16 July 2026

Submission on “Fair Trading Amendment Bill”

Finance and Expenditure Select Committee

internetnz

Who we are and why we are submitting

InternetNZ manages the .nz domain space

InternetNZ | Ipurangi Aotearoa is an independent, purpose driven, membership organisation responsible for the administration and maintenance of the .nz Domain Name System (DNS) on behalf of all New Zealanders.

We maintain the .nz registry and DNS infrastructure that ensures .nz websites and email addresses connect reliably 24/7. This involves accepting and processing registration requests for the .nz top level country code (ccTLD), maintaining a database of domain name registration data, and providing name servers to publish the zone file (i.e., information about the location of a .nz domain name) throughout the Internet.

The Domain Name Commission (DNC) (a subsidiary of InternetNZ) oversees the .nz domain name market, enforces the .nz Rules, authorises and de-authorises registrars, investigates complaints, and operates a dispute resolution service.

Revenue generated through the operation of .nz is reinvested in the ongoing maintenance of critical Internet infrastructure and global internet governance, informing Internet-related public policy, and supporting initiatives that strengthen Internet access, use and trust across communities in Aotearoa New Zealand.

You can read more about our work here and in our latest Annual Report.

Executive Summary

This submission responds to:

- the introduction of a legal “safe harbour” for online service providers taking voluntary scam disruption action proposed in the Fair Trading Amendment Bill, and;
- the non-legislative option being scoped to establish designated expert entities to identify scam disruption activity (referred to as a "trusted flagger”) set out in the accompanying Regulatory Impact Statement.

Overall we support both the introduction of the legal safe harbour and the establishment of a trusted flagger network. In our view there is a strong case to legislate the trusted flagger to provide entities higher certainty to act and assurance that their actions will meet the conditions of the safe harbour. The establishment of a legislated trusted flagger network alongside the proposed legal safe harbour will remove legal liability concerns that are acting as a barrier to timely voluntary scam disruption, and strengthen the ability to take timely disruption action through co-ordination across the ecosystem.

InternetNZ has an important and distinct role, that is small in scope, in scam disruption at the DNS level through the DNC (a subsidiary of InternetNZ) and by

operating the .nz registry. The DNC's scam disruption role currently involves ensuring .nz domain name registrant[1] information is correct and includes suspending or cancelling a .nz domain name if registration or identity data cannot be verified.

We note increasing attention within our own industry to do more to combat industrial level scams and fraud schemes that include technical abuse of DNS infrastructure including for delivery of phishing and malware. Generally our industry does not consider it has a role in judging content or content moderation. Locally, we have ongoing engagement with government agencies and the New Zealand Anti-Scam Alliance as part of the wider ecosystem of public and private actors working on detection of organised scam campaigns.

In this submission we note that for the legal safe harbour to cover appropriate domain level responses to scams now and in the future, InternetNZ which operates the .nz registry and the DNC need to be explicitly covered in the definition. To support this inclusion we recommend a new definition of *Internet domain name registration service* is added under new section 48U (4) to correctly describe the *type of services* that need to be covered by the safe harbour and bring about the policy intent.

We also suggest further consideration of some minor drafting changes that would ensure the proposed legislation better captures scam disruption processes at the domain name level accurately.

We recommend InternetNZ and the DNC are included under the legal safe harbour provision

Due to the narrowly scoped, but important role InternetNZ through the .nz registry and the DNC can play in scam disruption, we recommend both are included under the legal safe harbour provision proposed in this bill.

We propose this is enabled through the addition of the following new definition of an *Internet domain name registration service* to the new section 48U (4):

Internet domain name registration service means -

a) a service providing domain name registration services, whether wholesale or retail; and

b) a service providing oversight and compliance services to a registration service, including a service who has the power to validate, reject, suspend or cancel domain name registrations.

This would include InternetNZ as operator of the .nz registry as a service, and the DNC as an oversight and compliance service.

[1] A **registrant** is the individual or entity who holds the license that allows them to use a registered domain name for the duration of the license period. Definition adapted from .auDA definition as listed here: https://www.auda.org.au/news-insights/blog/key-terms-explained-registrants-registrars-resellers-and-registry/

InternetNZ plays a role in scam disruption through the .nz registry and the .nz Domain Name Commission

One way online scams are conducted is through DNS abuse. This is the use of the domain name system to intentionally deceive or cause harm. It includes:

- Registration abuse: where incorrect, fraudulent or misleading registration data is provided to a registry, and;
- Technical abuse of domain names: for example, phishing attacks,[2] delivery of malware[3] and pharming[4].

InternetNZ through the .nz registry has the technical ability to play a role in scam disruption at the DNS level. If directed by a competent authority, the registry can disable a domain name at the point of registration by implementing a registration hold or a domain name can be taken out of zone through suspending or cancelling it. When this happens the entire domain name is taken down, and any specific content or connected services is not able to be isolated for suspension or removal.

The .nz Domain Name Commission (DNC), is an independent subsidiary of InternetNZ and has an oversight role of the .nz ccTLD. The DNC's oversight approach is designed to ensure the ongoing security, stability, and resilience of the .nz domain name space and that the integrity of the .nz register is maintained. It aims to ensure a trusted and secure scheme of registration and renewal is in place that domain name holders can rely on.

DNC plays a limited but important role in scam disruption focusing on intervention where a domain name is being used, or is likely to be used, for scam activity. DNC scam disruption activity is conducted by verifying registration information to ensure compliance with the .nz Rules that specify registrant information must be of an identifiable individual over the age of 18 or a lawfully constituted entity[5]. The .nz Rules enable the DNC to suspend or cancel a .nz domain name via the .nz registry if

---

[2] **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or 'look-alike' emails, or luring end users to copycat websites. https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf

[3] **Malware** is malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.

[4] **Pharming** is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to [the attacker's] site instead of the one initially requested.

[5] .nz Rules can be found here: https://internetnz.nz/assets/Archives/nz-Rules/Version-3.2-of-.nz-Rules-17-March-2026.pdf

the domain name holder is not contactable, does not validate the data in the registration record, or if they do not verify their identity.

The DNC checks registration information through data validation and identity verification auditing. These are undertaken both proactively and reactively and, if failed, can result in the suspension of a domain name.

The DNC currently does not make judgments on the use of domain names, except in exceptional circumstances, such as when ordered to do so by competent authorities. Exceptional circumstances include terrorist and cyber security attacks, and other extraordinary events where the "use of the .nz domain name is causing, or may cause, irreparable harm to any person or to the operation or reputation of the .nz domain space".[6]

Based on shifts from the industry to do more to combat evidenced technical DNS abuse including phishing and malware, InternetNZ and the DNC are currently considering whether a further role could be undertaken to better respond to technical abuse in the .nz domain name space.

A legislated trusted flagger is important to enable scam disruption and give best effect to the safe harbour

We agree the establishment of a trusted flagger network to identify suspected scam activity will support entities to act. To give entities the confidence their actions will meet the conditions of the legal safe harbour and motivate scam disruption we recommend the trusted flagger is legislated. A legislated trusted flagger model would ensure the groups and processes involved maintain the 'trusted' status of the flagger network and effectively motivates voluntary action.

A trusted flagger with a statutory mandate would deliver the necessary assurance to the DNC that the actions are proportionate and that the legal thresholds of the safe harbour provisions are met. We note the majority of equivalent ccTLDs will only act on criminal conduct if directed to by Court Order or following a takedown direction from an empowered agency. We can provide you further information on other international ccTLD scam disruption practices upon request.

We also note the importance of the trusted flagger having appropriate information sharing abilities with both government agencies and private sector actors. A statutorily recognised trusted flagger would ensure appropriate controls around information sharing are adhered to.

[6] As set out in the .nz Rules: https://internetnz.nz/assets/Archives/nz-Rules/Version-3.2-of-.nz-Rules-17-March-2026.pdf

Recommendations

We recommend InternetNZ and the DNC are included under the legal safe harbour provision

Due to the narrowly scoped, but important role InternetNZ and the DNC, through the .nz registry can play in scam disruption, we recommend both are included under the legal safe harbour provision proposed in this bill.

To enable this inclusion we recommend the following definition of 'Internet domain name registration service' is added to section 48U (4):

Internet domain name registration service means -

a) a service providing domain name registration services, whether wholesale or retail; and

b) a service providing oversight and compliance services to a registration service, including a service who has the power to validate, reject, suspend or cancel domain name registrations.

Sub-point (a) in this definition, describes *the type of service* included as an *Internet domain name registration service* and would include all Registrars and Registries including the InternetNZ .nz registry. This is consistent with the other online service definitions, including *web hosting service* and *digital platform*, set out in proposed changes under 48U (4).

Sub-point (b) in this definition extends coverage to the oversight and compliance services of domain name services to ensure entities who play an active role in scam disruption at the DNS level are included under the legal safe harbour provision. This will cover the DNC due to the oversight and compliance role they hold for the .nz ccTLD.

Other Comments

- We note the phrasing of new section 48U (2) (c) (i) states: '*while the provider had reasonable grounds to believe that the activity* ***was*** *a scam*'. The reference to '*was*' in 48U (2) (c) (i) may be interpreted as applying only to scam activity that has been activated. We recommend phrasing is considered to clarify that this clause includes proactive disruption to prevent scam activity from occurring. This could include: 'was, or will be used for, a scam'.
- Online scams may be facilitated through automated processes, Artificial Intelligence (AI) agents, and sophisticated international criminal networks where it is difficult to identify the involvement of a person in the scam activity. We suggest further consideration is given to the reference to '*person*' in new section 48U (1) (a) to ensure it appropriately covers instances where personal involvement in scam activity is not able to be identified.

- New section 48U (4) lists the definition of use as: '***use*** *of an Internet domain name registration service includes use* ***by the registrant*** *of a domain name registered by the service.*' This definition would exclude use where, for example, a domain name is registered for a business and the registrant authorises employees of the business to use or manage services associated with the domain name. We suggest you consider removing the words '*by the registrant*' so this definition covers all instances where a domain name is used.