within the designated sector (and not just the majority). The chosen EDR scheme(s) should also provide affected third parties with the ability to request an explanation and the opportunity to challenge any determination. Further, the prevailing aim of enhancing consumer protection can only be met if the public has sufficient trust in the dispute resolution processes used. We believe failure to ensure this will lead to lack of engagement with the EDR schemes.

Transition period

To give entities sufficient time to prepare, we recommend a transition period of 12 months given the broad nature of the obligations imposed.

2.2 Sector designations and sector-specific codes

We note there remains considerable uncertainty regarding how fintechs, particularly those operating across multiple sectors, will be captured by any future sector designations under the SPF. While FinTech Australia recognises the need for regulation-making powers as a means of flexible, efficient and effective administration of legislation, we encourage the responsible Minister to carefully consider a principled approach to designating regulated sectors and developing sector-specific codes, so that obligations on regulated entities:

- are proportionate and effectively targeted to the scam activity and consumer risk in that sector;
- are clear, practical and technically feasible;
- are scalable and borne by those best placed to control the risk; and

- do not create regulatory overlap for entities who operate across multiple sectors.

Additionally, the Legislative Package makes no mention of the competition implications of the SPF. In designating sectors and developing sector specific codes, we recommend that any approved code under the bill² does not unreasonably restrict competition or unfairly disadvantage existing players, new entrants or smaller players in the market.

Many of FinTech Australia's members supply products and services which are adjacent to traditional financial services and operate horizontally across multiple sectors. It can be difficult to define the boundaries of relevant sectors without detailed knowledge of the industry in question. The designated sectors for the SPF will need to be defined with sufficient clarity to ensure that entities will know if they are bound by the SPF and how the obligations apply to them. The sector-specific codes should therefore also clearly outline the specific requirements for preventing, detecting, reporting, disrupting, and responding to scams for the relevant sector and be developed with regard to those entities necessarily involved in responding to scams - including, for example, payment services providers.

We encourage an ongoing formal consultation pipeline between the government and fintech industry before other sectors are designated within the scope of the SPF. This will enable the fintech ecosystem to provide feedback as the SPF evolves and ensure any regulatory updates or sector designations are developed collaboratively and with practical industry input, as has been the case in the development of the Legislative Package.

2.3 Definition of scams

FinTech Australia members also recommend the definition of “scam” in the Legislative Package be amended to clarify:

- the distinction between fraudulent activity, cybercrime and other relevant forms of wrongdoing, so that it is clear which conduct the SPF is seeking to regulate;
- how scam “attempts” are captured by the definition of “scam” and what constitutes an unsuccessful scam attempt. For example, there may be activities which never reach the stage of a customer trying to fund an ultimately unsuccessful scam or they could be further along in the scam chain; and
- that regulated entities may treat a collection of activities as a single scam based on their common characteristics. Currently, it is not clear if the same pattern of activity which is directed at multiple individuals will constitute the same scam, or multiple scams. We recommend that these activities are able to be aggregated and considered a single scam to allow for meaningful and accurate reporting and for other purposes.

² Treasury Law Amendment Bill 2024 (Cth) s 58CB.

Consideration should also be given to categorising scams based on the nature and severity of the threat (e.g. financial, identity theft, phishing, romance).

2.4 Extraterritoriality

FinTech Australia acknowledges that scammers often do not limit their operations to specific geographic areas, and that any action taken to detect, prevent and mitigate scams cannot apply solely to specific classes of individuals based on location or citizenship status.

However, the proposed extraterritorial reach of the SPF needs to be clarified in the draft bill. It is not clear from the Legislative Package how the SPF will operate in respect of certain financial services products which are commonly used overseas by Australians (often on a short term or transient basis), such as credit and debit cards and other products designed to be used outside of Australia. Regulated entities operating in global markets should not be unduly penalised for scam activities originating outside their control or jurisdiction. One potential solution would be the creation of bilateral agreements or international partnerships to ensure cross-border scam prevention aligns with the SPF's rules.

2.5 Safe harbour

FinTech Australia supports the proposed safe harbour for scam disruption activity where, among other requirements, the regulated entity acted in good faith and in a reasonably proportionate manner (s 58BZ of the draft bill). However, as drafted, the safe harbour poses some practical challenges. First, it seems to only relate to suspected scams and not to confirmed scams, and second, it requires regulated entities to take a definitive view of whether an activity is a scam within 28 days, which may be difficult to do. We recommend that the safe harbour be available to regulated entities who have acted in good faith and in a reasonable proportionate manner (taking into account the impact of reasonable steps) to disrupt the scam activity, regardless of whether the scam is confirmed within the relevant time period. Further, as mentioned above in paragraph 1.2 of this Submission, the impact of reasonable steps relating to the proportionality test should also be considered as part of the safe harbour.

2.6 Interactions with other laws

The obligations imposed by the SPF in relation to scams are potentially in conflict with other laws and which laws are intended to prevail should be clarified. For example, it needs to be clear that actions taken, and contract terms developed, in a good faith attempt to comply with the SPF scams obligations will not:

- contravene anti-money laundering tipping rules, privacy laws or unfair contract terms; and
- constitute breaches of obligations to act efficiently, honestly and fairly, consumer guarantees of due care and skill, and other similar standards.

2.7 Benchmarking against equivalent international regimes

FinTech Australia is aware of other scam prevention regimes which have been adopted internationally. This includes recent legislative developments in the United Kingdom on Authorised Push Payment (APP) fraud and online safety more generally. The UK's The Financial Services and Markets Act 2023 (FSMA 2023) introduces a new mandatory reimbursement scheme for APP fraud. Other notable developments include the European Union's Revised Payment Services Directive (PSD3)³, the Digital Services Act (DSA), and the Digital Markets Act (DMA), which aim to combat online payment fraud and the spread of scams.

FinTech Australia recommends a comparative review of the additional regulatory guidance available to industry under other international mandatory regimes and specific case studies of international best practices that can be applied to the Australian context. This will ensure that Australia adopts a best-of-breed approach and help avoid unintended consequences such as a talent drain or stifled innovation, as has been observed in certain international regimes.

FinTech Australia strongly recommends providing sector-specific guidance that is detailed and regularly updated in consultation with industry stakeholders. This will ensure that regulated entities have a clear understanding of their obligations, reducing compliance uncertainty.

Conclusion

FinTech Australia and its members thank the Treasury for the opportunity to provide their views on such an important suite of issues. We greatly appreciate Treasury's ongoing efforts to engage with the sector, including through the Legislative Package, and over the many past consultations with FinTech Australia and its members. We look forward to continuing to engage as the draft legislation is further considered and consulted on.

³ Directive 2023/0209 (COD) of the European Parliament and of the Council of 28 June 2023 on Proposal on Payment Services and Electronic Money Services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC; Ernest and Young, 'How PSD3 and PSR Will Shape Trends in EU Financial Services', ed Clément Robert and Susan Barton, EY (23 April 2024) <https://www.ey.com/en_gl/insights/financial-services/emeia/how-psd3-and-psr-will-shape-trends-in-eu-financial-service>.