29 January 2024

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

Classification: Public

Via submission portal:
https://app.converlens.com/treasury/scams/consultation-industry-codes

Cuscal consultation submission on the proposed features of the Scams Code Framework

Cuscal Limited (**Cuscal**) welcomes the opportunity to make a submission to Treasury on the proposed features of the Scams Code Framework (**Framework**), which would introduce obligations for the private sector in relation to scam activity, with a focus on banks, digital communications platforms, and telecommunications providers.

Background to Cuscal

Cuscal is an Authorised Deposit-taking Institution (ADI) that provides payment and regulated data services to banks, FinTech and 'PayTech' enterprises and corporates, enabling those clients to provide services to their end customers. As a B2B provider, Cuscal facilitates its clients' connections to the infrastructure layer of the Australian payments market. Cuscal has been operating since the 1960s (through its earliest predecessor) and has evolved from its origins as an aggregator of services for mutual ADIs to a manufacturer of products and services in its own right, and a trusted payments solution provider across a diverse client base.

Cuscal has Board representation with Australian Payments Plus (NPPA, BPAY, Eftpos) the Australian Payments Network and participates in numerous industry committees and forums.

As payment methods evolve, so do the efforts of criminals in their attempts to defraud businesses and consumers. Cuscal is committed to working with clients, Government, and other stakeholders to help defend the payment system against fraud, including scams.

Introduction

Subject to the feedback enclosed in this submission, Cuscal is supportive of the proposed Framework, which aims to establish a strong, whole-of-ecosystem regulatory Framework. This Framework incorporates a co-ordinated effort between the Government, regulators, and the private sector to deal with scam threats.

1. Framework

- In general, we support the proposed principles and key features of the Framework. This includes the proposal to implement an overarching legislative Framework with cross-sectoral, principles-based obligations. These obligations need to be supported by sector-specific codes and standards that would apply tailored obligations for the focus sectors.
- However, we note that the National Anti-Scam Centre (**NASC**) is still building out data-sharing capabilities. While the Australian Financial Crimes Exchange (**AFCX**) already helps coordinate some intelligence and data-sharing activities related to financial crime, Cuscal encourages Treasury to consider options to leverage such existing platforms rather than duplicating efforts, in line with one of NASC's overarching principles of avoiding duplication in favour of integration. For example, Treasury could consider mandating membership of the AFCX to establish a central data sharing body. Adequate funding, and Governance arrangements will be required for the relevant agency to process and analyse the incoming data. Standards for data quality submitted to the relevant agency must also be enforced. Creating multiple agencies receiving such reporting runs the risk of diluting their capabilities as each will require separate funding and compete for the same specialised workforce.
- To minimise reporting burdens, the Framework should determine who should receive the relevant data detailing the scam-related intelligence, to avoid needing to notify multiple authorities, e.g., AFCX, NASC and AUSTRAC.
- Further clarity is required on how data sharing will be facilitated by the Framework to allow for timely and secure data flows. These flows should not be unnecessarily hindered by contradictory legislative requirements (e.g., Principle 6 of the *Privacy Act 1988 (**Privacy Act**)* and the tipping off provisions of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (***AML/CTF Act***)).
- We also note that while sharing data with law enforcement has been considered under the Framework, the role of law enforcement in combating scams, based on this intelligence is not mentioned. To ensure that the Framework truly is 'whole-of-ecosystem' and to achieve the intended outcome of making Australia a harder target for scams, it is vital to have adequate consequences for the criminals. Such enforcement activities should be publicised as part of the broader public deterrent campaigns. While the Joint Policing Cybercrime Coordination Centre (JPC3) has been established, its responsibilities should be outlined within the Scams Code Framework, with adequate funding and resources to enable them to act on the intelligence provided to them.
- Similarly, the role of payment schemes has not been considered as part of the Framework. Schemes are well placed to identify variations in behaviour/volume/value trends and actions being taken by one participant that are inconsistent with other participants. This data should also be leveraged and provided to the central data agency for analysis and actioning. For example, CAMT is the agreed industry method for raising an NPP disputed transaction – we note that one major bank is raising 80% of the disputes in CAMT and another major is only raising 2%, this is likely to indicate a process or compliance issue. The NPP should be expected under the Framework to track and report such trends.
- Greater clarity is also required around timing for the various proposed activities e.g., dealing with identified/suspected scams, sharing information, maintaining records etc.
- Treasury should also include its intended approach to liability as part of the Framework. Cuscal is not supportive of the shared liability model. While this is reassuring for consumers, it can attract, and lead to an increase in, scams. Cuscal is in principle supportive of Singapore's waterfall approach, but further clarity should be provided around how this would be implemented under the proposed Framework. For example, who would make the determinations and how will this process fit between the broad and sector-specific codes? If an inter-sector approach is adopted, the ACCC would be the logical regulator, but it would need to be prepared (funded and resourced) to support the influx of cases that it would have to oversee.

2. Definitions

- 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". We understand that the intended breadth of the definition is to ensure it is relevant to the diverse sectors the Framework will apply to and is intended to capture not just payment but also data-gathering related activities, which enable the authorised payment/scam. Nevertheless, from a banking perspective, a scam is a subset of fraud in which a criminal uses deception to trick victims into authorising a payment. This is distinct from unauthorised fraud (covered under the ePayments Code). Cuscal believes that the global terminology of "authorised push payment" may be more appropriate. It may also be possible however to incorporate greater definitional clarity as part of the proposed supporting sector-specific Codes.

3. Sector-specific codes

- The consultation paper sets out potential obligations around scams prevention, detection, disruption, and response that could apply to each of the three sectors initially designated under the new Framework – banking, telecommunications, and digital communications platforms. The consultation paper only seeks preliminary feedback on these obligations, noting that the sector-specific codes will be developed through subsequent targeted consultation. Our preliminary assessment has, therefore, focused on the broad principles underlying the sector-specific codes.
- At this stage, the Framework focuses on three key sectors- banking, telecommunications, and digital communications platforms. To ensure a 'whole of ecosystem' approach, the Framework should solve not just for inter-bank transactions but consider other existing as well as emerging sectors, e.g., Payment Service Providers (**PSPs**).
    - Cuscal recommends that the proposed Scams Code Framework be reviewed against the uplifted definitions proposed in the Payments System Modernisation (Regulation of Payment Service Providers) Consultation, to ensure the Framework considers relevant payments intermediaries, and the level of friction, restriction and control that can and should be applied by such intermediaries in the context of the overarching payments ecosystem.
    - Cuscal notes that there is potentially a key gap posed by PSPs (for example through wallet-to-wallet transactions) and the merchants to whom they provide services (such as digital currency exchanges and international remittance agents). These merchants and PSPs that facilitate their activities should be included as a sector in the Framework at its inception and not as a 'future sector'. Treasury should give some thought specifically to what obligations could be imposed to ensure they can force a recouping of funds where a scam is involved. If this gap is not addressed as part of the proposed Scams Code Framework, the industry is likely to see a drastic increase of scam activity in the space.
    - For a 'whole of ecosystem' approach, Treasury should also further consider how the Framework will apply to the merchants to whom these PSPs provide services to, such as digital currency exchanges and international remittance agents.
    - Even if Treasury intends to adopt a risk-based approach by prioritising the three key sectors, a timeframe for implementation should be developed now for other in-scope sectors to ensure these loopholes are addressed within a specified timeframe and to allow the industry to prepare for the incoming changes.
- Cuscal would like to see greater clarity around the expectations in relation to blocking/disabling scammer accounts – timing, method, and approach in relation to potential tipping off provisions. 'Safe harbour' type protections against liability to other parties in the payments chain (i.e., account holders, payers, other institutions) for suspensions should also be considered as part of the Framework, if done in accordance with scam strategy and based on reasonable grounds.

- Further clarity is also required on how the Framework will ensure consistency of implementation of the sector-specific and overarching obligations. For example, a good deal will depend on technical implementation and adequate standards should be developed for each sector. Given AusPayNet's work on submitting to become an authorised standard-setting body (**ASSB**), they may be able to support the development of relevant technical standards for the payments ecosystem.
- Cuscal also recommends the following additional requirements be added to the Possible bank-specific obligations under the 'Detection and Disruption' sub-header:
    - A bank must implement robust customer onboarding processes to prevent the opening of accounts specifically for the purpose of receiving funds proceeding from a scam, whether directly or further downstream as part of attempts to launder scammed funds.
    - A bank must implement processes to identify and block payments to accounts opened specifically for the purpose of receiving funds proceeding from a scam, whether directly or further downstream as part of attempts to launder scammed funds.
    - A bank must implement processes to identify and block payments to existing accounts where transaction activity indicates that the account may be being used for the purpose of receiving funds proceeding from a scam, whether directly or further downstream as part of attempts to launder scammed funds.

4. Education

The consultation paper notes the importance of consumer education but provides little guidance on what exactly should be done by the sectors to reach consumers and what topics should be covered. Greater clarity is needed around expectations to ensure this is not a set and forget exercise and that all consumers get a consistent level of education no matter their provider. Scammers monitor the indicators consumers are educated to watch out for and adjust their approach in response. Accordingly, the content will need to be updated on an ongoing basis. Cuscal recommends that a centralised education campaign (e.g., through NASC) be considered as part of the Framework.

5. Benchmarking

Cuscal recommends that Treasury consider what guidance can be provided to the in-scope sectors to allow them to improve and uplift their approach over time. Some form of benchmarking should be incorporated into the Framework to measure and report on maturity levels and how sector participants are performing compared to their peers. This will encourage continuous improvement and help ensure processes and controls are uplifted as scam activity changes over time.

6. Compliance Costs

The Framework proposes significant compliance obligations. It is important that any obligations which rely on reference to textually subjective tests (such as a requirement to 'take all reasonable steps' to implement or prevent something) are clear and readily addressable by market participants. Cuscal recommends that Treasury undertake further targeted analysis and consultation to better understand the costs of the proposed legislation to the entire ecosystem, including the in-scope sectors, the nominated agencies, government and regulatory departments, and law enforcement.

In closing, we trust that our response will assist Treasury in formulating the features of the Scams Code Framework, and we look forward to further discussing our submission with you.

If we can be of any further assistance in the interim, please feel free to contact me at kmckenna@cuscal.com.au

Yours sincerely,

Kieran McKenna
Chief Risk Officer