

2 February 2024

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

By email: scampolicy@treasury.gov.au

Dear Sir/ Madam

Scams—Mandatory Industry Codes

1. This submission concerning the consultation paper titled “Scams—Mandatory Industry Codes”, which was released by Treasury on 30 November 2023 (the **Consultation Paper**), is made by the Financial Services Committee (the **FS Committee**) and the Media and Communications Committee (the **MC Committee**) of the Business Law Section (the **BLS**) of the Law Council of Australia.
2. The BLS thanks Treasury for the opportunity to comment on the Consultation Paper and agreeing to a short extension of time to allow the BLS to make this submission.

Key Points

3. The key matters the BLS wishes to raise with respect to the design of a future scams prevention framework are as follows:
 - (a) the proposed framework would likely be more effective in combatting scams if the following sectors were also within its remit:
 - (i) online marketplaces;
 - (ii) crypto-currency exchanges;
 - (iii) superannuation funds;
 - (iv) payment services providers;
 - (v) securities brokers; and
 - (vi) managed investment funds;
 - (b) the potential involvement of multiple regulators needs to be carefully considered;

- (c) the breadth of the proposed definition of “scam” may be problematic;
 - (d) the sharing of information will play a critically important role and is relevant beyond the sectors the proposed framework seeks to cover;
 - (e) clear and unambiguous regulatory guidance will need to be developed and disseminated in a timely fashion to prepare the regulated population for the new regime; and
 - (f) the chosen external dispute resolution (**EDR**) model must be developed with due care and attention to the flow-on consequences.
4. In reviewing the framework, which consists of four sector-specific codes and standards:
- (a) the FS Committee has focused its attention on banks and the financial sector, and has made some sector-specific points in this submission; and
 - (b) the MC Committee has focused on telecommunications providers and other communications networks and service providers.

Submissions

Proposed Scams Code Framework

5. The BLS applauds initiatives that are directed to the prevention and disruption of scams across the scam ecosystem, as well as responses to harm caused by scams.
6. The BLS considers that the structure of the proposed framework, comprising overarching legislation within the *Competition and Consumer Act 2010* (Cth) under the supervision of the Australian Competition and Consumer Commission, and the adoption of a principles-based approach, is appropriate. The BLS notes that the structure provides for flexibility and responsiveness while recognising the particular roles and exposure to the impacts of scams on:
- (a) the integrity of the financial sector, telecommunications providers, and digital communications platforms services and networks; and
 - (b) the confidence of consumers in those services.

Coverage of the Proposed Framework

7. As the Consultation Paper indicates, scammers exploit loopholes.¹ Accordingly, to prevent such exploitation, an ecosystem-wide approach to preventing, detecting and disrupting scams is needed.
8. However, the BLS notes that, at least initially, the designated sectors that are covered by the framework will exclude sectors that are known today to be key transmission mechanisms for the proceeds of scams or key sectors in the scam ecosystem, namely online marketplaces, crypto-currency exchanges,

¹ Page 6.

superannuation funds, payment service providers, securities brokers and managed investment funds.

9. The BLS is concerned that the exclusion of these sectors from the framework could compromise the effectiveness of the framework and introduce risks of unintended market consequences.
10. The BLS appreciates the impact that inclusion of those sectors may have on timing for the introduction and implementation of the framework, particularly given that there are no (or, at best, limited) industry sector codes, EDR schemes or other infrastructure to leverage in some of these sectors. The BLS submits that, at a minimum, the overarching framework should be enacted to demonstrate that the infrastructure for further action against scams is in place until further relevant sector codes can be developed and implemented.
11. Treasury may wish to consider the extent to which obligations developed for one sector could be applied to one or more other sectors (for example, by considering the extent to which all or some of the code applying to banks could apply to payment service providers and/or crypto-currency exchanges).
12. While the banks frequently “lead the way” in terms of compliance and models of best practice, the FS Committee notes that other service providers with fewer resources at their disposal are potentially more vulnerable to scammers, and is concerned that, should the banks alone be brought within the framework, scammers may be expected to then focus on the gaps in framework coverage by using different payment methods.
13. The FS Committee submits that the structure of any scam prevention code for the banking and financial sector would need to be able to accommodate a broad range of participants with overlapping functions. To this end, an umbrella code with sections specific to particular sectors or activities may provide sufficient flexibility to allow the particular threat environment and characteristics of each activity to be addressed without creating overlapping obligations and penalties for banks and other financial sector participants who engage in a range of different kinds of activities within the coverage of the framework.

The multi-regulator strategy

14. The BLS recognises that the proposed multi-regulator strategy would seek to leverage the existing expertise of sector-specific regulators. However, the BLS is concerned that this proposed approach could result in:
 - (a) duplication of actions and penalties; and
 - (b) overlapping and inconsistent approaches across regulators and sectors.
15. Therefore, the BLS submits that arrangements should be put in place to:
 - (a) avoid regulatory duplication and overlap;
 - (b) facilitate the sharing of information between regulators; and

- (c) promote consistency between regulators both at the sector level and across the framework.

These outcomes could be achieved through a coordination mechanism and/or consultation obligations.

16. While the Consultation Paper mentions the existing approach taken in the Banking Code of Practice issued by the Australian Banking Association, the FS Committee considers it important to note that:
 - (a) not all banks have adopted the Banking Code of Practice;
 - (b) other voluntary codes, such as the Customer-Owned Banking Code of Practice, also have significant membership; and
 - (c) there are some banks that are not a party to any code of conduct.
17. In light of this, and while noting that the voluntary codes may provide some additional consumer protection to customers of code subscribers, the BLS submits that it would be preferable to develop a comprehensive and consistent baseline solution as a framework for mandatory industry codes that are separate from any voluntary codes.

The definition of “scam”

18. The Consultation Paper proposes a definition to the following effect:

“A scam is a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means.”

19. The BLS supports a definition of “scam” that strikes a balance between ensuring certainty for regulated businesses and allowing for sufficient flexibility to capture new and emerging scam categories over time. However, the BLS considers that, as drafted, the proposed definition could cover other matters, such as non-scam related fraud.
20. The BLS is concerned that an overly broad definition of “scam” may pose a risk of overlap between scam-related obligations and other obligations, and could cause scam-related obligations to be imposed in relation to matters that were not intended to be covered by the framework. In particular, if a separate EDR scheme were to be established for scams, potential unintended consequences could include:
 - (a) overlap between the jurisdiction of the scam-related EDR scheme and existing EDR schemes; or
 - (b) an inappropriately broad exclusion from the jurisdiction of existing EDR schemes.
21. The BLS notes that, while the Consultation Paper refers to deception of a customer into authorising the fraud, this is not reflected in the proposed definition. Further, the question of whether a consumer authorises the fraudulent transaction is not without doubt. For example, in applying the ePayments Code, the Australian Financial Complaints Authority does not in all cases treat the transaction as having been authorised by the customer (for example in the case of virtual cards downloaded to

a scammer's wallet). Accordingly, the BLS submits that any definition would have to be aligned with existing obligations (including in the ePayments Code) to remove any potential for overlap or other unintended consequences.

22. The BLS is also concerned that the terms “dishonest” and “deceptive” as used in the proposed definition are too broad to capture the key attributes of a scam. For example, an investor in a pyramid scheme may be induced to participate by reason of misleading and deceptive representations of the promoter yet receive the promised benefits when other investors are left out of pocket.

Principles-based obligations

23. The BLS believes that a focus on prevention, detection and disruption of scams will help to reduce the risk of harm and loss that may then need to be addressed. For that reason, the BLS considers that the general principles should facilitate a robust mechanism to identify and take down scam content or transactions across sectors.
24. The BLS also considers that these obligations should be supported by provisions designed to facilitate prompt information sharing (both within and across sectors) to allow for prompt action to be taken in response to scams, such as removal of scam content.
25. Prompt responses to scams can require action by those outside the identified sectors. For example, prompt identification that a website is not a legitimate site of the organisation that it purports to represent may be aided by promptly confirming with the organisation that the website is fake. Therefore, the BLS submits that an information-sharing framework which extends beyond the identified sectors should be considered.

Risk-based approach

26. While the risk-based approach is flexible, the BLS notes that it can be applied in a number of ways and therefore suggests that, to give as much certainty as possible, regulatory guidance ought to be provided with sufficient prior notice to give industry a reasonable amount of time for implementation. It is critical that the types of risk that must be assessed and addressed are clearly articulated.
27. The FS Committee particularly wishes to note the “common carrier” nature of the payment system. It would be a significant departure from fundamental principles of the general law governing payments and a significant burden would be imposed on the resources of payment providers if they were required to enquire or “second guess” their customer in facilitating that customer's instructions. Delays in payment processing could have substantial adverse consequences for the transacting parties, and the FS Committee anticipates that any measures to combat scams which “build in” delay or add additional steps or verification requirements would ultimately increase costs imposed on both the participants in the payment system and the users of the payment system.

Information sharing

28. Information and data sharing across the scam ecosystem is a key component of an effective scam prevention framework.

29. The BLS notes that there are laws that may inhibit the free flow of information to facilitate the prevention, detection and disruption of scams, as well as actions taken in response to consumer harm associated with scams. These include the *Privacy Act 1988* (Cth) (to the extent that it relates to personal information) and the tipping-off prohibition under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), as well as obligations of confidence that arise at common law (such as the banker's duty of confidentiality).
30. It may be necessary to alter the operation of certain provisions of this nature in the context of dealing with scams to ensure that there can be prompt, effective and workable information sharing under the framework. The BLS notes that this is a more a policy than a legal matter.

Anti-scam strategy

31. The BLS notes that the Consultation Paper touches on whether an organisation's anti-scam strategy should have to be signed off by the highest level of governance within a business. The BLS submits that it is relevant to consider the capacity of the board or other peak body within the organisation to do so, having regard to the other matters within its remit and the distinction between board and management. The BLS supports a non-prescriptive approach to ensuring that an organisation's anti-scam strategy is authorised by and issued at an appropriately senior level of the organisation, and is subject to effective oversight.
32. The BLS submits that publication of an organisation's anti-scam strategy could potentially compromise the effectiveness of the strategy, as it may assist scammers to evade detection (for example, through by-passing the organisation's controls). As a result, on balance, the BLS submits that it would be preferable not to require organisations to publish their anti-scam strategy and leave it to each organisation to determine whether to create a public facing anti-scam policy (which might be used to build and/or maintain customers' trust and confidence in the organisation's ability to combat scams its customers may face).

Dispute resolution

33. It is important to have effective internal dispute resolution (**IDR**) and EDR arrangements in place to deal with customer complaints that arise from scam-related activity.
34. A scam typically involves multiple participants across sectors. As a result, it is likely that disputes arising from a scam will involve participants in more than one sector, including across different sectors within the proposed framework.
35. As the Consultation Paper indicates, there are existing EDR schemes which apply to some of the proposed designated sectors. However, the BLS notes that not all of those sectors currently have an EDR scheme, and considers that the use of existing EDR schemes could make it more difficult to add sectors that do not have an existing EDR scheme to the framework in the future.

36. In any EDR scheme arrangement it will be important that:
- (a) there is an EDR mechanism for all sectors in the scam ecosystem;
 - (b) consumers receive clear information about how to make a complaint;
 - (c) the EDR scheme is transparent and easy for consumers to navigate;
 - (d) the EDR scheme facilitates prompt and efficient resolution of disputes;
 - (e) there is consistency of outcomes; and
 - (f) fragmentation of complaints (for example between entities in multiple dispute resolution schemes) is avoided.
37. There are two potential EDR models that could apply in respect of the obligations in the framework:
- (a) a single scams scheme—that could be a new body or an existing ombudsman; or
 - (b) existing EDR schemes could be utilised (although new schemes would need to be developed for sectors that do not have an existing EDR scheme), with mechanisms to seek to bring them together to address disputes that cross multiple sectors.
38. While, on the one hand, the use of existing EDR schemes would allow their sector expertise to be leveraged, on the other hand:
- (a) this could be a barrier to promptly capturing new sectors within the framework, given that not all scam ecosystem industries have an EDR scheme;
 - (b) a mechanism for referral and apportionment among the EDR schemes would need to be developed;
 - (c) rules as to how liability to pay the consumer is allocated would need to be established;
 - (d) mechanisms to reduce the risk of inconsistency across industry EDR schemes and scheme arbitrage would need to be introduced; and
 - (e) arrangements for cooperation across schemes would need to be developed.
39. The BLS notes that having one EDR scheme that serves as a single point of contact would allow for liability to be apportioned more easily and provide for a single point of contact for victims and businesses.
40. However, the regulatory perimeter of the EDR scheme would need to be clear in order to avoid the potential for duplication or overlap with the existing EDR schemes.
41. For that reason, as noted above, the definition of “scam” is critically important. The BLS submits that the definition should avoid capturing traditional fraud type scenarios with a view to avoiding overlap with the non-scam jurisdiction of existing

EDR schemes. Further, the prospect of a complaint covering both a scam and other matters would need to be considered, and mechanisms would need to be put in place to address the treatment of that complaint between the existing EDR schemes.

42. Both EDR models would require legislative reform to, for example:
 - (a) clarify and amend jurisdiction of EDR schemes;
 - (b) ensure an appropriate level of consistency in decision making; and
 - (c) facilitate referrals and information flows between EDR schemes and participants where appropriate.
43. The BLS further notes that an efficient EDR scheme needs to be supported by robust and efficient IDR schemes across the ecosystem to allow for triaging. Currently, participants in some of the sectors that are proposed to be covered by the framework are not subject to statutory obligations relating to their IDR arrangements.
44. Appropriate IDR arrangements will assist in avoiding unnecessary escalation and burdening of scarce resources at the EDR level. That will require the framework to impose IDR requirements, including provisions designed to facilitate the prompt resolution of complaints across sectors and allocation of liability across the ecosystem at the IDR level.

Apportionment of liability

45. Given that a scam will typically involve multiple sectors and multiple participants, the BLS considers that there should be a statutory regime for apportionment of liability amongst participants. The BLS believes that such a regime would incentivise compliance across the whole scam ecosystem. Rules as to how liability to pay the consumer is allocated both in EDR and IDR would be required, as well as obligations to facilitate information sharing and co-operation among participants.

Bank-specific obligations

46. The Consultation Paper sets out a number of potential obligations that could form part of the banking (or financial sector) code to prevent, detect, disrupt and respond to scams. The FS Committee wishes to share the following comments and practical observations on certain of those obligations, as outlined below.

Prevention

47. The FS Committee considers that verification of a transaction obligation is potentially problematic as, by definition, scams entail the victim being deceived and consenting to the transaction. Indeed, banks frequently report customer complaints about conduct of banks that occurred as a result of the bank's efforts to protect that customer from a suspected scam. Further intervention, such as blocking or suspending suspected scam transactions, is likely only to increase this customer push back.

48. The FS Committee considers that it is appropriate to adopt a tailored approach in circumstances where:
- (a) the customer is assessed to be at high risk and therefore vulnerable; and
 - (b) the bank or payments processor has, or should have, information establishing that the proposed payment recipient is or is likely to be a scammer.
49. One approach to assist customers who have been deceived by a scammer may be to implement procedures for banks and payment providers to share any information they may have about the payee or recipient of the funds with the potential victim to assist that victim to understand the true position.
50. For example, a potential victim may reconsider their consent to a transaction if they become aware:
- (a) that the payee has been associated with scams in the past;
 - (b) that the payee is located in an unusual jurisdiction, which may not be where they claim to have been from; or
 - (c) of other similar information that the payment provider may reasonably be expected to hold.

The payer / potential victim would then have the opportunity to compare such information against their own understanding of the proposed transaction and consider whether they still wished to proceed with that proposed transaction.

Detection and disruption

51. The FS Committee considers it important that any obligations imposed on financial services providers with respect to identification of potential scam-related activity are framed so that they are not required to make legal decisions (as opposed to forming a reasonable suspicion) about whether an account is fraudulent, and a customer is a scammer.
52. The FS Committee agrees with the proposal that a bank must have processes in place to act quickly on information that identifies an account or transaction that is or is likely to be a scam. The FS Committee notes that there is a distinction between identifying a suspicious transaction, on the one hand, and taking action that may be to the detriment of one of the parties to the transaction, on the other. The FS Committee submits that it is important for banks and other payment providers to have adequate legal protection from liability in circumstances where they have formed a suspicion that a customer may be engaging or attempting to engage in fraud or other illegal activity.

Response (obligations to consumers)

53. The FS Committee supports the three proposals on responding to scams that are set out in the Consultation Paper. In particular, interbank cooperation is likely to be essential to the effectiveness of the framework when accounts have been compromised.

54. The FS Committee notes that scams are often international in nature and in many cases the funds stolen will be rapidly transferred overseas. The FS Committee submits that international cooperation through the correspondent banking network or other means to give extra-territorial reach to these methods is important to increase their effectiveness. The FS Committee acknowledges that, to the extent that this goes beyond the scope of the Consultation Paper, it will likely require further consideration.
55. The understanding and experience of FS Committee members is that banks generally do assist customers to recover transferred funds to the extent possible, although this is frequently constrained for the reason outlined above. A code could expand and facilitate this ability to recover funds to participants in the payment system beyond the larger banks and beyond the Australian jurisdiction.

Conclusion and further contact

56. The BLS would be pleased to discuss any aspect of this submission.
57. Please contact the chair of the FS Committee, Pip Bell (committeechairfsc@gmail.com), or the chair of the MC Committee, Connie Carnabuci (cbcarnabuci@gmail.com), if you would like to do so.

Yours sincerely



Dr Pamela Hanrahan
Chair
Business Law Section