Deloitte.

Scams – Mandatory Industry Codes

Deloitte Response to Scams Taskforce Consultation Paper

29 January 2024

Deloitte.

Deloitte Touche Tohmatsu
ABN 74 490 121 060
Quay Quarter Tower
50 Bridge Street
Sydney NSW 2000
Australia

Tel: +61 2 9322 7000
www.deloitte.com.au

29 January 2024

Scams Taskforce
Market Conduct and Digital Division
The Treasury
Langton Crescent
PARKES ACT 2600

Submission via Online Portal

Dear Assistant Treasurer, the Hon Stephen Jones MP, and
Minister for Communications, the Hon Michelle Rowland MP

Deloitte response to consultation paper on Scams – Mandatory Industry Codes

We are pleased by the recent release of the Consultation Paper on Scams – Mandatory Industry Codes (the "Draft Code", subject to consultation). The Draft Code is a welcome, necessary and substantial step forward in Australia's response to societal harm from scams.

Deloitte is committed to playing a role in Australia's initiative to reduce societal harm from scams. We have an experienced team consisting of local and global subject matter experts in fraud, identity, financial crime, cyber, privacy and customer response and outcomes who are focused on minimising the impact of scams. Each of these domains are pertinent not only in their direct relevance to combatting scams, but also with respect to the lessons learned across their maturity journeys.

With that background, we offer in our response a number of insights and opportunities that we observe to implement the Draft Code in a manner that will drive an effective and efficient cross-sector response to scams.

We would welcome the opportunity to further discuss any of our observations as part of the continued consultation process, including access to any of our local and global subject matter experts.

Kind regards

Lisa Dobbin
Partner | Australia and APAC Financial Crime Lead
Deloitte Touche Tohmatsu

Jonathan Perkinson
Partner | Deloitte Regulatory Operate
Deloitte Touche Tohmatsu

EXECUTIVE SUMMARY

At its core, the Draft Code obligates impacted businesses to gather, share and act on scam intelligence. Scam intelligence will be generated through analytics, information sharing across the ecosystem, and consumer reports and complaints, among other sources.

The Draft Code additionally obligates impacted businesses to maintain an anti-scam strategy, educate its workforce, implement a range of customer protective features, and provide access for its customers to user-friendly and supportive avenues when they have been impacted by a scam attempt, whether successful or unsuccessful.

The Draft Code solicits feedback in the form of 45 questions across topics on the framework, definitions, principles-based obligations, anti-scam strategy obligations, information sharing requirements, consumer response, sector-specific codes, and approach to oversight, enforcement and non-compliance. We believe the businesses that will be subject to the Draft Code are well placed to respond to those questions.

With Deloitte's considerable experience supporting regulatory change in Australia and globally, we have drawn on our domestic and global experiences to put forward observations and recommendations aligned with four topics that we believe will further enhance the Draft Code.

Topic 1: Cross-sector regulatory change

We support and find necessary the cross-sector approach of the Draft Code. We believe there is an opportunity for the Draft Code to consider the frameworks required to deliver cohesive and coordinated regulatory change across sectors, including consideration of integration with a unified Economic Crime regime.

Topic 2: Model for intelligence sharing and taking action on intelligence

Intelligence sharing is a cornerstone of the Draft Code, but its scope, speed and interrelationship with existing regulatory intelligence-sharing regulations and protocols may pose challenges. We suggest the Code address the need for a unified cross-sector scheme for intelligence sharing, including standardised taxonomies, privacy management, and system architecture. Moreover, formal clarity on intelligence thresholds and scope for taking action is essential to balance effectiveness and avoid unintended consequences.

Topic 3: Reimbursement of customer losses

The Draft Code rightly emphasises businesses taking reasonable steps to protect customers and acting promptly on scam intelligence. We know from our global experience that clear liability levels deliver the certainty required for operational planning, infrastructure investment and consumer reimbursement strategies. We see an opportunity for the Draft Code to introduce outcomes-based guidelines for reimbursement, considering various perspectives and striking a balance to incentivise customers and business stakeholders across the ecosystem to combat scams collectively.

Topic 4: Governance

We see an opportunity for the Draft Code to incorporate principles for good governance into its suite of obligations, which we believe to be key in keeping anti-scam strategies aligned with a landscape that can change rapidly.

On balance, we believe the Draft Code introduces sensible, straight-forward and appropriate obligations. We believe that when met they will result in an Australia that is far more resilient to scam activity.

TOPIC 1: CROSS-SECTOR REGULATORY CHANGE

Linkage to related Consultation Paper questions:

3. Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?
7. What impacts should the Government consider in deciding a final structure of the Framework?
16. Are the obligations set at the right level and are there areas that would benefit from greater specificity e.g., required timeframes for taking a specific action or length of time for scam-related record-keeping?

The Draft Code applies to the banking, telco and social media sectors as the primary sectors whose infrastructure is misused by scammers. The Draft Code includes a placeholder for future sectors which the Draft Code states may include superannuation, digital currency exchanges, other payment providers and online market places.

We believe the Draft Code's application across sectors is necessary and appropriate. We recognise though that cross-sector application adds to the number of regulators and existing regulatory regimes, and as a result, the complexity, that the Draft Code must navigate. Furthermore, the growing level of urgency around scams calls for the Draft Code to be progressed at speed.

Framework for Driving Cross-Sector Regulatory Change

Implementing regulatory change at speed within a single sector is a challenge, and that challenge will be exaggerated by implementing the regulatory change called for by the Draft Code across three initial sectors. It is foreseeable that a strong framework will be required to keep pace across sectors with active regulation and communication, and with contingency planning in place so that a lag in one sector will not slow the full national response down.

Whist it would not necessarily feature within the Draft Code, we believe a sufficiently resourced and task-oriented regulatory body with clear jurisdiction and access to enforcement vehicles will be called for to drive further development and implementation of the Draft Code across sectors. Such a body could also play a role in reconciling tensions and overlap with other existing sources of regulatory guidance and also ensure that all eco-system participants are adopting required infrastructure in a unified manner.

Strategic Vison for Economic Crime at the Regime Level

The complexity outlined in the Draft Code underscores the critical need for a unifying Economic Crime strategy at the national level. To fortify Australia's defences against scams and financial crimes, we believe that a 'whole of system approach' is called for. Such an approach should encompass diverse measures and harness the commitment and investment of the private sector. Drawing inspiration from the UK's Economic Crime Plan[1], we advocate for Australia to develop a shared strategic vision inclusive of scams, accompanied by a roadmap and clear measurement mechanisms. If desired and as advocated recently by a former AUSTRAC Chief Executive Officer[2], Australia could also develop a dedicated fraud sub-strategy to supplement the broader Economic Crime strategy.

The UK's approach, as outlined in the Economic Crime Plan, has yielded significant success. By encouraging joint efforts between public and private sectors, the Plan has fostered collaboration, commitment, and a shared vision. The strategic framework, supported by plans, processes, common Key Performance Indicators (KPIs), and a roadmap, has enhanced collective understanding and

[1] 'Economic crime plan 2019 to 2022', HM Treasury and Home Office. 12 July 2019, viewed on 23 May 2023, https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022.

[2] https://complyadvantage.com/insights/former-austrac-ceo-urges-holistic-national-anti-fraud-strategy/

accountability. Australia stands to gain substantially by adopting a similar model, fostering targeted action, investment, and the exchange of essential skills and infrastructure.

While acknowledging the time-consuming nature of implementing a strategy of this magnitude, the potential benefits are substantial. Genuine collaboration between public and private sectors requires legislative changes, but the long-term outcomes promise a considerable uplift in Australia's economic crime regimes. By investing in a shared strategic vision, Australia can proactively combat scams, improve risk identification and management, and fortify the collective resilience against evolving threats in the realm of economic crime.

Augmentation of the Code with Regulatory Guidance

Reflecting on other regimes that exist, there is a need for legislation to be supported and elaborated on through comprehensive guidance to assist organisations in operationalising frameworks. We believe it makes sense for legislation to define specific requirements such as regulatory reporting obligations and timelines. To complement legislation, there is a role for additional guidance to expand upon legislation for the benefit of covered organisations to provide guardrails for compliance and setting expectation levels (e.g. by providing practical examples of how "reasonable steps" or other qualitative terms should be interpreted).

TOPIC 2: MODEL FOR INTELLIGENCE SHARING AND TAKING ACTION ON INTELLIGENCE

Linkage to related Consultation Paper questions:

17. Do the overarching obligations affect or interact with existing businesses objectives or mandates around efficient and safe provision of services to consumers?
18. Are there opportunities to minimise the burden of any reporting obligations on businesses, such as by ensuring the same information can be shared once with multiple entities?
29. Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?

Efficient Model for Sharing of Intelligence

The Draft Code commendably mandates bilateral and multilateral sharing of scam intelligence among businesses, regulatory bodies, and scam prevention organisations. The sharing of risk intelligence at all levels is likely to promote a focus on broader outcomes including enhanced cooperation, increasing the possibility of recovery of the proceeds of scam activity as well as enabling the timelier awareness of and reaction to emerging criminal activity.

Recognising the centrality of swift and robust intelligence to combat scams, the Draft Code emphasises the diverse sources contributing to this intelligence reservoir, spanning internal risk analytics, third-party technologies, reports from other businesses, and information from scam and fraud organisations.

As the momentum of intelligence sharing accelerates, we anticipate a challenge – the potential for managing intelligence to overwhelm businesses subject to the Draft Code. Drawing from our experience in financial crime, AML and cyber threat intelligence, we advocate for the establishment of a unified cross-sector intelligence sharing scheme. This scheme, under the jurisdiction of a designated party, should standardise taxonomies, govern privacy and permissions, and manage the architecture facilitating seamless intelligence flow across the ecosystem.

Establishing a scheme that will guide the ecosystem towards a common language on scams will help future-proof the usefulness of the intelligence it will produce and share. We envision intelligence to

drive automated actions across the ecosystem, and for AI to play an increasing role over time in analysing and driving intelligence response.

Protecting Privacy While Sharing Intelligence
Balancing the need for effective intelligence sharing with privacy concerns poses a significant challenge. Establishing clear guidelines on what information can be shared, and with who, and how to protect individuals' privacy will be crucial.

We note that there are existing models and technologies, such as those used in Australia's Cyber Threat Information Sharing (CTIS) shared cybersecurity services, that offer a reference point to the exchange of actionable intelligence whilst avoiding the exchange of privacy-restricted information.

Taking Action on Intelligence
The Draft Code rightly stipulates that businesses must swiftly act on received scam intelligence. In essence, this obligation necessitates businesses, especially in the banking and telco sectors, to interrupt transactions or offboard customers flagged as potential scammers. However, the practical implementation of this obligation requires careful consideration.

Addressing the level, form and quality of intelligence is imperative. The Draft Code should address the threshold for certainty in identifying a party as a scammer. While urging businesses to act on intelligence, it is crucial to acknowledge the complexities of taking action. Systems for efficient, effective and justifiable action must be developed, recognising the inevitability of false positives and negatives.

Businesses need a regime that allows them to act or abstain from action in good faith based on available intelligence without fear of reprisal. This regime should consider the weight assigned to intelligence from different sources and parties, factoring in observable patterns to enhance the accuracy of decisions.

In summary, the Draft Code holds significant potential to further fortify its impact by addressing two critical aspects:

i. Establishing a unified intelligence sharing scheme: Assigning jurisdiction to a named party for developing a standardised intelligence sharing scheme ensures that the downstream actions of businesses are codified and automated, streamlining the management of the intelligence payload.

ii. Intelligence thresholds for action: Directly incorporating intelligence thresholds into the Draft Code creates a structured approach to decision-making, ensuring businesses can efficiently and effectively manage their scam intelligence payload, including the automation of intelligence actions over time.

TOPIC 3: REIMBURSEMENT OF CUSTOMER LOSSES

Linkage to related Consultation Paper questions:
4. Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors?
15. Are there additional overarching obligations the Government should consider for the Framework?

The Draft Code makes clear the expectation that businesses must take "reasonable steps" to protect customers, including acting in a "timely manner" on scam intelligence. However, it currently lacks

explicit directives on the circumstances and extent of a business's obligation to reimburse customer losses.

By inference, a business may be expected to reimburse customer losses where it has failed to take reasonable steps or act in a timely manner on scam intelligence. In our assessment, relying on inference alone may consequently shift the reimbursement burden primarily onto the business which takes the report from the scam victim. This situation could inadvertently relieve other implicated entities, such as those whose customer receives scammed funds, of economic incentive to prevent misuse of their services. This approach may also create additional volumes of complaints, which are already reported to be placing strain on both IDR and EDR processes[3], adding further complexity and administration given currently the Ombudsman frameworks are largely industry-based. Further, under a national "no wrong door" approach for a customer to report a scam, neutral parties such as ScamWatch receiving scam reports will be called on to exercise judgment when supporting a victim with a loss-recovery request.

Drawing from international models, where various reimbursement philosophies have been legislated, we observe a direct link between such legislation and heightened investment in scam reduction capabilities by businesses. We believe an outcomes-oriented approach to liability and customer reimbursement could be addressed within the Draft Code which would establish responsibility for losses where a party has acted with vigilance and care, and conversely introduce a level of responsibility for losses where a party has fallen short of their obligations. We consider that the Shared Responsibility Framework introduced by the Singaporean Government provides a useful example of an outcomes-oriented approach that applies to businesses across the scam value chain.

Recognising the intricacies involved, we acknowledge that developing guidelines for loss reimbursement necessitates a delicate balance, addressing conflicting interests to instil the right economic incentives across stakeholders. Outcomes-oriented reimbursement guidance will need to consider the following tensions:

Customer Overly favourable reimbursement guidelines may inadvertently foster customer complacency, potentially attracting more scam activity to Australia.	**Business** Conversely, if reimbursement guidelines overly favour businesses, the economic incentive to invest in scam reduction initiatives may diminish.
FSI of Scam Victim Misdirected reimbursement guidelines may undermine the economic incentive to eradicate money mules within the FSI used by a scammer.	**FSI Used by Scammer** Overemphasis on reimbursement for FSIs used by scammers may inequitably spread liability where customer protections at the FSI of the scam victim have fallen short.
Banks If reimbursement guidelines focus solely on banks, it may reduce the economic incentive for telcos and social media to act in disconnecting scammers from their infrastructure.	**Telco and Social Media** While it may not be suitable for these entities to reimburse customer losses in every scenario, holding them accountable for failing to meet obligations will incentivise diligent efforts to disconnect scammers from their infrastructure.

[3] Scams help drive 'unsustainable' increase in complaints about banks, finance firms to AFCA, ABC News, 9 January 2024, accessed 18 January 2024, https://www.abc.net.au/news/2024-01-09/scam-complaints-about-banks-finance-services-rise-at-afca/103293210

The absence of clear reimbursement guidelines in a future marked by high levels of intelligence sharing poses a significant risk of conflicts over loss apportionment across the ecosystem. This potential for disputes between businesses may impede timely resolution, detrimentally affecting scam victims.

To foster fair, consistent, and equitable reimbursement outcomes for customers and businesses alike, we recommend the formulation of guidelines within the Draft Code. Moreover, consideration should be given to the administration of these guidelines, including the possibility of vesting a neutral party to oversee the regime and facilitate expeditious resolution in cases of misaligned loss apportionment among multiple parties.

TOPIC 4: GOVERNANCE

Linkage to related Consultation Paper questions:

15. Are there additional overarching obligations the Government should consider for the Framework?
24. Are there any reasons why the anti-scams strategy should not be signed off by the highest level of governance within a business? If not, what level would be appropriate?

The Draft Code includes an ecosystem-wide obligation to develop, maintain, and implement an anti-scam strategy that sets out the business' approach to scam prevention, detection, disruption and response, based on its assessment of its risk in the scams ecosystem.

We believe a sound governance framework will be key to monitor the performance of the anti-scam strategy and ensure it keeps abreast of developments in the scam landscape. We believe the Draft Code could incorporate guidance on expected levels of governance and oversight of senior management and the Board.

Introducing principles related to good governance will drive businesses subject to the code to establish clear responsibilities / accountabilities for managing the development of the businesses anti-scam strategy and activities. It will also drive the consideration of risk appetites and metrics to monitor the extent to which the businesses' anti-scam performance is within appetite.

Deloitte.