TCF submission to the Finance and Expenditure Committee

On the Fair Trading Amendment Bill 2026

16 July 2026

Introduction

1. This submission on the Fair Trading Amendment Bill (the Bill) is made on behalf of the New Zealand Telecommunications Forum (TCF), the industry association for the telecommunications sector. Our members include network operators, retail service providers, and the companies that own and operate cell towers.

2. We comment on:

    a. The safe harbour for scam disruption

    b. Penalty issues.

The safe harbour

Summary of proposed amendments

3. The TCF supports the introduction of a safe harbour for online service providers who act in good faith to disrupt scam activity. But as drafted, the safe harbour will not enable telecommunications service providers to act quickly and at scale. We propose some additions:

    a. That the safe harbour be available to service providers in three sets of circumstances:

        i. When a service provider is acting at the direction or request of government.

        ii. When a service provider acts on intelligence provided by a government agency or a trusted third party authorised through a government process. In such cases a service provider would be deemed to have reasonable grounds.

iii. When a service provider does its own due diligence (as already provided for in the Bill).

b. Making the safe harbour available to third party organisations that provide block lists and trusted flagger services to service providers. Such organisations should be selected through a simple registration process.

c. A defence against liability for investigative actions.

Telco scam disruption activity

4. Telecommunications providers are on the front line of scam disruption, investing significantly in tools and partnerships to combat them. They disrupt scam activity in three main ways:

    a. Domain name (website) blocking

    b. SMS (standard text message) blocking

    c. Call blocking.

5. Providers subscribe to validated malicious domain feeds maintained by specialist third-party providers. These feeds are populated using rigorous classification processes based on extensive sets of metrics and external intelligence. When a domain is validated as malicious it is published to their feed. Providers receive the feed and dynamically block automatically. This process is fully automated for the three mobile telecommunications networks in Aotearoa, with blocking taking place almost immediately after a domain is added to the list. Critically, telcos take no additional steps to examine or verify each domain. They rely on the specialist provider's classification, but will only do this where they have full confidence that the specialist has the expertise, tools and processes to identify scams swiftly and accurately. Requiring telecommunications providers to validate and confirm for themselves that a domain is malicious is not efficient, is resource intensive, and will slow the pace at which scam websites can be blocked.

Why a safe harbour is needed

6. The safe harbour is needed to cover the situations where service providers are asked to take blocking action, by an expanded number of organisations, in circumstances where they cannot examine and verify the basis of each request.

7. In these circumstances, a service provider may take action based on third-party identification of a scam, but may inadvertently disrupt a legitimate service. In such cases service providers could be found liable (in tort or negligence) for blocking a domain. If a legitimate business or agency has its domain blocked, its website cannot be accessed, it will not be able to operate and could lose revenue or cause loss to third parties. In such cases they could sue the service provider who did the blocking.

What is missing

8. The safe harbour as drafted will not be sufficient to protect service providers from liability and enable them to block scam websites at the scale and speed needed to combat rising levels of increasingly sophisticated scam activity. There are several elements missing.

    a. **An authoritative source** (from the government or a third party authorised by government) **on what websites to block**. This will enable telcos to act swiftly, by allowing them to rely on authorised intelligence without additional verification.

    b. **Protection for the specialist third parties** that produce block lists and offer trusted flagger services.

    c. Defence against liability for infringements for the **investigative actions** needed to identify scam websites. The safe harbour only applies to "any action they take to disrupt the activity" which may not be broad enough to cover the investigative phase.

An authoritative source on what to block

9. Having an authoritative source on what to block is important for three reasons: speed, liability and transparency.

10. Speed is everything. Scammers know that verification and approval processes take time and actively exploit that window. But specialist providers can detect and validate scams almost instantly. Using these feeds telcos can implement blocks in minutes provided that they have total confidence in the feeds and are protected when relying on them.

11. Without being able to rely on an authoritative source on what web domains, text messages or calls are most likely scams, and a legal protection for disruption of those activities, providers would need to do their own checks. They will not be able to automate the process and rely on the intelligence of specialist third parties that provide block lists. This manual checking means scams cannot be blocked at the necessary speed and scale, leaving consumers with less protection.

12. As currently drafted the requirement in 48U(1)(b) that "the provider of the online service has reasonable grounds to believe that the activity is a scam" makes online service providers responsible for determining what is a scam and puts the onus on them to prove that blocking was "reasonably proportionate to the nature of scale of the activity" and that they had reasonable grounds to block it. This is a very high bar to meet, with the conditions for claiming the safe harbour creating new verification burdens. The Bill doesn't define reasonable grounds and it is unclear whether reliance on a specialist third party's validated classification constitutes reasonable grounds.

13. Our suggested expansion of the the safe harbour removes the verification burden on service providers in two circumstances:

a. When a government agency (or organisation authorised by government) directs or requests a service provider to block a domain. If government is asking for something to be blocked it should not place a verification burden on the service provider.

b. When a service provider acts on intelligence provided by a government agency or an authorised third party. In such cases a service provider would be deemed to have reasonable grounds.

14. We propose that the Government put in place a simple registration process for authorising the specialist third parties that provide blocklists and trusted flagger services to service providers. This will give service providers a chain of trust up to government, and avoids a further administrative burden on service providers to do due diligence on the third party organisations and to justify this when seeking to rely on the safe harbour provision.

15. MBIE has been working on the design of a trusted flagger system, but has not shared details with industry stakeholders. Without this information it is not possible to know if the Government's trusted flagger proposal would meet industry requirements for an authoritative source. We recommend the Committee ask MBIE to share its proposal with industry as soon as possible, so that it can be taken into account when stakeholders address the Committee.

Third party specialist classification bodies have no protection

16. Section 48U applies only to providers offering 'online services', which includes telcos, website hosting companies, digital platforms and domain name registration services. The specialist third parties that provide block lists and trusted flagger services are most likely not 'online service providers' and would be outside the scope of the safe harbour provisions. This could deter these specialists from operating in New Zealand or result in them being so cautious that their intelligence is significantly watered down. We therefore propose that:

    a. Specialist third parties that provide blocklists and trusted flagger services be included in the safe harbour.

    b. As noted above, these organisations are authorised by the Government, through a registration process.

Investigative actions not covered by safe harbour

17. As currently drafted, the safe harbour only provides a defence against civil liability actions taken to *disrupt* scam activity. In our view, this is not broad enough to cover the investigative phase of trying to identify scams, which occurs prior to a disruption action being taken. This could limit the investigative actions taken by providers as if they don't end up taking any action, they could be liable for the work that was undertaken to get to that outcome.

18. We propose that section 48U is updated to make it clearer that "actions" include steps taken by a provider in the lead up to deciding whether or not to take any action to disrupt scam activity.

Penalties

Summary of submission points on penalties

19. We submit that:

    a. Evidence has not been presented to justify the proposed changes to penalties. FTA penalties have significantly increased over time, and have acted as an effective deterrent. The conduct of a small minority is better addressed by further prosecutions rather than a regime change.

    b. If pecuniary penalties are retained as proposed:

        i. The Bill should distinguish between system errors and deliberate misleading conduct.

        ii. More guidance will be needed on how to calculate the quantum of a pecuniary penalty.

No evidence to support the problem definition

20. We disagree with the problem definition that the "current penalties regime settings in the Fair Trading Act (FTA) are not as effective and efficient as they could be". No qualitative evidence was provided during the targeted consultation or in the regulatory impact statement (RIS) to justify the proposed changes to penalties. The RIS acknowledges there is limited data on how current penalties influence behaviours and what penalty level is effective.

21. On the contrary:

    a. Our members take their FTA compliance obligations seriously. When FTA-related errors occur, our members cooperate with the Commerce Commission and seek to meet their obligations to their customers. The RIS discounts the impact that providing information to traders and compliance advice letters have, with no effort apparently made to compare their effectiveness to the more costly preferred option.

    b. FTA penalties have significantly increased over time. These penalties do have an impact on business in New Zealand. Increases are also compounded in circumstances where a number of large corporates have recently received a 25 percent uplift on their penalties to ensure any fine "stings" (this is wording used in the High Court).

    c. There are only limited circumstances where the current penalties regime has failed to provide adequate deterrence, particularly to the level that warrants law reform on this scale. The conduct of a small minority can be addressed by further prosecutions, which inevitably lead to significant, and higher, penalties that take into account previous conduct.

d. Higher penalties under the Financial Markets Conduct Act 2013 (FMCA) has not acted as a deterrent given the large number of banks and insurers who have admitted liability and received civil pecuniary penalties in the last two years.

Systems errors should not be treated in the same manner as deliberate misleading conduct

22. FTA breaches can result from system errors. Businesses rely on a myriad of systems to deliver their services, such as consumer records and billing systems that create and send customer invoices at scale. As an illustration, monthly billing relies on a range of data sources and inputs to generate an accurate and timely invoice. An accidental failure of any of these systems could result in incorrect bills being sent, and in principle presentation of an incorrect bill could be considered a FTA breach (i.e. a trader misrepresenting the applicable price for a contracted service).

23. It is extremely concerning that system errors could attract penalties at the level proposed in the Bill, when they do not have a clear or controllable cause, in circumstances where a business has done all it can to reduce the possibility of error. Penalising system errors at these levels will deter business uptake of automated tools that are essential to drive productivity and growth such as AI (a strategy being promoted by the Government). Without these automated systems costs to consumers are likely to rise, and operators will be less willing to develop innovative new services that rely on these tools.

24. If the proposed penalties are retained, the Bill should distinguish between system errors and deliberate misleading conduct. The Committee should have no confidence that system errors will be distinguished in Commerce Commission enforcement practice. Enforcement practice to date shows little evidence that the Commission will recognise the practical distinction between incorrect statements that arise from a deliberate intention to mislead versus statements produced accidentally by system error.

25. We support the following recommendations from Business New Zealand:

    a. To introduce a safe harbour or materially reduced penalties for first-time inadvertent system failures where a business acts promptly to remediate and compensate affected customers, with full enforcement preserved for repeat or unremediated failures

    b. The director liability settings be reconsidered to ensure that personal exposure is proportionate in the context of system failures outside an individual's direct control.

More guidance would be needed to help calculate penalties

26. If pecuniary penalties are introduced as proposed, there will be no precedent to guide the courts on how to determine the appropriate penalty. While the Bill includes a list of considerations the Court must consider (and guidance for the maximum amount), it doesn't have any detail on how to calculate a penalty. This will extend the time it takes to reach settlements, and prevent some settlements being reached ahead of a trial. This problem could be addressed through guidance on calculating the quantum of the pecuniary penalty.

27. We also consider requiring parties to finalise an agreed penalty through a hearing in the High Court creates delays and increases costs, as well as generating uncertainty during the settlement negotiations, as the agreed figure could be changed by the High Court. Forcing the parties to the High Court could also create a precedent for future claims, which incentivises each party to maximise or minimise the settlement rather than prioritising efficient resolution of the matter. We propose adding a requirement that where the parties reach a settlement, that the claim should be settled in full and final out of court.

28. We also suggest that the order to the Commerce Commission to apply any penalty to their costs first should expressly extend to any investigation costs as well, so the Commerce Commission can't seek to recover these from defendants.

29. If there are any questions about this submission please contact kim.connolly-stone@tcf.org.nz in the first instance.