29 January 2024

Scams Taskforce
Market Conduct and Digital Division
Treasury
Langton Cres
Parkes ACT 2600

By email only: scamspolicy@treasury.gov.au

Australian Payments Network (AusPayNet) welcomes the opportunity to respond to Treasury's consultation on introducing a regulatory framework for mandatory industry scam codes.

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.

Introduction

The increasing prevalence of scams in Australia poses a significant threat to individuals, businesses, and society as a whole. 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 scams and other forms of economic crime.

We therefore welcome the Government's commitment to introducing a regulatory framework that will ensure that key sectors in the scams lifecycle have appropriate measures in place to prevent, detect, disrupt, and respond to scams. As noted in the consultation paper, current anti-scam measures vary widely across the scams lifecycle, and efforts to address scams are often siloed within particular businesses or sectors. Subject to our feedback below, AusPayNet considers that the proposed framework will help enable a consistent, whole-of-ecosystem approach to combatting scams that will both reduce the scope for criminal actors to exploit any vulnerabilities and make Australia a harder target for scammers. It will also provide support to the various initiatives already being undertaken by the industry, regulators and Government to reduce scam activity and its impacts.

This submission has been prepared by AusPayNet in consultation with its members. In developing this submission, interested members participated in a consultation process to discuss key issues and provide feedback to inform our response to the consultation paper. Our feedback has also been informed by the insights gained through AusPayNet's work with the industry on combatting economic crime over recent years.

Framework and Principles

AusPayNet is broadly supportive of the proposed guiding principles and the key features of the scam codes framework. These features include an overarching legislative framework that sets out the roles and responsibilities of regulators and entities across the scams lifecycle in addressing scams, supported by sector-specific codes and standards that would apply tailored obligations for each designated sector. Importantly, the proposed framework would also be supported by dispute resolution mechanisms, as well as regulatory enforcement and penalty provisions to encourage broad compliance.

Role of Industry Standards

AusPayNet notes that the overarching cross-sectoral code is intended to be principles-based, enabling the obligations to be 'flexible enough to account for the differing nature and sizes of regulated businesses'. Similarly, the sector-specific codes are intended to allow for more tailored obligations for each designated sector, while still 'providing sufficient flexibility for businesses to determine how best to meet the intent of the obligations considering business size, risk profile and complexity.'

AusPayNet broadly supports this approach. We understand that setting detailed requirements on how every entity within the scams lifecycle should prevent, detect, disrupt and respond to scams 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.

However, some members also consider that in the absence of supporting guidance or standards, some principles-based obligations could lead to inconsistent outcomes or customer experience. To mitigate this risk, such obligations could be supported by detailed standards that ensure an appropriate level of consistency, interoperability, and 'minimum standards' across the industry where required. This could also assist the relevant regulators in monitoring compliance with the codes. As the self-regulatory body for the payments ecosystem, AusPayNet could lead the banking and broader payments industry in developing standards for any payments-related obligations, where the industry sees a need for such coordination to effectively comply with the obligations under the relevant codes.

Additional Guidance

Some members have also raised concerns about several ecosystem-wide and sector-specific obligations for which additional regulatory guidance could help facilitate consistency and reduce uncertainty for businesses within designated sectors. We note that the consultation paper already proposes that 'the ACCC could play a role in working with businesses on their anti-scam strategies to ensure they are fit-for-purpose and consistent with similar businesses in their sector'. Similar best practice guidance – developed by either the ACCC or the relevant sectoral regulator, as appropriate – could assist in establishing an appropriate level of consistency and certainty around matters such as:

- factors that an organisation should account for in assessing its own risks in the scams lifecycle;
- reasonable steps that should be taken to prevent misuse of an entity's services by scammers (particularly noting that the proposed obligation sets a relatively high threshold that requires an entity to take '*all*' reasonable steps to ensure compliance);

- minimum requirements for effective anti-scam systems;
- practical requirements for acting on any scam intelligence received (noting that a large quantity of intelligence may be received through cross-sectoral information sharing channels, and it may be difficult for smaller businesses in particular to act on all of this 'in a timely manner'); and
- whether entities in the scams lifecycle have the right to block any suspected scam transactions to meet the proposed obligation to 'where possible, prevent a consumer being scammed'.

Such guidance may be particularly important for smaller entities who have less expertise in this area, and for whom the proposed penalties for non-compliance would be significant. More detailed guidance could also assist external dispute resolution bodies and regulators in fairly and consistently assessing whether entities have complied with the codes (both within and across sectors).

Definitions

The definition of a 'scam' is one of the most important elements underpinning the framework, as it will determine the scope of criminal activities that entities would be expected to address under the codes. The consultation paper proposes to define a 'scam' as 'a dishonest invitation, request, notification or offer, designed to obtain personal information for a financial benefit by deceptive means'. The paper separately notes that this definition 'is not intended to capture unauthorised fraud, such as cybercrimes that may use hacking, data breaches, and identity theft, that do not involve the deception of a consumer into 'authorising' the fraud'. The distinction between authorised and unauthorised fraud is a key concept in delineating scams from other types of fraudulent activity, and should be explicitly referenced within the definition. In the absence of this clarification, the proposed definition could be interpreted to include all types of fraud and phishing activities.

Distinguishing between enabling criminal activity leading to either authorised or unauthorised fraud will also assist in clarifying the delineation between the bank-specific scams code and the ePayments Code. Several members have highlighted the importance of this delineation, as any potential overlap would introduce significant complexity and ambiguity, and could lead to inconsistent and less timely outcomes for consumers who have lost funds through scams that are similar in substance but have been effected through slightly different mechanisms. These members have suggested that clear guidance on the types of criminal activities that fall under each code would be beneficial, and that the ePayments Code (which is expected to be reviewed in the coming years) should explicitly exclude all scams covered under the scam codes framework.

We have also received feedback that the use of the term 'personal information' in the definition could limit the Codes' applicability. For example, scams impacting businesses (as opposed to individuals) may not be captured under this definition. There are also instances of scams that seek to obtain access to information such as login credentials for banking applications, which may also not meet the definition of 'personal information'.

In addition to refining the overarching definition of a 'scam', we also encourage Treasury and the relevant regulators to establish a broader, standardised scam-related taxonomy that would be used across all sectors in the scams lifecycle. Clear and consistent definitions will be critical for effective information sharing and analysis.

Scope of Designated Sectors

The consultation paper explains that, for the purposes of the framework, entities within the Telecommunications sector would be defined as 'Carriers and Carriage Service Providers' under the *Telecommunications Act 1997*. We note that this definition includes Internet Service Providers (ISPs). The consultation paper also notes that a coordinated effort must be made to 'prevent scammers from contacting consumers through key communications channels', that 'online scam content can take many forms across a range of services, including… emails', and that 'for the purposes of the Framework, 'digital communications platforms' covers all digital platforms that provide communications or media-type services that can be exploited to share [scam] material, including… online services whose primary function is to enable interaction between two or more end-users'.

Contrary to this, our understanding from recent discussions with Treasury is that ISPs and email service providers are not currently intended to be captured within the proposed Telecommunications and/or Digital Communication Platforms sectors. Given the prevalence and impact of scam emails and websites, we strongly encourage the inclusion of ISPs and email service providers within the scope of the initial set of sectors to be designated under the framework.

Scamwatch data show that email-based scams led to over $75 million in losses in 2023 (the third-highest scam delivery category by value, and the second highest by number of scams reported), while website-based scams led to losses of almost $70 million (the fourth-highest category by value).[1] The inclusion of these entities would therefore have a significant positive impact on limiting harms to consumers and businesses across Australia.

As part of this, we would recommend including obligations in the relevant sector-specific codes to ensure the timely blocking or takedown of malicious websites and emails (as has already been done with SMS and phone calls). Cross-sectoral information sharing on malicious websites should also be enabled under the proposed ecosystem-wide obligations. We understand that this may be a significant step up for some businesses within the Telecommunications and/or Digital Communications Platforms sectors, and the existing *Reducing Scam Calls and Scam Short Messages Code* may require some significant revisions to account for the inclusion of these entities. However, excluding these businesses from the scam codes framework would leave two of the key channels already being used by scammers unaddressed, and greatly reduce the effectiveness of the intended whole-of-ecosystem approach.

Inclusion of Other Sectors

More broadly, we understand that the initial sectors proposed to be covered by the framework – banks, telecommunications providers and digital communications platforms – are those that are considered to be the most targeted by scammers. However, some members have suggested that all key sectors within the scams lifecycle should be designated from the outset. As noted in the consultation paper, 'scammers quickly adapt and are likely to shift their focus and activity to less regulated parts of the scams ecosystem'. Given the lead time that is likely to be required to designate

[1] Scamwatch Scam Statistics (accessed 22 February 2024)

a new sector, and consult on and implement a new sector-specific code, delaying the designation of other important sectors could lead to a significant increase in scam activity in those areas.

In particular, a few members have argued that non-bank payment service providers (PSPs) should be subject to mandatory scam codes alongside banks. Developments in the payments ecosystem over the past two decades have meant that banks often no longer have end-to-end visibility or control over many payments, 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). Including PSPs under the scam codes framework would 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, and help prevent a material shift in scam activity to the non-bank segment of the payments industry. This would also ensure that the liability framework recognises that there are many entities that can have obligations to address scam risks within a single transaction flow, and would be consistent with Treasury's proposal under a concurrent consultation to mandate compliance with the ePayments Code for all PSPs.[2] Developing the two codes at the same time would also recognise that while some sector-specific obligations would need to be tailored to account for the different nature of the businesses and activities across these two sectors, there may be some obligations that should apply equally to both banks and non-bank PSPs. Joint consultation that spans both sectors may therefore be beneficial in developing the two sectoral codes.

Information-sharing arrangements

AusPayNet supports the proposals to improve information-sharing arrangements across the scams lifecycle. With the growing complexity and sophistication of scams, cross-sectoral collaboration to identify and disrupt such criminal activity is becoming increasingly important. However, there are several challenges to effective information-sharing arrangements that need to be considered.

One of the challenges arises from existing privacy laws and tipping-off provisions in legislation. We note that the Government is currently undertaking a review of Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime. In our submission to the consultation on the AML/CTF reforms in June 2023, AusPayNet had expressed support for reviewing the tipping-off offence to enable private-to-private pre-suspicion information-sharing, which would remove a significant barrier to the early detection and disruption of economic crime in Australia. Relatedly, we also supported the proposal to provide statutory exemption for regulated entities when assisting an investigation of a serious offence, to further promote and enable more efficient cross-sectoral collaboration on combatting economic crime. The outcomes of the AML/CTF review will be an important factor in determining the scope of information-sharing arrangements under the scam codes framework.

Similarly, members have queried how the proposed information-sharing arrangements would interact with existing privacy laws, and how customers may be impacted by any information shared about them by an entity seeking to comply with its obligations under the scam codes.

The consultation paper also highlights that the National Anti-Scam Centre (NASC) is currently building out data-sharing capabilities to enhance scams information-sharing across the ecosystem. We encourage Treasury to consider options to leverage existing arrangements where appropriate – such

---

2 Consultation on Payments System Modernisation (Regulation of Payment Service Providers)

as the Australian Financial Crimes Exchange (AFCX) platform – to reduce duplication and operational burden on industry. This would be in line with one of the NASC's overarching principles of 'don't duplicate, integrate'.

Given the significant operational burden that enhanced reporting and information-sharing could impose on regulated entities, and particularly on smaller businesses, further consideration should also be given to prioritising between the different reporting and information-sharing requirements. For example, while recording and reporting data on the number of scams prevented could be useful for understanding the impact of the regulatory framework and whether further changes are required, this may be a lower priority to impose on smaller entities than sharing intelligence about suspected scam activity.

Dispute resolution

AusPayNet supports the stated intention in the consultation paper that internal and external dispute resolution 'operates coherently across the system… so that consumers are not referred back and forth between businesses and different EDR schemes'. We also understand that the proposed framework largely aims to utilise existing industry and regulatory arrangements wherever possible (including existing dispute resolution requirements and schemes within each of the designated sectors).

However, some members have expressed concerns about aspects of this approach. In particular, they recommend that a single external dispute resolution mechanism be implemented to manage complaints across all sectors within the scams lifecycle. This would be expected to reduce complexity, limit potential inconsistencies, and improve customer outcomes under the framework.

Conclusion

AusPayNet appreciates the opportunity to respond to Treasury's consultation on introducing a regulatory framework for mandatory industry scam codes. This framework will be critical to enabling a whole-of-ecosystem approach to addressing the growing threat of scams to individuals and businesses in Australia, and making Australia a harder target for scammers. We look forward to continuing our engagement with Treasury as it progresses this work over the coming months. 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