New Zealand Banking Association
Te Rangapū Pēke

Submission

to the

Finance and Expenditure Select Committee

on the

Fair Trading Amendment Bill

16 July 2026

NEW ZEALAND BANKING ASSOCIATION – TE RANGAPŪ PĒKE
PO Box 3043, Wellington 6140, New Zealand
www.nzba.org.nz

About NZBA

1. The New Zealand Banking Association – Te Rangapū Pēke (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following sixteen registered banks in New Zealand are members of NZBA:

- ANZ Bank New Zealand Limited
- ASB Bank Limited
- Bank of China (NZ) Limited
- Bank of New Zealand
- China Construction Bank (New Zealand) Limited
- Citibank N.A.
- The Co-operative Bank Limited
- Heartland Bank Limited
- The Hongkong and Shanghai Banking Corporation Limited
- Industrial and Commercial Bank of China (New Zealand) Limited
- JPMorgan Chase Bank N.A.
- Kiwibank Limited
- Rabobank New Zealand Limited
- SBS Bank
- TSB Bank Limited
- Westpac New Zealand Limited

Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Sam Schuyt
Policy Director & Legal Counsel
sam.schuyt@nzba.org.nz

Introduction

4. NZBA welcomes the opportunity to provide feedback to the Finance and Expenditure Committee (**Select Committee**) on the Fair Trading Amendment Bill (**Bill**). NZBA commends the work that has gone into developing the Bill.

5. Our submission focuses on the "safe harbour" provisions set out in clause 33 of the Bill.

6. In brief, NZBA submits that, while creating protections for businesses taking reasonable, good faith activity to protect New Zealanders from fraud and scams:

   6.1. the application of the safe harbour needs to be sufficiently broad to ensure it achieves its intended effect; and

   6.2. there are a number of other legal and / or regulatory barriers that can make organisations hesitant, or unable, to take prompt and decisive action against scammers. In our view, these issues need to be addressed in addition to the safe harbour considerations included in the Bill.

Scope of safe harbour

Captured entities

7. Clause 33 of the Bill, broadly, provides a defence against civil liability for actions taken to disrupt scams. The clause has a narrow application, with the protection it offers only applying to online service providers, in relation to activities carried out through an online service.

8. The definition of "digital platform" at s 48U(4) does include "an internet-based system that facilitates transactions", which may have been intended to capture online banking services such as internet banking platforms. However, the current drafting is ambiguous, and the examples given are materially different from the services that banks offer.

9. We submit that the scope of this defence is too narrow, and does not reflect the range of participants and activities in the anti-scam ecosystem – which includes banks, telecommunications providers and digital platforms. The safe harbour provisions should therefore be amended to explicitly include banks.

10. The ability to move quickly to stop scams plays a critical role in protecting New Zealanders, whether this is through shutting down fake websites, sharing information about known fraudsters, or freezing accounts and returning stolen money. We recognise the importance of acting quickly to help prevent financial harm from occurring through fraud and scams, and support amendments that help maximise efficiencies, balanced against fair and reasonable treatment of customers.

11. Banks face similar levels of legal and operational risk as telecommunications and digital platform providers when taking action to respond to fraud and scams. Where banks take steps to restrict or block banking facilities, or share information with telecommunications or digital platform providers to enable them to act, they may be exposed to claims or disputes from affected parties.

12. Banks have voluntarily committed, following NZBA's update to the Code of Banking Practice, to provide improved protection for customers against scams and compensate customers for certain scam losses. This reflects a strong customer-outcome focus and a willingness to take responsibility that is not yet consistently observed across all parts of the scam ecosystem.

13. For example, banks share information about digital fraud transactions and 'money mule' accounts via the Fraud Information Exchange. This can enable banks to, among other things:

    13.1. identify high-risk transactions and provide warnings to customers in advance of payments being made;

    13.2. where appropriate, stop or delay payments or close accounts; and

    13.3. recover stolen funds before they are moved overseas (following which, the funds are significantly more difficult to trace and recover).

14. However, these activities create risks of civil liability where actions are taken to disrupt scams (for example, blocking a payment or closing an account), as well as other legal risks, as discussed below. While banks have adopted measures to reasonably verify fraudulent activities before taking action to mitigate these risks, time is of the essence when it comes to responding to scams. The lack of any protection for actions taken to prevent scam activity, in good faith, can slow down this process or dissuade banks from taking proportionate action due to defensive or overly cautious decision making.

15. The banking industry has also been a strong supporter of the Government's Anti-Scam Alliance initiative, and is committed to collaborating across sectors to better protect New Zealanders from scams and fraud. However, for that collaboration to be truly effective, all participants should operate on a level playing field, with equivalent access to supporting legal frameworks. A consistent scope applicable to providers of online banking / transaction services is critical to ensuring meaningful participation, shared accountability, and the best possible outcomes for customers and the wider community. Excluding banks from the scope of the protections risks weakening cross-industry collaboration and limiting the overall effectiveness of the Anti-Scam Alliance initiative.

16. Further, we note that overseas jurisdictions, such as the UK, have statutory mechanisms that reduce the legal risk for regulated entities sharing information for

financial crime purposes. Expanding the safe harbour to apply to financial institutions in New Zealand will better align with the direction of travel overseas.

17. Accordingly, we submit that the safe harbour provision should be expanded beyond only online service providers and online services, to apply to banks and other organisations that are actively participating in New Zealand's anti-scam ecosystem to protect customers.

18. This could be achieved, for example, by replacing references to "online service" with "service", along with the definition of "service" explicitly listing services provided by registered banks and non-bank deposit takers as within scope. We would be happy to engage further to assist with specific drafting on this point.

Scale of activity

19. The Bill requires a provider of online services to consider whether their proposed responses are reasonably proportionate to the nature and scale of the activity before taking action (s 48U(2)(a)).

20. However, the action to be taken is often binary – for example, block / do not block a website; allow / do not allow a payment. Requiring entities to consider the scale of a scam activity may lead to confusion as to whether they can take the appropriate action or not, limiting the intended benefits of the Bill.

    20.1. For example, it is advantageous to take down scam sites at their inception if they are clearly identifiable as such, rather than waiting for them to grow in scale – leading to negative consumer outcomes – until the response (closing the site) is proportionate to the scale of the scam activity. While this is a fairly extreme example, it does illustrate that the requirement to consider the scale of a scam activity might lead to confusion about the appropriate time at which an intervention becomes proportionate and justifiable.

    20.2. Equally, in the fraud data-sharing space for banks, common actions are often binary (stop / do not stop a payment) – the requirement to consider the "scale" of a mule account, which is receiving stolen funds, risks creating unnecessary confusion.

21. NZBA submits that the reference to "scale" in s 48U(2)(a) should be removed. The requirement to consider the proportionality of a response in relation to the "nature" of an activity would still be retained, which in our view should provide sufficient scope for entities to consider any proposed action in the wider context of the impacts that action may cause.

Additional regulatory barriers to anti-scam activities

22. In addition to widening the number of entities and activities that should be afforded the safe harbour, NZBA submits that the protections should be expanded to address other

legal barriers that can negatively impact the ability of organisations to help protect customers from fraud and scams.

23. Banks, for example, in undertaking the activities set out at paragraph 13 above, may be exposed to risks, or otherwise be limited in their ability to act, under:

    23.1. The Privacy Act 2020, where information related to suspected scam activities may include personally identifiable information (e.g. details about mule accounts, suspected scammers and suspected victims).

    23.2. The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (**AML/CFT Act**), where information-sharing of suspected scam activity may be limited under the Act's "tipping off" provisions.

    23.3. The Defamation Act 1992, where entities face risks of defamation where an action is taken in good faith (for example, to provide warnings about certain websites) and the domain owner later claims reputational harm.

    23.4. The Financial Markets Conduct Act 2013 (more specifically, the Conduct of Financial Institutions (**CoFI**) regime), where banks may risk breaching the Fair Conduct Principle under CoFI if they take action against a customer / a customer's account based on information received from another bank before completing their own investigations.

24. The risks posed by this legislation can impact the ability of banks in their efforts to help prevent or mitigate scam losses, either by restricting the types of activities that can be taken (e.g. the limitations on information-sharing under the Privacy Act), or slow down processes to ensure compliance (e.g. independently verifying information received from another bank to avoid breaching the CoFI regime).

25. As previously noted, time to respond can often be an important factor in an entity's ability to prevent a scam, or recover scam losses. While we agree it is important to take reasonable steps to sufficiently verify an action is fraudulent before responding to it, current legislative constraints can make this process disproportionately burdensome.

26. We submit that the safe harbour in the Bill should go further, by explicitly excluding liability under the legislation identified above for entities who comply with the requirements of s 48U. In our view, the safeguards included in the current drafting of the Bill (i.e., requirements for proportionate responses, good faith actions, and reasonable grounds for believing an activity was a scam) would sufficiently protect against disproportionate or insufficiently verified actions.

27. While these legislative barriers could be addressed independently, we consider that the Bill provides an apposite opportunity to address them consistently and in one

place, ensuring that protections and responsibilities are better aligned across participants in the anti-scam ecosystem, with greater flexibility and certainty.

27.1. We have previously addressed legislative overlap through the use of exemption notices. For example, NZBA worked with the Ministry of Justice to address the tipping off concerns set out at paragraph 23.2 above, resulting in the publication of the Anti-Money Laundering and Countering Financing of Terrorism (Class Exemptions) Amendment Notice 2025. This enabled information sharing between banks for fraud and scam prevention purposes without breaching the tipping-off provisions under the AML/CFT Act.

27.2. However, obtaining exemption notices is not our preferred approach. It is often time-consuming and operationally complex, requires ongoing review and periodic re-consultation due to the generally time limited nature of exemptions, and in our experience this approach does not provide sufficient agility or flexibility. This is particularly relevant given the growing desire to extend information-sharing arrangements to a broader range of domestic and international participants who are not currently covered by existing exemption notices.

28. For completeness, we note that addressing these barriers would not dilute the banking industry's scam protection commitments as reflected in the recent updates to the Code of Banking Practice. Those commitments would continue to apply in full. Moving to a clearer, more permanent and broader safe harbour would provide greater certainty and help to enable more timely and effective information sharing and preventative action.