Australian
Finance
Industry
Association

29 January 2024

Mr James Kelly
First Assistant Secretary
Market Conduct and Digital Division
Treasury
Langton Crescent
PARKES ACT 2600
Sent via email: scamspolicy@treasury.gov.au

Dear Mr Kelly

SCAMS – MANDATORY INDUSTRY CODES

The Australian Finance Industry Association (AFIA) is the only peak body representing the entire finance industry in Australia. [1] We appreciate the opportunity to respond to the 'Scams – mandatory industry codes' Consultation Paper (Consultation Paper).[2]

We represent over 150 members, including bank and non-bank lenders, finance companies, fintechs, providers of vehicle and equipment finance, car rental and fleet providers, and service providers in the finance industry. We are the voice for advancing a world-class finance industry and our members are at the forefront of innovation in consumer and business finance in Australia. Our members finance Australia's future.

We collaborate with our members, governments, regulators and customer representatives to promote competition and innovation, deliver better customer outcomes and create a resilient, inclusive and sustainable future. We provide new policy, data and insights to support our advocacy in building a more prosperous Australia.

[1] Australian Finance Industry Association (afia.asn.au).
[2] Treasury, *Scams – Mandatory Industry Codes, Consultation paper*, November 2023, https://treasury.gov.au/consultation/c2023-464732

INTRODUCTORY COMMENTS

Scams have become widespread in the Australian economy, with the Australian Competition and Consumer Commission (ACCC) reporting financial losses to scams of at least $3.1 billion in 2022.[3]

AFIA supports the introduction of a framework which provides protection for consumers and encourages industry collaboration to identify perpetrators of scams more effectively. Consumer needs and business obligations must be appropriately balanced to ensure consumers are aware of their options if they are affected by a scam, and businesses have clarity in the obligations that apply to them.

To that extent, AFIA supports a whole ecosystem approach to address scams, including the proposed introduction of an overarching principles-based framework, embedded within primary legislation, with sector specific codes and standards underpinning this framework.[4]

While the Consultation Paper suggests three initial sectors to be designated and brought under the framework – banks, telecommunications providers, and digital platforms – future relevant sectors are to be identified. As scam activity occurs across sectors and jurisdictions, we consider it will be crucial to have clear definitions and criteria to apportion responsibilities across businesses in different sectors.

AFIA suggests including additional clarification to the definition of a scam, and an alignment across jurisdictions and industries. We consider that providing additional clarity will help consumers to better understand whether a scam has occurred and what their rights are, while also enabling businesses to respond effectively. Additionally, we consider that the reporting obligations relating to sharing of intelligence would benefit from clearer guidelines to mitigate against any risk of hesitancy in sharing information.

AFIA recognises the importance of implementing anti-scam strategies and welcomes further explanation on how the new obligations will interact with existing privacy and competition laws as well as other regulatory requirements. We believe that ensuring transparency in scam monitoring and prevention, along with clear processes for unblocking payments or accounts, is crucial.

Our detailed comments can be found within **Attachment A** to this submission.

[3] Treasury, *Scams – Mandatory Industry Codes*, Consultation paper, November 2023, p 4. Citing ACCC (2023), *Targeting Scams*.
[4] Ibid. p 8.

We would appreciate the opportunity to discuss our recommendations further. Should you wish to discuss our submission or require additional information, please contact Sebastian Reinehr, Senior Policy Adviser, at sebastian.reinehr@afia.asn.au.

Yours sincerely

Roza Lozusic
Executive Director, Policy and Public Affairs

ATTACHMENT A:

1. Definitions

Treasury proposes a new definition of a 'scam' that aims to clearly define what constitutes a scam in the Australian context, differentiating it from other types of fraud that do not involve deceiving a consumer into authorising a fraudulent act.

Treasury proposes that the new definition will align with the definition of fraud within the Commonwealth Fraud Control Framework and the *Criminal Code Act 1995 (Cth),* being 'intentional or reckless deception'. [5] However, Treasury indicates that 'unauthorised fraud' is not intended to be included in the framework.

We consider that additional clarity on the scope and the application of 'authorised fraud' to scams would be appropriate, particularly in scenarios where there is a combination of authorised and unauthorised fraud. For example, a telecommunications hack that is used to coerce payment authorisation consent.[6]

The definition of scams could be further defined by providing explicit examples for each sector. It would be helpful to receive clarification on whether buyer fraud is included in this definition, for example, where a purchase is made with a stolen credit card and later disputed by the legitimate cardholder.

To mitigate against any interpretation issues, AFIA is supportive of a definition that includes examples which are well-understood across the industry, and guidance about the definitions interaction with other legislation to determine whether there are any jurisdictional issues.

2. Obligations

AFIA acknowledges the critical importance of anti-scam measures to provide protection to consumers. We believe the obligations proposed should also be balanced against existing requirements and consideration of the practical implications for business implementing the measures.

2.1. Prevention, Detection and Disruption

AFIA recognises the importance of businesses developing anti-scam strategies. We seek clarity over the proposed requirement to take 'all reasonable steps' to prevent scams.[7] Further clarification on this requirement would lead to a more efficient and effective use of investment and resources to prevent scams.

AFIA notes that there can be concerns about the reliability and accuracy of scam intelligence. Businesses that act on unverified or incorrect information could lead to wrongful accusations, which may risk consumer detriment.

[5] part 7.3 *Criminal Code Act 1995 (Cth)*
[6] Treasury, *Scams – Mandatory Industry Codes*, Consultation paper, November 2023, p 10
[7] Ibid, p 11

It is not currently clear whether businesses who acted in good faith, but on incorrect intelligence, would be considered liable, should a consumer seek redress.

2.2. Response (obligations with respect to consumers)

Treasury proposes that affected businesses should also have effective, transparent, and accessible complaints handling processes for consumers to report scams or make complaints about the business's response to scam activity.

AFIA acknowledges the need for effective dispute resolution processes when responding to consumer complaints and is supportive of this proposal noting that (as acknowledged in the Consultation Paper) financial firms already have industry specific internal dispute resolution (IDR) and external dispute resolution (EDR) arrangements in place.[8]

2.3. Reporting (obligations to regulators and other businesses)

The obligation for businesses to promptly notify other businesses, the National Anti-Scams Centre (NASC), and relevant regulators of intelligence about suspected or identified large-scale or emerging scam activities may be challenging for businesses where intelligence collection and analysis is still developing. [9]

AFIA recommends that 'sufficient and credible intelligence' for reporting purposes be clarified as any ambiguity could result in inconsistent information being shared, reducing the effectiveness of these measures. Additionally, the potential reputational impacts of reporting high numbers of scams, where unverified, could deter some businesses from transparent reporting.

Furthermore, AFIA notes we have been advocating for the development of a mechanism that enables the real-time exchange of timely and pertinent information necessary to prevent financial crimes, Particularly cyberattacks and scams. We recommend that Government convenes and leads a working group to develop a new network, comprising all finance industry participants, which would facilitate a secure exchange of this information.

2.4. Anti-scam Strategy

The Treasury proposal requires businesses to develop an anti-scam strategy with high-level approval and sign-off, such as from the Board or similar level of governance. Regular review and reporting on the effectiveness of the strategy and compliance is expected, though publication of the strategy is not mandatory.[10]

[8] Ibid
[9] Ibid, p 36
[10] Ibid, p 37

AFIA recommends that publishing best practice guidance would be beneficial for businesses to understand the expected standard of anti-scam strategies.[11] It is important that there is clarity in the review processes by the Australian Competition and Consumer Commission (ACCC) and the practicality of businesses implementing these strategies is considered, including identity verification in financial transactions.

2.5. Information Sharing and Reporting Requirements

Under the proposed framework, businesses would be mandated to actively respond to scam intelligence disseminated by other businesses, industry associations, law enforcement, and regulatory authorities, including the National Anti-Scams Centre (NASC). [12] This response entails a series of proactive measures, such as the removal of scam-related content, issuing warnings to consumers, and restricting access to services for users identified as scammers.

AFIA is supportive of a collaborative effort to combat financial crime and scams. We caution that there is a need for these interactions to be governed by a carefully considered approach that adheres to privacy and competition laws, taking into account the need for explicit consent when handling and sharing personal data, and is clear in its execution requirements. As discussed above, the accuracy of scam intelligence requires some development and mechanisms for sharing information, ideally in real-time, should be further considered by the Government and financial services participants.

AFIA recommends a clearer outline of the duty to notify other businesses in the event of a scam, and of the threshold for a 'reportable scam'. If there is any uncertainty or lack of clarity regarding the reliability of the scam intelligence being relied upon, it can become challenging to justify penalisation if a threat ultimately materialises. Furthermore, this ambiguity could potentially result in businesses being hesitant to share information, fearing legal repercussions or breaches of privacy regulations.

2.6. Consumer Reports, Complaints Handling, and Dispute Resolution

The proposed framework creates a reporting mechanism for users to report scams, including in cases where they have identified but not been affected by a scam.[13] The requirement for information sharing raises questions about interaction with privacy and competition laws and the potential need for explicit consent.

AFIA notes that the obligations to notify other businesses requires additional clarity. The level of oversight and input from regulatory bodies, such as the Office of the Australian Information Commissioner (OAIC), is a critical area requiring further guidance. This is necessary for businesses to understand their responsibilities and the extent of regulatory expectations. Such guidance would not only help in aligning the anti-scam measures with privacy and competition laws, but also ensure a balanced approach to information sharing, thereby maintaining consumer trust and business integrity.

[11] Ibid, p 13
[12] Ibid, p 38
[13] Ibid, p 39

3. Oversight/Compliance

Treasury's proposed framework introduces a multi-regulator oversight and enforcement model. This approach recognises the existing roles, responsibilities, expertise, and links regulators have across different parts of industry in combating scams.[14]

In addition, there will be penalties for non-compliance with obligations under the framework. This includes not only redress options available via IDR and EDR (e.g. compensation for scam losses), but new penalties for non-compliance.[15]

Similarly, additional penalties for breaches of sector-specific obligations would be set under the sector-specific enabling legislation. The Consultation Paper notes that Government and regulators will work through the necessary arrangements to avoid two regulators taking simultaneous action against a breach under the Framework.

AFIA supports a clear process that avoids duplication and the potential for regulators taking simultaneous action.

We acknowledge the importance of transparency in scam monitoring and prevention, coupled with a clear process for unblocking payments or accounts. This stance is informed by the Australian Financial Complaints Authority (AFCA)'s view that banks are contractually obliged to follow customer instructions and do not have a general duty to prevent customers from engaging in transactions, even if they are potentially harmful.

AFCA has previously stated that:

> *'A bank is contractually obliged to follow its customer's mandate or instruction"* and *"Generally, a bank does not have a fiduciary duty to advise the complainant that a transaction … is not in its best interests, or: an obligation to monitor transactions on its customer's behalf, maintain watching briefs for scams, for its customer's benefit, prevent the customer from dealing with funds they are contractually entitled to access, and/or reimburse a customer for authorised payments to a third party'*[16].

In an example, an ADI identified a consumer was sending money to a scammer and blocked the transaction. The consumer then filed a complaint with AFCA against the ADI to release the payment, and then, later, filed another AFCA complaint for allowing the funds to go through to the scammer. This creates a no-win situation in which AFCA can be used against a financial firm for both allowing and preventing a scam. A clearer delineation of what banks can and can't do is important to ensuring they are empowered to react effectively.

[14] Ibid, p 22

[15] Ibid, p 23.

AFIA recommends measures that enhance the matching of account names to numbers, and steps to prevent the establishment and operation of fraudulent and 'mule' accounts. Additionally, special consideration is required for consumers who are at risk of vulnerability, including people experiencing domestic abuse who may be coerced into recalling payments.