# Regulatory Impact Statement: Updating the penalties regime in the Fair Trading Act 1986

| | |
|---|---|
| **Decision sought** | Analysis produced for the purpose of informing final Cabinet decisions |
| **Agency responsible** | Ministry of Business, Innovation and Employment (**MBIE**) |
| **Proposing Minister** | Minister of Commerce and Consumer Affairs |
| **Date finalised** | 10 September 2025. |

The Minister proposes changes to the *Fair Trading Act 1986* to strengthen penalties and support better compliance. These changes respond to concerns that current penalties are often too low to deter business behaviour, and that the enforcement process can be inefficient.

The goal is to make penalties more effective, reflect harm and commercial gain, and align with other laws. This will help create a fairer trading environment for consumers and businesses.

Two key changes are proposed:

- Shift most criminal offences to civil penalties. Serious breaches, like obstructing investigations, would remain criminal.
- Increase maximum penalties. The most serious breaches would face penalties similar to those under the *Financial Markets Conduct Act 2013*.

The proposals are based on targeted consultation and follow guidance from the Law Commission and the Legislation Design and Advisory Committee.

## Summary: Problem definition and options

***What is the policy problem?***

The Fair Trading Act already includes a three-tier penalties regime, but the current levels are outdated and too low to deter non-compliance. Tier 1 offences carry maximum penalties of $200,000 for individuals and $600,000 for body corporates, with lower penalties for Tier 2 and Tier 3 offences. The penalties regime in the Fair Trading Act is increasingly seen as outdated and ineffective. Several signs suggest it is not working as intended:

- **High and rising complaint volumes:** The Commerce Commission receives a large and growing number of complaints. Between 2020 and 2024 complaints rose by around 22.7 per cent.
- **Penalties too low to influence behaviour:** The Commission has advised that current penalties are often outweighed by the commercial gain from breaching the Act. For example, One New Zealand (formerly Vodafone) was fined $3.6 million for misleading conduct, while the estimated gain was over $22 million See explanatory note on estimated commercial gain at the bottom of page 8
- **Inefficient enforcement:** Criminal proceedings require proof beyond

reasonable doubt. This can be slow, complex, and resource-intensive. The Commission has said this burden can prevent it from taking action, even when harm is clear.
- **Misalignment with other legislation**: The Fair Trading Act relies on criminal offences, while other regimes like the Financial Markets Conduct Act and *Commerce Act 1986* use civil penalties. This creates uncertainty and inconsistency for businesses and regulators.

These issues limit the effectiveness of the Act and undermine its purpose: to protect consumers, support fair competition, and build confidence in the market.

***What is the policy objective?***

To modernise and strengthen the Fair Trading Act's penalties regime so that it:
- Provides meaningful and proportionate penalties.
- Enables more efficient enforcement by the Commerce Commission.
- Aligns with other commercial legislation.
- Supports a fair and confident trading environment.

***What policy options have been considered, including any alternatives to regulation?***

Two proposals were assessed, each with multiple options:

**Proposal A:** Enhance enforcement of the Fair Trading Act
- Option One: Keep the current criminal-only model.
- Option Two (preferred): Introduce a civil pecuniary penalties regime to the Act to enhance compliance.
- Option Three: Provide additional resources to the Commission to enhance compliance.

**Proposal B:** Increase maximum monetary penalties.
- Option One: Keep current penalty levels.
- Option Two: Align Tier 1 penalties with the Commerce Act and increase Tiers 2 and 3.
- Option Three (preferred): Align Tier 1 penalties with the Financial Markets Conduct Act and increase Tiers 2 and 3.
- Option Four: Align Tier 1 penalties with the Australian Consumer Law and increase Tiers 2 and 3.

***What external consultation has been undertaken?***

MBIE ran a two-week targeted consultation starting 28 July 2025, seeking views on shifting to civil pecuniary penalties and raising penalty levels to improve deterrence. MBIE received 18 written submissions and held meetings with consumer groups, businesses, and law firms. While we acknowledge the consultation period was short, officials have reflected stakeholders' main concerns in the proposals and analysis set out in this document.

Consumer groups generally supported the proposals. Business groups raised concerns about proportionality and safeguards. Law firms supported modernisation but emphasised the need for a clear evidence base.

***Is the preferred option in the Cabinet paper the same as the preferred option in the RIS?***

Yes. Both recommend:
- Shifting most criminal offences to civil penalties (Proposal A, Option Two).
- Increasing penalties in line with the Financial Markets Conduct Act (Proposal B, Option Three).

## Summary: Minister's preferred option in the Cabinet paper

### Costs (Core information)

**Monetised costs:**

- Higher penalties for businesses that breach the Act. For example, Tier 1 penalties increase from $600,000 to up to $5 million or more, depending on commercial gain.
- Potential increase in enforcement activity by the Commerce Commission, with any associated costs likely to be met from within baselines.

**Non-monetised costs:**

- Increased compliance costs and legal exposure for businesses that breach the Fair Trading Act.
- Possible reputational impacts from civil proceedings, though less than criminal convictions.

**Distributional impacts:**

- Costs fall primarily on businesses that breach the Act.
- Larger firms may be more affected due to higher potential penalties linked to commercial gain.
- Consumers and compliant businesses are not expected to bear direct costs.

### Benefits (Core information)

**Monetised benefits:**

- Reduced consumer harm: Fewer breaches mean fewer consumers are harmed. Eg by overpaying or receiving goods or services they did not want.
- Improved market competition: The proposal helps level the playing field by discouraging misleading conduct that could give a firm an unfair competitive advantage. This can lead to better pricing, more efficient markets, and increased consumer trust.
- Avoided enforcement costs: Civil proceedings are generally less costly than criminal prosecutions, saving resources for the Commerce Commission and courts.

**Non-monetised benefits:**

- More flexible enforcement tools for the Commerce Commission.
- Avoidance of criminal stigma for businesses that breach the Act, while still enabling meaningful penalties.
- Increased consumer confidence in fair trading practices.

**Distributional impacts:**

- Benefits accrue to consumers through fewer breaches and fairer market practices.
- Commerce Commission gains a more flexible enforcement toolkit.
- Businesses benefit from clearer alignment with other commercial legislation.

### Balance of benefits and costs (Core information)

The RIS suggests that the benefits of the Minister's preferred option are likely to outweigh the costs. This is based on qualitative evidence, comparisons with other legislation, and feedback from targeted consultation.
**Benefits vs costs**: The preferred option is expected to:

- Improve compliance by increasing the financial consequences of breaching the Act.
- Make enforcement more efficient by shifting to civil proceedings.
- Ensure penalties are proportionate to the harm caused and commercial gain made.

Costs will mainly affect businesses that breach the Act. Benefits will be shared across consumers, compliant businesses, and regulators.
Change over time: The benefit-cost balance is expected to improve over time. Higher penalties, once imposed in case law, may reduce the number of breaches in future. This could lower enforcement costs and reduce harm to consumers. The Commerce Commission will be able to take action more efficiently, especially for lower-level breaches.

**Judgement confidence:** The RIS draws on enforcement experience, stakeholder feedback, and alignment with other legislation. It uses guidance from the Law Commission on pecuniary penalties to support the shift to civil enforcement. However, there is limited empirical data on deterrence and optimal penalty levels.

## Implementation

**Responsibility**:

- MBIE will lead legislative changes (MBIE is responsible for administering the Act).
- The Commerce Commission will enforce the penalties regime (the Commission is the existing enforcement agency for the Act).

**Risks and mitigation**:

- Risk of over penalisation mitigated by judicial discretion and tiered penalty structure.
- Stakeholder concerns about proportionality addressed by aligning with FMC Act rather than Commerce Act or Australian law.
- Select Committee process will allow further refinement and stakeholder input, helping to address concerns about the short consultation timeframes to date.

**Timing and transition**:

- Bill planned for introduction by December 2025 (Category 5).
- Transitional arrangements may be needed to support implementation and awareness.

## Limitations and Constraints on Analysis

This analysis has several limitations that affect the level of confidence in the conclusions drawn:
**Evidence gaps:** There is limited data on how current penalties influence business behaviour or what penalty levels are most effective. Most of the analysis relies on qualitative indicators, such as complaint volumes, enforcement challenges, and case studies.
**Time and consultation constraints:** The policy process was completed at pace. Consultation was targeted rather than public and ran for two weeks. While this provided useful feedback, some stakeholders raised concerns about the timeframe and scope of engagement.
**Scope of proposals:** Some proposals consulted on are not being progressed at this stage. This reflects stakeholder concerns and the need for further evidence before advancing more complex or contentious changes.

**Use of comparative frameworks:** The analysis draws on penalty settings in the Financial Markets Conduct Act as a benchmark. This supports consistency across regimes but may not fully reflect the unique features of the Fair Trading Act.
**Law Commission guidance:** The design of the civil regime is informed by the Law Commission's guidance on pecuniary penalties. This supports the proportionality of shifting most breaches from criminal to civil enforcement.
**Judgement confidence:** The RIS presents a reasoned view that the benefits of the preferred option are likely to outweigh the costs. However, this is a cautious judgement. The evidence base is limited, and further scrutiny through the Select Committee process will be important to test and refine the proposals.

**I am satisfied that, given the available evidence, this RIS represents a reasonable view of the likely costs, benefits and impact of the preferred option.**

**Responsible Manager's signature:**
**Glen Hildreth, Manager, Consumer Policy Building, Resources and Markets**
**5 September 2025**

## Quality Assurance Statement

| **Reviewing Agency:** MBIE | **QA rating:** Partially meets |
|---|---|

**Panel Comment:** Quality Assurance Panel from MBIE has reviewed the Regulatory Impact Statement (RIS) prepared by MBIE titled, "Updating the penalties regime in the Fair Trading Act 1986" in September 2025.

The Panel consider that the information and impact analysis summarised in the RIS partially meets the Quality Assurance criteria.

While the Panel considers that "partially meets" assessment reflects the limitations in the available evidence and empirical data, the Panel notes that this limitation has been addressed in part by aligning policy options with comparable legislation.

## Section 1: Diagnosing the policy problem

### What is the context behind the policy problem and how is the status quo expected to develop?

1. The *Fair Trading Act 1986* (the **Fair Trading Act**, or the **Act**) is a cornerstone of New Zealand's consumer protection framework. It aims to foster a trading environment where consumers' interests are protected, businesses compete effectively, and consumers and businesses participate confidently. To this end, the Act:
    a. prohibits certain unfair conduct and practices in relation to trade
    b. promotes fair conduct and practices in relation to trade
    c. provides for the disclosure of consumer information relating to the supply of good and services
    d. promotes safety in respect of goods and services.[1]
2. All breaches of the Act carrying monetary penalties are determined under criminal law. Breaches are prosecuted by the Commerce Commission in the District Court or dealt with through infringement notices for low-level offences. Criminal offences must be proven beyond reasonable doubt, and penalties are capped at relatively low levels.
3. The current penalties regime groups offences into three tiers, based on the type and seriousness of the conduct. The highest tier (Tier 1) applies to unfair conduct (such as misleading representations), product and service safety, and pyramid selling schemes. Tier 1 offences carry a maximum penalty of $200,000 for individuals and $600,000 for body corporates, except for pyramid schemes, which carry a $600,000 maximum for both.
4. Tier 2 applies to breaches of management banning orders under Part 5A of the Act. These orders are used to prevent individuals from managing businesses where serious misconduct has occurred. The maximum penalty for Tier 2 offences is $60,000 for individuals.
5. Tier 3 covers lower-level breaches, including failures to comply with consumer information standards and rules around consumer transactions and auctions. These offences typically involve administrative or technical non-compliance. The maximum penalties are $10,000 for individuals and $30,000 for body corporates The penalties regime in the Act has not been reviewed for around ten years.
6. Stakeholder feedback gathered through targeted consultation suggests that the current penalties regime is not operating as intended. Consumer NZ described the penalties as too low to deter breaches, citing persistent issues such as misleading pricing and advertising. FinCap noted that weak enforcement discourages financial mentors from reporting breaches, contributing to ongoing harm. Citizens Advice Bureau New Zealand and

[1] See the purpose statement in section 1A of the Act, https://www.legislation.govt.nz/act/public/1986/0121/latest/whole.htm#DLM5836703.

Community Law Centres Aotearoa stated that the regime fails to hold larger businesses accountable and does not incentivise compliance.

7. Legal and commercial submitters also raised concerns about the regime's effectiveness. MinterEllisonRuddWatts and Summerset Group Holdings Limited observed that the current penalties lack proportionality and may not reflect the seriousness of some breaches. The New Zealand Law Society noted that resourcing constraints and procedural complexity can limit enforcement outcomes. Buddle Findlay acknowledged that while reputational risk may deter some businesses, penalties are often cumulative and still insufficient to shift behaviour.

8. These views suggest that, without reform, the status quo is likely to result in continued non-compliance, limited deterrence, and constrained enforcement capability.

## What is the policy problem or opportunity?

9. The current penalties regime in the Fair Trading Act is no longer fit for purpose. It does not provide sufficient deterrence for many types of conduct, is inefficient to enforce in practice for a lot of the commercial conduct the Act deals with, and it is increasingly misaligned with other commercial legislation in New Zealand and overseas. These issues limit the Commerce Commission's ability to respond effectively to breaches of the Act and create uncertainty for businesses about the consequences of non-compliance.

### Issue one: High and rising complaint volumes suggest persistent non-compliance

10. The Commerce Commission continues to receive a high volume of complaints about potential breaches of the Fair Trading Act, with a clear upward trend over time. Between July 2020 and July 2025 total complaints on the Fair Trading Act rose by around 22.7 per cent increasing from 8,841 to 10,851. Over this time the Commission received over 48,000 complaints related to the Fair Trading Act. This sustained level of complaints suggests that non-compliance with the Act is widespread and persistent.

11. Common complaint themes include misleading advertising, inaccurate pricing, refund refusals, non-delivery of goods, and subscription traps.

12. These complaints reflect a range of consumer harms and indicate that many businesses may not be sufficiently deterred from engaging in unfair practices. The volume and nature of complaints also place pressure on the Commerce Commission's resources and may undermine public confidence in the effectiveness of the Act.

13. Confidentiality and Confidentiality both reported high and persistent volumes of consumer complaints about misleading pricing, advertising, and other breaches, supporting the view that non-compliance remains widespread. Confidentiality

Confidentiality

14. Confidentiality noted that weak enforcement discourages reporting, particularly among vulnerable consumers, and that the current regime does not provide sufficient incentive for businesses to comply.

## Issue two: The criminal penalties regime does not effectively deter, or address, breaches of the Act

15. In its 2023 Briefing to the Incoming Minister, the Commerce Commission noted that the Fair Trading Act could benefit from improvements, and that current penalties are often "too weak to deter repeat offending"[2]. The Commission also highlighted that some firms treat fines as a "cost of doing business" [3] and that "commensurately chunky penalties"[4] are needed to prevent sustained breaches by powerful firms. The penalties regime is intended to deter breaches and equip courts to respond effectively when breaches happen. However, the current regime does not provide sufficient deterrence for many types of conduct.

16. Businesses typically assess the likelihood of detection, potential penalty and expected commercial gain before engaging in potentially unlawful conduct. In practice, this means businesses weigh up the risk of enforcement against the financial benefit of non-compliance[5]. And under the current penalties regime, that balance can often favour breaching the Act given the relatively low penalty levels currently. This issue is particularly significant for large scale businesses because the significant commercial gain they can make from offending can easily outweigh even the maximum penalty in the Act currently.

17. Between 2020 and July 2025, the Commerce Commission secured over 50 Fair Trading Act enforcement outcomes involving financial penalties. Penalties ranged from under $10,000 to over $5.9 million, with several cases involving repeat offenders. Despite these outcomes, the average penalty remains modest relative to the commercial gain in many cases. For example, in a recent case taken against One New Zealand (formerly Vodafone), the company was convicted on 18 counts under section 11 of the Act and fined $3.6 million for misleading customers about its FibreX broadband service. The Commission estimated that the commercial gain from the conduct was over $22 million. This gap highlights the limited deterrence effect of current penalty levels

See explanatory note on the estimated commercial gain

18. This case was not an isolated incident. Vodafone has a long history of enforcement action under the Fair Trading Act, including:

---

[2] New Zealand Parliament, *Compendium of Annual Review Reports 2023/24,* page 12.
[3] Commerce Commission, *Briefing to the Incoming Minister – Commerce and Consumer Affairs* (November 2023), p. 16. https://comcom.govt.nz/__data/assets/pdf_file/0010/342100/Briefing-to-the-Incoming-Minister-Commerce-and-Consumer-.pdf
[4] Rebecca Stevenson, 'It has to hurt': Commerce Commission chairman John Small says fines for breaching consumer law are too weak, Interest.co.nz, 6 September 2023. Available at: https://www.interest.co.nz/business/124137/it-has-hurt-commerce-commission-chairman-john-small-says-fines-breaching-consumer
[5] Law Commission, *Pecuniary Penalties – Guidance for Legislative Design,* page 16.

This explanatory note, added on 26 May 2026 provides additional context to the information in the Regulatory Impact Statement and was not part of the material considered by Cabinet when decisions were taken. The RIS refers to an estimated "commercial gain" of over $22 million in the Vodafone FibreX case. This figure reflects an estimate of additional subscriber revenue identified by the Commerce Commission, rather than a quantified measure of total commercial gain. The courts did not determine a specific level of commercial gain. The example is included to illustrate the potential scale of financial incentives, rather than as a precise measure or a basis for the preferred option

a. A **$960,000 fine in 2012** for misleading broadband and mobile promotions;

b. A **$165,000 fine in 2016** for false price representations in mobile plan invoices;

c. A **$350,000 fine in 2019** for false invoicing over a six-year period;

d. Multiple formal warnings between 2011 and 2020 for misleading advertising, loyalty promotions, and pricing claims.

19. This pattern of repeat offending over more than a decade suggests that the current penalties regime has not provided sufficient deterrence for breaches by a high-profile, well-resourced firm. It illustrates how some businesses may treat fines as a manageable cost of doing business, particularly where the commercial gain from non-compliance significantly exceeds the penalties imposed.

20. Another example of the back of deterrence is the Lion's Share gifting scheme, operated by Shelly Cullen. In 2024, the court imposed a penalty of $5.9 million — the highest ever imposed under the Act – consisting of the maximum fine available for pyramid conduct of $600,000 and the amount of estimated commercial gain of $5.3 million.[6] Despite this, Ms Cullen publicly stated: "I'm going to make history as one of the biggest scammers in New Zealand," and "What's the consequences, $600,000 slap on the hand?" Her comments, recorded in sentencing notes, reflect a clear disregard for the law and suggest that even substantial penalties may not deter intentional or repeat offending. This case highlights the need for a regime that can respond proportionately to serious misconduct and escalate enforcement where required.

21. The limited deterrence effect of the current regime likely stems from its criminal law model and the relatively low monetary penalties available. Because criminal convictions carry reputational stigma, the regime relies on lower fines to balance that punitive effect. This limits the ability to impose higher monetary penalties that would more effectively deter breaches and which could change the equation for businesses considering whether breaching the Act is worthwhile.

22. However, businesses are primarily motivated by financial outcomes. Significant monetary penalties are likely to be a more effective deterrent than the threat of criminal convictions.[7] This suggests that the current criminal law-based regime may not be well suited to deterring breaches of the Act.

23. Confidentiality and Confidentiality stated that current penalties are often treated as a cost of doing business, particularly by larger firms, and do not provide an effective deterrent. In

[6] Under section 40A of the Act, the court may impose an additional penalty equal to the commercial gain from a breach of section 24 (pyramid selling), if satisfied the breach occurred in the course of producing a commercial gain. However, this provision applies only to pyramid schemes and does not extend to other types of unfair conduct, limiting its deterrent effect.

[7] Law Commission. Ibid.

their submission ConsumerNZ said "*We strongly agree the current penalties regime in the Fair Trading Act (FTA) is not as effective and efficient as it could be and does not provide businesses and others with the right incentives to comply*". FinCap and Consumer NZ argued that the low level of penalties and the difficulty of securing criminal convictions mean that repeat offending is not uncommon.

### Issue three: The criminal law regime is inefficient for addressing certain breaches of the Act

24. The Commerce Commission has also noted that, under the current criminal regime, it is administratively inefficient to take action against many breaches, even where there is clear evidence of consumer harm. This is primarily because criminal proceedings must be proven to the higher standard of 'beyond reasonable doubt', which makes enforcement action slower, more complex, and more resource intensive.

25. The cost and effort of meeting the criminal standard of proof can discourage enforcement action. In some cases, the Commerce Commission may decide not to pursue breaches of the Act where the harm is clear but the evidentiary burden is too high. This means some offending may go unaddressed, even when it causes direct consumer harm, limiting the Act's ability to prevent unfair conduct.

26. Additionally, many of the provisions of the Act are strict liability offences. In these cases, imposing criminal liability, including the stigma of a conviction, may not be proportionate to the nature of the conduct. This raises fairness concerns and further complicates enforcement.

27. Between 2020 and 2025, the Commerce Commission received over 10,000 Fair Trading Act-related concerns annually. However, only a small proportion of these resulted in litigation, typically 2–4 per cent per year. Most investigations led to non-litigation outcomes, with 70–80 per cent resulting in information being provided to traders and 12–18 per cent resulting in compliance advice. Warnings, infringement notices, and settlements were used sparingly. See Annex Two for more detail on enforcement outcomes over the past five years.

28. In 2024 alone, the Commerce Commission received over 11,000 complaints, reflecting a significant increase in consumer concern. While the Commission has expanded its litigation fund to pursue more cases, many complaints are addressed through non-litigation tools such as formal warnings and compliance advice letters. For example, the Commission issued a warning to Law Debt Collection Ltd for misleading representations and a compliance advice letter to Vector regarding unfair contract terms. These tools are useful but may not provide sufficient deterrence for businesses that consider the potential high commercial gain from conduct in undertaking a breach of the Act. The proposed reforms aim to strengthen the Commission's enforcement toolkit by enabling more efficient civil proceedings and higher penalties.

29. However, officials consider that criminal liability is suitable for a small number of serious breaches. These include cases where the course of law or justice is impeded, such as breaching a management banning order or

obstructing the Commerce Commission's investigations, as well as other 'truly criminal' types of conduct like operating a pyramid scheme or major product safety breaches. In these instances, criminal convictions and the higher procedural safeguards afforded by criminal proceedings are appropriate.

30. Confidentiality and Confidentiality highlighted that the high burden of proof required for criminal prosecutions can discourage both complaints and enforcement action, leading to under-reporting and under-enforcement. In their submission Confidentiality said "*We consider the lower burden of proof will make it easier for the Commission to bring successful actions against businesses that have breached the FTA. We also consider that more effective and visible enforcement of the law is likely to lead to more reporting of potential breaches*" Confidentiality and Confidentiality noted that civil proceedings may allow for more flexible and timely enforcement.

### Issue four: The penalties regime in the Fair Trading Act is out of step with how other commercial legislation is enforced

31. The Fair Trading Act's penalties regime is based on criminal law, which is increasingly out of step with other commercial legislation in New Zealand and Australia. Other regimes use civil penalties with higher maximum monetary penalties to address similar types of conduct. This misalignment creates inconsistency and enforcement challenges.

32. Both the *Commerce Act 1986* and the *Financial Markets Conduct Act 2013* (the **FMC Act**) use civil proceedings and provide for higher monetary penalties than the Fair Trading Act. While these Acts have different purposes, they all deal with commercial conduct. The FMC Act in particular, addresses similar behaviour to the Fair Trading Act, such as misleading and deceptive conduct and unsubstantiated representations, but does so through a different enforcement model.

33. Inconsistent penalties for similar conduct across commercial legislation can create confusion and inefficiencies for regulators and businesses. For regulators, it complicates decisions about which enforcement pathway to pursue, such as whether the Financial Markets Authority should act under the FMC Act or refer a matter to the Commerce Commission under the Fair Trading Act. This can lead to duplicated effort, delays, and uncertainty about jurisdiction.

34. For businesses, the lack of alignment makes it harder to understand and compare the consequences of non-compliance, especially for firms operating across sectors. These overlaps reduce predictability, increase compliance complexity, and undermine the clarity and coherence that commercial law should provide.

35. Alignment also supports proportionality in penalty design. It ensures that similar types of conduct attract similar penalties across regimes, and that more serious breaches are penalised more severely. For example, misleading conduct under the FMC Act may attract penalties of up to $5 million, while similar conduct under the Fair Trading Act is capped at $600,000. Under the Commerce Act, penalties for anti-competitive conduct

can reach $10 million or more, or be scaled to three times the commercial gain or 10% of turnover.

36. These settings reflect the seriousness of the conduct and ensure that penalties are proportionate to the harm caused. In contrast, the Fair Trading Act's lower penalty ceiling may understate the impact of breaches and reduce deterrence. Greater alignment helps ensure that penalties are scaled appropriately to the nature and impact of the breach, supporting fairness, coherence, and predictability in the regulatory system.

37. In Australia, the 'Australian Consumer Law' (included within the Competition and Consumer Act 2010) provides for both criminal and civil pecuniary penalties, depending on the nature and seriousness of the breach. s. In 2022, Australia significantly increased its penalties in response to concerns that existing levels were too low to deter breaches. This reinforces the trend toward civil enforcement models for commercial conduct with high penalty levels for breaches.

38. Confidentiality and Confidentiality supported aligning the Fair Trading Act's penalties regime with other commercial legislation, such as the FMC Act, to improve consistency and predictability for businesses.

## What objectives are sought in relation to the policy problem?

39. The objectives of this work are to ensure that the Fair Trading Act has an up-to-date, effective and efficient penalties regime that:

    a. Supports a fair and confident trading environment for consumers and businesses.

    b. Provides meaningful and effective deterrence and proportionate punishment for breaches.

    c. Enables more effective and efficient enforcement by the Commerce Commission.

    d. Aligns with other similar commercial legislation in New Zealand, and comparable international approaches.

## What consultation has been undertaken?

40. MBIE undertook a two-week targeted consultation between 28 July and 8 August 2025 on the proposals in this paper, alongside other potential changes.

41. Stakeholders consulted included industry bodies, consumer advocacy organisations, law firms, financial institutions, utilities companies, dispute resolution services, standards organisations, and government agencies. MBIE received 18 written submissions. MBIE held meetings with key industry groups and other stakeholders, such as larger law firms.

42. While some supported the proposals, businesses and business advocates raised strong concerns about the consultation process and proposals. Key themes included:

    a. The size of the consultation paper and the short consultation timeframe (two weeks) limited meaningful engagement. Some requested public

consultation, rather than just targeted consultation, given the significance of the changes proposed.

b. Concerns about whether the problem was clearly defined and whether sufficient evidence had been provided to support the proposed changes.

c. The potential impacts on compliance costs and investment certainty.

d. Concerns about the shift from a criminal law-based to a civil law-based penalties regime and size of the proposed maximum monetary penalties.

43. Feedback from submitters has informed the development of the preferred approach in this RIS. MBIE's targeted consultation paper, sought views on seven options for reforming the penalties regime, including replacing criminal offences with civil pecuniary penalties, increasing maximum fines, and expanding infringement offences.

44. Submitters broadly supported modernising the regime but raised concerns about proportionality, evidential thresholds, and the need to retain criminal liability for serious breaches. In response to this feedback, MBIE refined the scope of proposed penalties, confirmed the retention of criminal offences for conduct involving intent or obstruction, and clarified the rationale for civil penalties in cases of strict liability. The RIS reflects these refinements and aims to balance effective deterrence with fair enforcement.

45. MBIE has advised Ministers of stakeholders' concerns. MBIE acknowledges that the targeted consultation was limited in scope and duration. To address this, officials will use the Select Committee process to engage more broadly with stakeholders, test the proposals in greater depth, and refine the legislative settings as needed. This stage will provide an opportunity for stakeholders who were not part of the initial consultation to share their views and for Parliament to consider any remaining concerns about proportionality, enforcement, or implementation.

## Section 2: Assessing options to address the policy problem

### What criteria will be used to compare options for each proposal to the status quo?

46. The following criteria will be used to evaluate options for both Proposal A and Proposal B:

    a. **Effectiveness –** the extent to which the option provides sufficient incentives to effectively promote compliance with the Fair Trading Act (aligns with the objective of supporting a fair and confident trading environment).

    b. **Efficiency –** the extent to which the option enables enforcement action to be undertaken efficiently, at appropriate cost and complexity (aligns with the objective of ensuring efficient enforcement activity).

    c. **Proportionality –** the extent to which the option reflects the nature of the conduct and potential harm that may be caused by breaches of the Act (aligns with the objective that punishment for breaches is proportionate).

    d. **Alignment –** the extent to which the option aligns with comparable New Zealand commercial law (aligns with the objective that the Act aligns with comparable legislation).

### What scope will options for each proposal be considered within?

47. The scope of options for each proposal has been shaped by Ministerial direction and stakeholder feedback received during targeted consultation.

48. Options have been developed to reflect the practical enforcement challenges identified by the Commerce Commission, and to ensure consistency with comparable legislation.

### What proposals are being considered?

49. Two proposals are being considered in this RIS:

    a. Enhance enforcement of the Fair Trading Act (**Proposal A**); and

    b. Increasing the maximum monetary penalties provided for in the Fair Trading Act (**Proposal B**).

50. Proposal B above follows from the recommended option under Proposal A to amend the penalties regime in the Act to enhance compliance. Proposal B considers the maximum penalty levels that could be set under the amended penalties regime.

#### Proposal A: Enhance enforcement of the Fair Trading Act

*Options considered*

**Option 1 –** Status quo

51. Under Option 1, all breaches of the Act (these are detailed in Annex Two) would continue to be treated under the criminal law, with the potential imposition of fines by the District Court on conviction.

**Option 2** – Introduce a civil pecuniary penalties regime to the Act to enhance compliance

52. Option 2 involves amending the Fair Trading Act to enhance the effectiveness of the penalties regime to address issues of non-compliance and make enforcement more efficient. Under this option, amendment legislation would shift most (but not all) criminal offences under the Act to pecuniary penalties. Pecuniary penalties are defined as (non-criminal) monetary penalties imposed by a court under civil procedure where:[8]
    a. liability is established on the civil standard of proof (ie 'on the balance of probabilities')
    b. the pecuniary penalty can be substantial
    c. no criminal conviction or imprisonment results
    d. penalties are paid to the Crown, rather than any victim, ie pecuniary penalties are not intended or designed to compensate.
53. Under this option, pecuniary penalties could enhance compliance with the Act by enabling action to be taken that better addresses the financial motivations behind breaches of the Act by body corporates. It would achieve this by removing the possibility of a criminal conviction and replacing it with civil penalties with much higher maximum fine amounts. It can also make enforcement more efficient by removing the need to prove a breach to the criminal standard of 'beyond reasonable doubt' – a high standard that may not be warranted for some conduct that is not 'truly criminal'.
54. Implementing Option Two would result in the following changes to the penalties regime:
    a. Most strict liability offences under section 40 of the Act (including subsections 40(1), 40(1A), and 40(1B)) would be replaced with civil pecuniary penalties.
    b. Some offences would remain criminal, specifically where the conduct is considered serious or involves obstructing enforcement, such as:
        i. Sections that relate to serious and 'truly criminal' conduct – like undertaking a pyramid scheme or very serious product safety breaches;
        ii. Breaching a management banning order;
        iii. Resisting, obstructing, or delaying enforcement officers;
        iv. Failing to supply information or giving false or misleading evidence to the Commission.
55. These offences often involve serious conduct or deliberate non-cooperation or deception, and we consider that the reputational impact of a criminal conviction is considered proportionate to the harm caused.

[8] Law Commission "Pecuniary Penalties: Guidance for Legislative Design", Report 133 (August 2014) at p. 14, para 1.1, https://www.lawcom.govt.nz/our-projects/law-relating-civil-penalties?id=917.

56. The Commerce Commission would still have the option of taking criminal proceedings in some instances under the Crimes Act 1961 for prohibited conduct considered to be particularly egregious. For example, section 240 of the Crimes Act relates to using deception for gain or to cause loss (including by knowingly or recklessly making false representations). This gives the Commission flexibility in its enforcement approach.

**Option Three –** Provide additional resources to the Commission to enhance compliance

57. Under option Three the Fair Trading Act would remain unchanged, but the Commerce Commission would receive increased funding to improve enforcement under the current criminal regime. This could include additional legal resources, improved case triaging, and enhanced public guidance.

58. The goal would be to improve deterrence and responsiveness without changing the legal framework – instead, this option would seek to enhance compliance with the Act and increase deterrence by increasing the volume of enforcement activity the Commission could undertake.

## Stakeholder views on options

59. Stakeholders expressed a range of views on the three options for improving enforcement under the Fair Trading Act:

    a. **Option One:** Some submitters, including Confidentiality (and those who supported their submission), supported retaining the current criminal model. Confidentiality questioned whether the proposed shift to civil penalties was justified and raised concerns about the removal of criminal sanctions, which they considered an important deterrent.

    b. **Option Two:** Several legal and commercial submitters supported legislative change, noting that civil enforcement is increasingly used in commercial law and allows for more proportionate and efficient responses. Confidentiality and Confidentiality favoured the shift to civil penalties, while the New Zealand Law Society observed that civil proceedings may enable more timely enforcement and better reflect the nature of most breaches. Consumer advocacy groups including Confidentiality and Confidentiality also supported legislative change, highlighting that the lower burden of proof in civil proceedings could improve enforcement outcomes and encourage more reporting of breaches. Confide ntiality stated, “We consider the lower burden of proof will make it easier for the Commission to bring successful actions against businesses that have breached the FTA.”

    c. **Option Three**: No submitters explicitly recommended increasing the Commission’s resourcing as a standalone alternative to legislative reform. However, Confidentiality noted that resourcing constraints at the Commerce Commission can limit enforcement outcomes.

**How do the options compare to the status quo?**

**Table Two: Proposal A - Enhance enforcement of the Fair Trading Act**

| | Option One – (*Status quo*) | Option Two – (*Introduce a civil pecuniary penalties regime to the Act to enhance compliance* ) | Option Three – (*Provide additional resources to the Commission to enhance compliance*) |
|---|---|---|---|
| **Effectiveness** | • Criminal penalties are lower than civil ones, limiting deterrence, especially for larger firms that treat fines as a manageable cost.<br>Rating: **0** | • Option Two may provide more meaningful and effective deterrence than the status quo. the proposed change under this option can be set at significantly higher levels than criminal fines, because they do not carry the reputational stigma or procedural safeguards associated with criminal convictions.<br>• This allows penalties to more directly target the financial incentives behind breaches, especially where conduct is motivated by commercial gain. For example, a penalty set at three times the value of the gain made can outweigh the benefit of non-compliance and act as a strong deterrent.<br>• Supported by Law Commission guidance that pecuniary penalties are a flexible and effective tool for promoting compliance in regulatory regimes.<br>Rating: ++ | • Increased resourcing would allow the Commerce Commission to take more cases, investigate more non-compliance, and improve visibility of enforcement.<br>• This may improve deterrence, especially for lower-level breaches. However, the deterrent effect may remain limited for serious breaches due to low maximum penalties and the burden of proof required under criminal law.<br>• The Commission is already using non-litigation tools extensively. In 2024/25, over 80 per cent of investigation outcomes involved information or compliance advice. Which suggests that the issue is not a lack of guidance, but rather the limited deterrence available under the current penalties regime.<br>Rating: + |
| **Efficiency** | • Criminal proceedings require proof beyond reasonable doubt and follow strict procedures, which are more onerous than civil ones due to stigma and potential imprisonment.<br>• The criminal regime may not be efficient for addressing breaches of the Act that often deal with commercial conduct.<br>Rating: **0** | • In most cases, the proposed legislative change would allow the Commerce Commission to establish liability on the balance of probabilities, avoiding the higher burden of proof warranted in criminal cases.<br>• Civil rules of evidence and procedure are less onerous than criminal rules because they do not carry the same reputational or punitive consequences. This makes enforcement faster, less complex, and less costly.<br>• Admissions can be made without admitting criminal wrongdoing, reducing the need for trial and saving resources.<br>• While civil proceedings afford fewer procedural protections, many defendants are large corporates with significant legal resources which may seek to use these resources to limit their liability in a civil case.<br>Rating: + | • Additional funding could help the Commerce Commission could take enforcement action on a greater number of breaches.<br>• However, enforcement of serious and higher-end breaches would still rely on criminal proceedings, which are slower and more resource-intensive than civil processes.<br>Rating: - |
| **Proportionality** | • The nature of the conduct and potential harm caused from breaches of the Fair Trading Act may not warrant the application of the criminal law (aside for the most serious breaches).<br>• Given that most breaches of the Act are not truly criminal by their nature and in terms of their potential harm, they may not be deserving of the stigmatising effect (socially and/or reputationally) of a criminal conviction.<br>Rating: **0** | • The proposed legislative change better reflects the nature and harm of most breaches under the FTA's. These breaches typically involve financial harm, not physical harm or serious moral wrongdoing, and are often strict liability offences. A civil regime is more proportionate for this type of regulatory conduct.<br>• Pecuniary penalties allow courts to impose meaningful consequences without over-penalising conduct that is regulatory rather than criminal in nature.<br>• For serious breaches, such as obstructing investigations or knowingly misleading consumers, the Commerce Commission retains the ability to pursue criminal charges under the Crimes Act.<br>Rating**: ++** | • The Commission already has a range of tools it can use to take proportionate action in relation to breaches – like issuing warnings or providing guidance. Under this option, it would be able to take more of these enforcement measures.<br>However, issues of proportionality in the Act would persist – the low maximum penalties in the Act would not enable appropriately significant enforcement response, or deterrent, for the largest breaches of the Act or conduct by the largest firms. These issues could not be addressed by providing the Commission with more resourcing because the penalties are limited by the current provisions in the Act.Rating: - |
| **Alignment** | • The FTA's reliance on criminal offences is increasingly out of step with other commercial legislation in New | • Option Two would bring the FTA' into closer alignment with other commercial legislation in New Zealand and Australia, | • This option retains a criminal-only enforcement model, which is increasingly out of step with other commercial legislation in |

| | Option One – (*Status quo*) | Option Two – (*Introduce a civil pecuniary penalties regime to the Act to enhance compliance* ) | Option Three – (*Provide additional resources to the Commission to enhance compliance*) |
|---|---|---|---|
| | Zealand and Australia.<br>• Comparable regimes like the Financial Markets Conduct Act and the and Commerce Act use civil penalties for similar conduct, such as misleading representations and unfair practices.<br>• This misalignment creates inconsistency for regulators and businesses and may reduce the predictability and coherence of the regulatory framework.<br>Rating: **0** | including the Financial Markets Conduct Act and Commerce Act.<br>• The Financial Markets Conduct Act is a good comparator, as it also covers 'fair dealing' provisions that mirror many of the Fair Trading Act's prohibited conduct sections. Aligning the Fair Trading Act's penalties regime with the civil regime used in the Financial Markets Conduct Act would therefore support a more consistent legislative regime on the types of fair dealing and conduct behaviours that both Acts deal with.<br>• Greater alignment improves consistency, reduces compliance complexity, and enhances predictability.<br>Rating: **+** | New Zealand and Australia.<br>• It does not address misalignment with regimes like the FMC Act or Commerce Act, and the limited deterrence effect of the low penalties in the Act would persist.<br>Rating: **-** |
| **Overall assessment** | • The current criminal-only model is increasingly seen as outdated and ineffective.<br>• It provides limited deterrence, particularly for larger firms, and is inefficient to enforce due to the high burden of proof and procedural complexity.<br>• It does not reflect the nature of most breaches and is out of step with other commercial legislation.<br>Rating: **0** | • This option enables more proportionate and efficient enforcement, improves deterrence by allowing for higher penalties, and aligns the Fair Trading Act with other modern regulatory regimes.<br>• Given that businesses, particularly large ones, consider the potential financial gain from a breach, encouraging their compliance likely rests on addressing the limited deterrence of the current penalties regime in the Act.<br>• It retains criminal liability for serious breaches, ensuring appropriate safeguards remain in place.<br>Rating: **+** | • This option could improve enforcement outcomes by enabling the Commerce Commission to take more cases and increase visibility of enforcement.<br>• But this benefit would likely only be realised for low-end offending as the limitations of the current low penalties regime would persist.<br>Rating: **-** |

| **Key for qualitative judgements:** | | | | |
|---|---|---|---|---|
| **++**<br>much better than doing nothing/the status quo/counterfactual | **+**<br>better than doing nothing/the status quo/counterfactual | **0**<br>about the same as doing nothing/the status quo/counterfactual | **-**<br>worse than doing nothing/the status quo/counterfactual | **--**<br>much worse than doing nothing/the status quo/counterfactual |

### Proposal B: Increase the size of maximum monetary penalties in the Act

60. Under Proposal B, MBIE proposes increasing maximum monetary penalties to strengthen deterrence and ensure the penalties regime more effectively addresses unfair conduct. This proposal links closely to our preferred option under Proposal A – to introduce a civil pecuniary penalties regime to the Act to enhance compliance. MBIE assessed four options for updating penalty levels under the Fair Trading Act, each involving a three-tier structure based on the seriousness of the conduct.

61. The proposed approach retains the existing offence tiers in the Act.

    a. Offences currently covered by section 40(1) and 40(1A)including contraventions of Parts 1, 3, and 4, and breaches of section 24, would move to Tier 1.

    b. Breaches of management banning orders under section 46C going into Tier 2.

    c. Offences currently covered by section 40(1B), including contraventions of Part 2 and Part 4A, would move to Tier 3.

62. This ensures that the most serious offences under the current regime are matched with the highest penalties, without reclassifying individual provisions. This ensures alignment with the Act's current provisions.

63. The four options considered are summarised below and set out in Table 1:

64. **Option One –** Status quo:

    a. Retain current maximum monetary penalties. Tier 1 penalties would remain set at $200,000 for individuals and $600,000 for body corporates.

    b. Tier 2 penalties would remain at $60,000 for individuals.

    c. Tier 3 penalties would remain at $10,000 for individuals and $30,000 for body corporates.

65. **Option Two** – Increase penalties, with Tier 1 aligned with the Commerce Act

    a. Increase penalties, with Tier 1 penalties aligned with the highest available under the Commerce Act. This includes a maximum penalty of $500,000 for individuals and $10 million for body corporates, or higher amounts based on commercial gain or turnover.

    b. Tier 2 penalties would increase to $200,000 for individuals.

    c. Tier 3 penalties would increase to $60,000 for individuals and $200,000 for body corporates.

66. **Option Three** – Increase penalties, with Tier 1 aligned with the Financial Markets Conduct Act (preferred):

    a. Increase penalties, with Tier 1 penalties aligned with the Financial Markets Conduct Act. This includes a maximum penalty of $1 million for

individuals and $5 million for body corporates, or higher amounts based on gain or loss avoided.

b. Tier 2 and Tier 3 penalties would increase in line with Option Two.

67. **Option Four –** Increase penalties, with Tier 1 aligned with Australian Consumer Law

a. Increase penalties, with Tier 1 penalties aligned with the Australian Consumer Law. This includes a maximum penalty of AUD$2.5 million for individuals and AUD$50 million for body corporates, or higher amounts based on benefit obtained or turnover.

b. Tier 2 and Tier 3 penalties would increase in line with Options Two and Three.

68. Stakeholder views on increasing penalties varied:

a. Some submitters, including Confidentiality supported retaining the status quo **(Option One)** and expressed concern that higher penalties could increase compliance costs and reduce investment certainty, or deter businesses looking to invest in New Zealand.

b. Few submitters supported aligning with the Commerce Act model **(Option Two)**. While acknowledging the need for stronger deterrence, some noted that Commerce Act penalties are designed for more serious anti-competitive conduct, such as cartel behaviour, and may not be appropriate for breaches of consumer law.

c. Legal submitters such as Confidentiality and Confidentiality favoured alignment with the Financial Markets Conduct Act **(Option Three)**, noting that it deals with similar types of conduct, such as misleading or deceptive representations, and provides a proportionate and familiar model for enforcement.

d. Similarly, while stakeholders acknowledged the trend toward higher penalties in Australia **(Option Four)**, there was limited support for adopting the Australian Consumer Law model. Confidentiality nd Confidentiality raised concerns that the penalty levels may be disproportionate in the New Zealand context and could overstate the commercial gains typically associated with Fair Trading Act breaches.

**Table 2: Current maximum monetary penalties in the Fair Trading Act and three options for increasing the size of the maximum monetary penalties**

<table>
<tr><th>Tier</th><th>Option One – Status quo</th><th>Option Two – Commerce Act model</th><th>Option Three – FMC Act model (preferred)</th><th>Option Four – Australian Consumer Law</th></tr>
<tr><td rowspan="3">1</td><td colspan="4">Applies to Part 1 (Unfair conduct) (except sections 9, 14(2), 24, and 23), Part 3 (Product safety), or Part 4 (Services safety)</td></tr>
<tr><td>• $200,000 for individuals<br>• $600,000 for body corporates</td><td rowspan="2">• $500,000 for individuals<br>• For body corporates the greater of:<br>- $10 million, or<br>- 3x commercial gain (if ascertainable), or<br>- 10 per cent of turnover (if gain not ascertainable)</td><td rowspan="2">• The greater of:<br>- $5 million (body corporate) and $1 million for individuals, or<br>- 3x gain made or loss avoided, or<br>- consideration for the transaction</td><td rowspan="2">• AUD$2.5 million for individuals<br>• For body corporates the greater of<br>- AUD$50 million<br>- 3x benefit obtained, or<br>- 30 per cent of adjusted turnover of the corporation's adjusted turnover during the breach turnover period for the contravention</td></tr>
<tr><td>Section 24 (Pyramid selling schemes)<br>• $600,000</td></tr>
<tr><td rowspan="2">2</td><td colspan="4">Applies to Part 5A (Management banning orders)</td></tr>
<tr><td>• $60,000 for individuals</td><td colspan="3">• $200,000 for individuals</td></tr>
<tr><td>3</td><td colspan="4">Applies to Part 2 (Consumer information standards) and Part 4A (Consumer transactions and auctions)</td></tr>
</table>

| | | |
|---|---|---|
| | • $10,000 for individuals<br>• $30,000 for body corporates | • $60,000 for individuals<br>• $200,000 for body corporates |

## How do the options compare to the status quo?

### Table Three: Proposal B - Increase the size of maximum monetary penalties in the Act

| | Option One – *Status quo* | Option Two – *Increase penalties, with Tier 1 penalties set in line with the Commerce Act* | Option Three – *Increase penalties, with Tier 1 penalties set in line with the Financial Markets Conduct Act* | Option Four – *Increase penalties, with Tier 1 penalties set in line with Australian Consumer Law* |
|---|---|---|---|---|
| **Effectiveness** | • The current penalty levels may not offer sufficient incentives to promote compliance, particularly for larger firms where the commercial gain from breaching the Act can exceed the maximum fines. This limits the deterrence effect of the regime and may reduce its ability to prevent unfair conduct.<br>Rating: **0** | • Option Two would strengthen deterrence by increasing the downside risk of non-compliance, especially where breaches are financially motivated.<br>• Penalties that reflect or exceed the commercial gain from a breach are more likely to promote compliance as the ability to impose fines that exceed commercial gains means that businesses cannot just treat any fine as a cost of doing business.<br>Rating: **+** | • Option Three would also strengthen deterrence by increasing the downside risk of non-compliance, especially where breaches are financially motivated.<br>• However, this option retains components that enable penalties to be set with reference to commercial gains made. This means that businesses cannot just treat any fine as a cost of doing business.<br>Rating **+** | • Penalties under the Australian Consumer Law are significantly higher than those currently available under the Fair Trading Act, including penalties of up to AUD$50 million for corporations.<br>• These levels are likely to provide strong incentives to comply, particularly for large firms where the commercial gain from misleading conduct may be substantial.<br>Rating **++** |
| **Efficiency** | • There is no material difference in administrative efficiency between the options, as all involve court-imposed penalties.<br>Rating: **0** | • No difference between Options.<br>Rating: **0** | • No difference between Options.<br>Rating: **0** | • No difference between Options.<br>Rating: **0** |
| **Proportionality** | • The current penalty levels may not reflect the nature or impact of many breaches. In some cases, penalties are too low to be proportionate to the harm caused or the commercial benefit gained. This limits the ability of courts to impose consequences that match the seriousness of the conduct and harm caused.<br>Rating: **0** | • Tier 1 penalties include a formula that allows the court to impose the greater of a fixed amount, 3 times the commercial gain, or 10 per cent of turnover. This enables penalties to reflect the financial benefit of the breach, particularly for larger firms, and enables fines to be set that are proportionate to the nature of the breach.<br>• Tier 2 and Tier 3 penalties are also increased from current levels but remain relatively lower, supporting a structured response across offence types.<br>• However, the Commerce Act model is designed for more serious conduct, such as cartel behaviour, and may result in penalties that are disproportionately high for some Fair Trading Act breaches.<br>Rating: **+** | • Tier 1 penalties are based on the Financial Markets Conduct Act and allow the court to impose the greater of a fixed amount, three times the gain made or loss avoided, or the consideration for the transaction. This links penalties to the financial impact of the breach.<br>• Tier 2 and Tier 3 penalties are increased but remain relatively lower.<br>• Compared to Option Two, this approach avoids the risk of over-penalising Fair Trading Act breaches, as the FMC Act deals with similar types of conduct, such as misleading or deceptive representations.<br>Rating: **++** | • Penalty levels set in the Australian Consumer Law reflect the size and scale of their economy and markets as a proxy for the level of commercial gains that could be achieved by breaching the legislation.<br>• It is likely that setting maximum monetary penalties in New Zealand at levels similar to those for the Australia Consumer Law may mean that penalties disproportionately overstate the potential commercial gains achievable from breaches relative to commercial gains achievable in Australia.<br>Rating: **--** |
| **Alignment** | • The Fair Trading Act's maximum penalties are low compared to other commercial legislation in New Zealand, such as the Commerce Act and the Financial Markets Conduct Act and compared to the Australian Consumer Law. This creates inconsistency across regimes that deal with similar types of conduct, such as misleading representations and unfair practices.<br>Rating: **0** | • Option Two would result in Fair Trading Act penalties being higher than those available under the Financial Markets Conduct Act for similar conduct, such as misleading or deceptive representations. This would reduce legislative alignment.<br>• It may also mean that the most serious Fair Trading Act breaches attract penalties equivalent to those imposed for cartel conduct under the Commerce Act, which are generally considered more serious in that they undermine free market competition.<br>Rating: **-** | • Tier 1 penalties are based on the 'fair dealing' provisions in the Financial Markets Conduct Act, which address similar types of conduct to those prohibited under the Fair Trading Act.<br>• This supports strong consistency across regimes that deal with comparable behaviour.<br>• A fundamental principle of penalty design is that similar offences should attract similar penalties to ensure fairness in how different laws are applied.<br>Rating: **++** | • While the Australian Consumer Law deals with similar types of conduct, adopting its penalty levels would make the Fair Trading Act's penalties significantly higher than those in other New Zealand commercial legislation, including the Financial Markets Conduct Act and the Commerce Act.<br>• This would create significant inconsistency across domestic regimes and reduce clarity for businesses operating in New Zealand.<br>Rating: **--** |
| **Overall assessment** | Current penalty levels are too low to deter breaches, especially by larger firms. They lack proportionality and alignment with other regimes and offer limited incentives to comply.<br>Rating: **0** | Option Two would strengthen deterrence by allowing penalties to be set with reference to commercial gain and with significantly higher penalties of up to $10 million for businesses. However, the Commerce Act model is designed for more serious anti-competitive conduct and may result in disproportionately high penalties for typical | Option Three offers a balanced approach. It improves deterrence while maintaining proportionality and alignment with similar legislation. The FMC Act deals with comparable conduct, making it a suitable benchmark. This option supports fairness, consistency, and effective enforcement. Rating: **++** | Option Four provides strong deterrence but risks excessive penalties that may not reflect the scale of harm or gain in the New Zealand context. It could create misalignment with domestic regimes and reduce clarity for businesses, raising concerns about fairness and consistency. |

| | Option One – *Status quo* | Option Two – *Increase penalties, with Tier 1 penalties set in line with the Commerce Act* | Option Three – *Increase penalties, with Tier 1 penalties set in line with the Financial Markets Conduct Act* | Option Four – *Increase penalties, with Tier 1 penalties set in line with Australian Consumer Law* |
|---|---|---|---|---|
| | | Fair Trading Act breaches. It also risks misalignment with other consumer protection legislation.<br>Rating: **+** | | We also note that Australia has a much larger economy and consumer market that warrants imposition of much higher penalties in their market given the much higher potential gain that can be made from offending, and the much higher potential impacts to consumers.<br>Rating: **-** |

| **Key for qualitative judgements:** | | | | |
|---|---|---|---|---|
| **++**<br>much better than doing nothing/the status quo/counterfactual | **+**<br>better than doing nothing/the status quo/counterfactual | **0**<br>about the same as doing nothing/the status quo/counterfactual | **-**<br>worse than doing nothing/the status quo/counterfactual | **--**<br>much worse than doing nothing/the status quo/counterfactual |

## What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

69. Based on the analysis in this paper, and the available evidence of a problem, MBIE considers that the combination of Proposal A, Option Two (introducing civil pecuniary penalties for most breaches of the Fair Trading Act) and Proposal B, Option Three (increasing maximum monetary penalties in line with the Financial Markets Conduct Act), is most likely to address the problem, meet the policy objectives, and deliver the highest net benefits.

70. Proposal A, Option Two would shift most breaches from criminal offences to civil pecuniary penalties. This would improve enforcement efficiency by removing the need to meet the higher criminal standard of proof, allowing the Commerce Commission to take action more efficiently for the types of commercial conduct the Act deals with. It would also reduce the procedural burden associated with criminal prosecutions, while retaining criminal liability for the most serious breaches, such as obstructing investigations or breaching banning orders, where the reputational impact and procedural safeguards of a criminal prosecution remain appropriate.

71. The Law Commission has noted that pecuniary penalties are increasingly used in regulatory regimes because they offer a flexible and effective enforcement tool. They can impose significant financial consequences without the procedural burden of criminal trials, making them well-suited to promoting compliance in commercial contexts.[9]

72. Proposal B, Option Three would increase maximum penalties in a way that reflects the financial impact of breaches and aligns with comparable legislation. Tier 1 penalties would be based on the Financial Markets Conduct Act, which deals with similar types of conduct, such as misleading or deceptive representations and unsubstantiated claims. This supports proportionality by ensuring penalties are scaled to the benefit gained or harm caused and avoids the risk of over-penalising Fair Trading Act breaches by applying penalty levels designed for more serious conduct under the Commerce Act. The tiered structure also ensures that less serious breaches remain subject to lower penalties, maintaining a balanced and proportionate regime.

73. In response to stakeholder feedback, MBIE refined the proposals by retaining criminal liability for certain serious breaches, narrowing the scope of civil penalties to strict liability offences, and aligning maximum penalties with the Financial Markets Conduct Act rather than the Commerce Act or Australian Consumer Law. These changes reflect concerns about proportionality, enforcement burden, and legislative consistency, and aim to balance effective deterrence with fair and practical enforcement. Officials acknowledge that the Financial Markets Conduct Act and Fair Trading Act deal with different sectors and types of businesses. The Fair Trading Act applies to all businesses in New Zealand while the Financial Markets

[9] Law Commission, Pecuniary Penalties – Guidance for Legislative Design, Foreword, page iv

Conduct Act applies to typically larger firms involved in financial markets and services like major banks, listed companies and insurers. However, we still consider that aligning the penalties in the Fair Trading Act with those in the Financial Markets Conduct Act is appropriate due to the need to ensure that maximum penalties can address fair trading conduct by any business operating here regardless of their size – from corner dairies through to the largest multi-national retailers – by ensuring that maximum penalties in the Act have enough 'headroom' to address conduct of any scale. Without this headroom, the Act's ability to address the most serious conduct, or breaches by the largest businesses, is limited. It is important to note that courts retain discretion to set penalties up to the maximum amount and that they have readily applied this discretion to set penalties at lower levels than the maximum in many cases to date.

74. This combined approach best meets the objectives of the reform: it strengthens deterrence, enables more efficient enforcement, supports proportionality, and aligns the Fair Trading Act with other commercial legislation in New Zealand.

### Limitations with our analysis

75. MBIE acknowledges that the policy process to consider these changes has been undertaken at pace, and that there are limitations in the available evidence. While there is a clear rationale for reform, including concerns raised by the Commerce Commission and stakeholder feedback, there is limited empirical data on the extent to which the current penalties regime has failed to deter non-compliance across sectors or over time.

76. There is also limited evidence to inform what an appropriate penalty level should be. To mitigate this, MBIE has recommended aligning penalties with comparable legislation, notably the Financial Markets Conduct Act, which addresses similar types of conduct and provides a tested benchmark for penalty design.

77. Further consultation on the proposals will be undertaken through the Select Committee process, which will provide an opportunity to test the proposed changes more fully with stakeholders and refine the approach if needed.

## Is the Minister's preferred option in the Cabinet paper the same as the agency's preferred option in the RIS?

78. Yes, the Minister's preferred option under Proposal A and Proposal B are the same as officials' preferred options in this RIS.

## What are the marginal costs and benefits of the preferred options in the Cabinet paper?

| Affected groups | Comment | Impact | Evidence Certainty |
|---|---|---|---|
| **Additional costs of the preferred options compared to taking no action** | | | |
| Regulated groups – New Zealand businesses | Businesses facing enforcement action for breaches of the Fair Trading Act will face increased potential penalties under proposed changes – though the exact amounts will still be determined by the courts on the facts of each case.<br>Therefore, costs would not accrue to most businesses – only if they breach a provision in the Act. | High (but depends on the facts of each case and would impact a limited number of businesses) . | Low – level of impact on businesses will depend on the level of penalty imposed by the courts on a case-by-case basis. This is uncertain for future cases. |
| Regulators – Commerce Commission | May result in the Commerce Commission taking more enforcement action under a civil proceedings and pecuniary penalties regime.<br>However, the costs of taking civil proceedings should be lower relative to taking criminal proceedings under the Act currently. | Low - Medium. | Low – unclear how many additional cases would be undertaken. |
| Ministry of Justice | The Ministry will incur some increased operational costs in processing civil penalties imposed by the courts.<br>System changes will be needed to reflect changes to offence rules, which the Ministry estimates at $200,000 (+/- 50 percent) which cannot be met within baselines and will be reassessed after Cabinet decisions are made. | Low - Medium | Moderate – based on information and estimates provided by the Ministry of Justice. |
| New Zealand consumers | No direct costs to consumers. | None. | Not applicable. |
| **Non-monetised costs** | Much higher potential costs for businesses breaching the Fair Trading Act, and likely increased costs for the Commerce Commission's enforcement activities. | Medium. | Low – as above. |
| **Additional benefits of the preferred options compared to taking no action** | | | |
| Regulated groups – New Zealand businesses | Businesses would avoid the stigma of criminal convictions under many of the Fair Trading Act's enforcement provisions, though noting that these come with much higher potential penalties than under the Act currently.<br>Increased compliance is also likely to benefit compliant businesses by reducing unfair competitive advantages held by non-compliant firms, supporting a more level playing | Low. | Low – benefit of avoided stigma from criminal convictions is unable to be quantified. |

| | | | |
|---|---|---|---|
| | field. | | |
| Regulators – Commerce Commission | Benefits from having access to a more effective, efficient and flexible regulatory toolkit means that the Commerce Commission can take the most appropriate course of enforcement action for many breaches.<br>More likely to pursue lower level breaches, which supports market confidence. | Medium. | Low – unable to be quantified. |
| New Zealand consumers | Less likely to be impacted by conduct that breaches the Fair Trading Act as the penalties regime will better deter breaches. This can reduce instances where consumers pay more for goods and services or incur the costs of bad purchases (like goods or services not asked for). | Medium. | Low – the level of benefit to consumers based on avoided breaches is unable to be estimated with certainty. |
| **Non-monetised benefits** | Increased benefits to consumers through fewer future breaches of the Act, while the Commerce Commission benefits through having a more effective and efficient enforcement toolkit. | Medium. | Low – as above. |

# Section 3: Delivering an option

## How will the proposal be implemented?

*The changes proposed will be implemented through amendment legislation*

79. The proposals set out in this RIS, once agreed by Cabinet, will be implemented by amending the Fair Trading Act through an amendment bill. Constitutional Conventions

80. Constitutional Conventions The actual commencement date for the new regime will be determined as part of drafting the Bill. Officials will also consider, as part of drafting, whether a transition period is needed for businesses to familiarise themselves with the changes before they come into effect.

81. Changes to the Act will not apply retrospectively. MBIE will continue to administer the Fair Trading Act.

*The Commerce Commission will be responsible for enforcement*

82. The changes in this RIS will be enforced by the Commerce Commission – the existing enforcement agency for the Fair Trading Act. The Commerce Commission has an existing and well-established enforcement function that

[10] Noting that this rating is yet to be confirmed at the time of writing.

will monitor compliance with the amended regime and take enforcement action where necessary.

83. Enhancing the penalties regime may lead to more enforcement action being taken by the Commission. Any additional enforcement activity, or resource needs, will likely be met by the Commission from within baselines (this is to be confirmed at the time of writing).

*Communicating the changes to those affected*

84. The Fair Trading Act applies to all New Zealand businesses and individuals in trade – from small and medium enterprises (SMEs) to large corporates. The Commission will issue guidance about the amended penalties regime before it comes into force to outline the changes to New Zealand businesses and consumers.

85. The Commission is experienced in issuing guidance for similar regulatory changes in the past – including previous amendments to the Fair Trading Act (see the Commission's *Your Obligations as a Business* webpage here: Commerce Commission - Your obligations as a business). The Commission will:

    a. Update its website;
    b. Update its online enforcement response guidelines;
    c. Update its online criminal prosecution guidelines;
    d. Potentially develop new public-facing guidelines related to civil proceedings; and
    e. Develop or update training for investigators and implement this new training.

*Implementation risks*

86. Submitters on the draft proposals have raised a potential risk that implementing higher penalties in the Act could make New Zealand a less attractive destination for companies to invest or operate due to the higher financial risks from breaching our consumer law.

87. We have considered this risk and note that, while the changes lift the maximum penalties under the Act, these are not to levels that are higher than comparable regimes internationally. For example, Australia has much higher penalties for breaches of its consumer law, and their regime has not proven a barrier to investment.

88. However, we note the potential risk and will consider this risk as part of monitoring and evaluation (discussed below).

### *How will the proposals be monitored, evaluated, and reviewed?*

89. As the Commerce Commission already enforces the Act, it has well-established processes for monitoring and reporting on compliance. The Commission will update MBIE (as the Commission's monitoring agency) on how the proposed amendments to the Act are enhancing its enforcement abilities.

90. The Commerce Commission will monitor the effectiveness of the changes and the benefits to its enforcement of the Act. The Commission will:

91. Monitor compliance with the Act and whether the changes in this paper have had the benefits and effects anticipated – like deterring breaches of the Act more effectively. Monitoring will consider:

    a. consumer complaints data (and whether the recent increasing trend of complaints decreases as a result of these proposals);

    b. whether the changes lead to more enforcement action being taken, and whether these are more efficient in terms of cost and time taken;

    c. whether the levels of penalties issued by the courts have increased.

92. Continue reporting quarterly to MBIE and the Minister of Commerce and Consumer Affairs about compliance with the Act through their existing quarterly reporting process.

93. MBIE will work with the Commission to update Ministers on benefits of the regime and any implementation issues (including unintended consequences or implementation risks, like deterring investment) and whether further amendments to the enforcement regime are necessary later.

94. If the monitoring activity above reveals issues with the amended penalties regime, MBIE will consider options for addressing them, test options with the Commission, and advise the Minister of Commerce and Consumer Affairs accordingly.

95. An evaluation of the regime's effectiveness will be undertaken at a later date, yet to be determined.

## Annex One: Current maximum monetary penalties for criminal offences under the Fair Trading Act 1986

| Offence type | Offence section | Breaches under the Act | Current maximum monetary penalties |
|---|---|---|---|
| **Criminal** | 40(1) | Breaches of a provision of:<br>Part 1 of the Act (relating to unfair conduct), except for sections 9, 14(2), 23 or 24;[11, 12]<br>a. Part 3 of the Act (relating to product safety); or<br>b. Part 4 of the Act (relating to safety of services). | **$200,000** fine in the case of an individual and **$600,000** in the case of a body corporate.<br>However, see section 40(2) below in this table for condition on imposing the maximum fine. |
| | 40(1A) | Breaches of section 24 (relating to the prohibition on promoting or operating a pyramid selling scheme). | **$600,000** fine.<br>However, see section **40(2)** below in this table for condition on imposing the maximum fine.<br>In addition to any fine imposed under section 40(1A), under section **40A**, the court may, on the application of the Commerce Commission, order the person to **pay an amount not exceeding the value of any commercial gain resulting from the breach if the court is satisfied that the breach occurred in the course of producing a commercial gain**.<br>The standard of proof in proceedings for a court order under section 40A for an additional penalty for a breach of section 24 involving commercial gain is the standard of proof that applies in civil proceedings (ie 'on the balance of probabilities'). |
| | 40(1B) | Breaches of a provision of:<br>a. Part 2 (relating to consumer information); or<br>b. Part 4A (relating to consumer transactions and auctions). | **$10,000** fine in the case of an individual and **$30,000** in the case of a body corporate.<br>However. see section 40(2) below in this table for condition on imposing the maximum fine. |
| | 40(2) | | With respect to the penalties in section 40 of the Act above (ie as set out in sections 40(1), 40(1A) and 40(1B)), where a person is convicted, whether in the same or separate proceedings, of two or more offences in respect of breaches of the same provisions of the Act and those breaches are of the same or a substantially similar nature and occurred at or about the same time, the aggregate amount of any fines imposed on that person for those convictions **cannot exceed the amount of the maximum fine that may be imposed for a conviction for a single offence**. |
| | 46E | Breach by a person of a management banning order made against him or her. | **$60,000** fine. |
| | 47F | Resisting, obstructing or delaying: | **$10,000** fine in the case of an individual and **$30,000** in the case of a body corporate. |

[11] **Section 9** relates to misleading and deceptive conduct generally, which is prohibited. There is no offence in relation to section 9. Misleading and deceptive conduct is prohibited more specifically under other sections in Part 1 of the Act and breaches of those provisions are an offence under Act. **Section 14(2)** relates to the prohibition on the use of physical force, harassment, or coercion in connection with the sale or grant or possible sale or grant of an interest in land, or the payment for an interest in land. **Section 23** relates to the prohibition on the use of physical force, harassment, or coercion in connection with the supply or possible supply of goods or services or the payment for goods or services. A breach of sections 14(2) or 23 (both relating to use of physical force, harassment or coercion) **is not an offence under section 40(1) of the Act, and therefore there are no penalties for breaches of these sections**. **Section 24** relates to the prohibition on promoting or operating a pyramid selling scheme (see section 40(1A) below in this table).

[12] Note that **section 26** in Part 1 of the Act prohibits goods being imported into New Zealand that bear a "false trade description" (ie any representation which if made in connection with the supply or possible supply of goods or with the promotion by any means of the supply or use of goods would constitute a breach of sections 13(a), 13(d) or 13(j) of the Act. Such goods are prohibited to be imported under section 96 of the Customs and Excise Act 2018. It is a criminal offence under section 388(1) of the Customs and Excise Act to import such goods. Under section 388(2) of the Customs and Excise Act, a person convicted of an offence is liable to a maximum fine of $5,000 in the case of an individual and $25,000 in the case of a body corporate. See also **section 33** of the Act where there is an equivalent effect in relation to the importation of goods which, if supplied, would constitute a breach of Part 3 (relating to product safety) of the Act.

| Offence type | Offence section | Breaches under the Act | Current maximum monetary penalties |
|---|---|---|---|
| | | a. any product safety officer exercising a power under sections 33C (relating to safety of products) or 33D (relating to suspension of supply notices);<br>b. any authorised person acting pursuant to a search warrant issued under section 47; or<br>c. any authorised employee exercising a power to enter a "place" under section 47L. | |
| | 47J | Refusing or failing to comply with a notice under section 47G (relating to requirement that a person supply information or documents or give evidence to the Commerce Commission); or in purported compliance with the notice, supply information, or supply a document, knowing it to be false or misleading. | **$10,000** fine in the case of an individual and **$30,000** in the case of a body corporate. |

## Annex Two: Enforcement outcomes to date for complaints about Fair Trading Act breaches

As at 4 September 2025

| | Financial Year (FY) | 20/21 | | 21/22 | | 22/23 | | 23/24 | | 24/25 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **Reported Concerns** | 10,047 | | 7,889 | | 11,805 | | 11,918 | | 11,736 | |
| 2 | **Reported Concerns FTA** | 8,841 | 88% | 7,075 | 90% | 10,664 | 90% | 10,762 | 90% | 10,851 | 92% |
| 3 | **Investigation Outcomes** | 437 | | 245 | | 323 | | 352 | | 293 | |
| 4 | **Info to trader** | 276 | 63% | 164 | 67% | 260 | 80% | 261 | 74% | 207 | 71% |
| 5 | **Compliance Advice** | 80 | 18% | 36 | 15% | 38 | 12% | 52 | 15% | 38 | 13% |
| 6 | **No further action** | 54 | 12% | 28 | 11% | 13 | 4% | 15 | 4% | 25 | 9% |
| 7 | **Litigation** | 8 | 2% | 6 | 2% | 6 | 2% | 10 | 3% | 12 | 4% |
| 8 | **Warning** | 17 | 4% | 10 | 4% | 5 | 2% | 13 | 4% | 9 | 3% |
| 9 | **Enforceable undertaking** | | | | | 1 | 0% | | | 1 | 0% |
| 10 | **Infringement Notice** | 1 | 0% | | | | | | | 1 | 0% |
| 11 | **Commission Settlement** | 1 | 0% | | | | | | | | |

**Notes:**

Concerns often relate to more than one Act and investigations often relate to more than one concern. Some concerns are still under investigation so won't be counted under investigation outcomes.

# Regulatory Impact Statement on the safe harbour provision to support online service providers to disrupt online scams

| | |
|---|---|
| **Decision sought** | Cabinet decision on introducing legislative limitations on civil liability (a legal "safe harbour provision") for online service providers for disrupting suspected online scams, provided certain conditions are met. |
| **Agency responsible** | Ministry of Business, Innovation and Employment |
| **Proposing Minister** | Minister of Commerce and Consumer Affairs |
| **Date finalised** | 22 May 2025 |

The Minister is proposing to introduce a limitation on civil liability (a legal "safe harbour provision") for online service providers when they take action to disrupt suspected online scams. The safe harbour provision would apply only if specified conditions are met. These may include, for example, a good faith requirement, that the online service provider had reasonable grounds for believing the content is scam content, and a requirement for the online service provider to promptly reverse the action in the event of an error.

The Minister is also proposing to scope complementary, non-legislative designated expert entities (referred to as a "trusted flagger") to identify suspected scam activity and support proactive scam intervention by issuing disruption recommendations to online service providers. The preferred option therefore includes both a regulatory measure (a safe harbour provision) and a non-regulatory measure (scoping trusted flaggers). This regulatory impact analysis is primarily focussed on assessing the introduction of the safe harbour. Further detail regarding the trusted flaggers is still being worked through but it will not require legislative change, regulatory oversight or additional funding. If the implementation of trusted flaggers is delayed or not progressed for any reason this will not impact the introduction of the safe harbour provision.

These two proposals together are designed to reduce perceived legal risk and enable more confident, timely action by online service providers to prevent scams, without imposing new duties or regulatory burdens on online service providers. It is a targeted and proportionate approach that supports solutions led by the online service provider industry, while maintaining appropriate safeguards for consumers and businesses.

Outlined below is a summary of the type of entities that are intended to be captured by the term "online service provider":

| Entity Type | Role | Actions They Can Take |
|---|---|---|

| | | |
|---|---|---|
| Domain Name Registrar / Host (e.g. Domainz) | Manages registration of website domain names (e.g. www.scamwebsite.co.nz). | Suspend, cancel, or redirect a domain name associated with scam activity. |
| Website Hosting Provider (e.g. Bluehost) | Hosts the website content and underlying files on a server. | Take down or disable access to scam-related content or entire websites. |
| Telecommunications Provider / Internet Service Provider (ISP) (e.g. Spark and OneNZ) | Provides internet access and routing for users. | Block access to scam websites or domains at the network level (e.g. Domain Name System (DNS) or Internet Protocol (IP) blocking). |
| Digital Platform Provider (e.g. Google and Meta) | Distributes or links to content via search, social media, or advertising. | Remove or demote scam-related posts, advertisements, pages, or user accounts. |

## Summary: Problem definition and options

**What is the policy problem?**

Online service providers are key players in detecting and disrupting online scams. However, they face potential legal risk when taking proactive steps to detect and disrupt scams. We have used the term "disruption" in this analysis to refer to actions including blocking, removing, sinkholing[1], or otherwise restricting access to suspected scam content. Online service providers have told us that the potential exposure to liability under contract or tort law if legitimate activity is inadvertently affected is stopping them from confidently taking more proactive measures to disrupt scams.

This potential liability risk has created a risk-averse operating environment, where online service providers may delay or avoid taking timely action – even when they have strong indicators of scam activity. As a result, known scams could remain active for longer than necessary, increasing the risk of consumer harm and eroding trust in digital systems.

**What is the policy objective?**

The proposed change aims to reduce concern among online service providers that they could be legally liable if they make errors, and support their confident, timely disruption of suspected online scam activity. The objective is to create an enabling environment for voluntary, industry-led responses, where providers can act quickly and proportionately to disrupt scams without fear of liability. Success will be measured by:

- increased proactive scam disruption (e.g. website sink holing)
- feedback from online service providers of increased legal clarity and confidence to disrupt scams, and
- reduction in scam-related harm to consumers over time.

**What policy options have been considered, including any alternatives to regulation?**

1. **Status quo (no regulatory change)**
   Online service providers would continue to bear the risk of civil liability if they disrupt suspected scam content in error. Given the risk averse nature of the online service provider industry, we anticipate online service providers to continue to take a cautious approach and not disrupt suspected scams if this could expose them to legal risk.

2. **Establish a 'trusted flagger' mechanism (an expert entity whose reports are prioritised) for scam identification**
   A government-supported operational entity would be established to help identify scam activity and provide recommendations to online service providers on scam content. This would improve confidence and willingness to act but would not remove

[1] Sinkholing is a cybersecurity technique used to quietly take control of scam or malicious websites. Instead of shutting the website down, internet traffic is redirected to a safe server run by a trusted organisation. This stops the scam from working and can also help gather information about who is being targeted.

liability or create a duty for online service providers to act on the entity's recommendations. This is a non-regulatory option.

3. **Legislative limitation on liability (a "safe harbour provision")**
   Government would introduce a legislative limitation on civil liability for online service providers taking reasonable steps to disrupt scams by establishing a new legislative defence. The provision would be subject to conditions to protect the interests of legitimate businesses using online services and prevent misuse.

4. **A positive duty to act**
   Government would introduce a legislative requirement for online service providers to take reasonable, proportionate steps to disrupt scams. This would increase accountability by imposing enforceable obligations. It would require regulatory oversight.

**What consultation has been undertaken?**

We have been engaging with industry since early 2024 on strategic and coordination issues related to addressing scams. Since late 2024, our engagement has focused on potential regulatory hurdles and solutions, including the issue of liability for online service providers who disrupt scams. Our targeted consultation with industry and consumer groups includes:

a) Government Agencies and Private Sector Scams Data workshop in November 2024
b) A workshop in December 2024 to understand problems relating to disrupting scam activity.
c) A workshop in March 2025 to test a wider set of coordination and regulatory proposals to address scams.

A summary of the workshops can be found at **Annex 1**.

Most attendees supported taking a targeted regulatory approach, and for government to provide a legislative safe harbour provision to address liability risks for disrupting suspected scam websites.

We have not undertaken any public consultation due to the Minister's expressed concern for moving ahead with this proposal quickly. Should regulatory changes be progressed, stakeholders will have an opportunity to provide feedback during the select committee stage.

There are currently no plans to publish an exposure draft.

**Is the preferred option in the Cabinet paper the same as preferred option in the RIS?**
Yes

## Summary of Minister's preferred option: option 2 and option 3: clarifying expert entities to serve as 'trusted flaggers' and establishing a legislative limitation on civil liability

### Costs (Core information)

The Minister's preferred approach is to combine option 2 and option 3, clarifying expert entities to serve as "trusted flaggers" and establishing a legislative limitation on civil liability (a safe harbour provision). Only the legislative limitations on civil liability have regulatory implications.

The approach would impose minor compliance costs on online service providers. These costs would relate primarily to one-off adjustments to internal processes for assessing and meeting safe harbour provision conditions. Courts may occasionally be involved in determining whether conditions for the safe harbour provision are met, but this is expected to be infrequent.

Modest resourcing may be required to establish or support existing entities to perform the trusted flagger role, but this is expected to be manageable within baselines.
Legitimate businesses that use online services may experience some disruption if online service providers mistakenly block their content. We consider the probability and impact of this risk to below, given that there will be clear procedural safeguards to minimise the risk, and a process for online service providers to reverse the disruption should they have made an error.

There are no significant direct costs for government, as implementation relies on existing legal and regulatory mechanisms. Minor resources may be required for awareness-raising, but no new operational systems or public funding streams are proposed.

### Benefits (Core information)

The approach would reduce online service providers' concerns that they would be legally liable if they mistakenly disrupt a legitimate business, which online service providers report has prevented them from confidently disrupting suspected scam websites. The trusted flagger model would enhance online service providers' decision-making credibility and support faster, coordinated scam content removal.

Consumers would benefit from earlier intervention in scam incidents, which would reduce the harm that scams cause to consumers and build consumers' trust in digital systems. These benefits are non-monetised but potentially high and supported by international precedent and stakeholder submissions.

The proposals could bring confidence and eventual financial reward to legitimate businesses that operate online as trust in the system increases.

### Balance of benefits and costs (Core information)

We assess that the benefits of the preferred approach outweigh the costs. Implementation is low-cost and builds on existing civil remedies. The approach would reduce barriers that have prevented online service providers from disrupting scams. The approach also supports

broader efforts to strengthen trust and safety in digital services. The approach is aligned with international frameworks, including Australia's, and is expected to improve system responsiveness, which will reduce consumer losses to scams over time.

## Implementation

The option to limit potential civil liabilities would be implemented through a legislative amendment. This will function as a defence to civil claims in tort or contract where an online service provider has acted in accordance with defined safe harbour provision conditions. No dedicated funding is required. This option is intended to support earlier and more confident disruption of scams by online service providers, without requiring a comprehensive legislative framework or a new regulator.

The trusted flagger option is a non-legislative mechanism: Expert entities that can identify likely scam content and provide coordinated disruption recommendations to online service providers (a trusted flagger model). This will be implemented operationally via an existing government agency, or the new anti-scam alliance under development. This option would support scam identification and website disruption recommendations, improving consistency and confidence in provider decision-making. The trusted flagger roles may require minor operational resources but can be delivered within existing baselines. The implementation of the legislative safe harbour is not dependent on the trusted flagger and can proceed independently.

## Limitations and Constraints on Analysis

We have not conducted full public consultation on this policy issue, nor on the full range of options, due to time constraints and Ministerial direction. Had consultation occurred, it would have provided further evidence on the nature and scale of the problem, stakeholder views on liability risks, and the potential impacts on legitimate businesses whose online activity may be mistakenly disrupted.

To partially mitigate this, we reviewed select committee submissions on Australia's Scam Prevention Framework Bill, which also included a legislative safe harbour provision to address industry concerns about disrupting scams. This enabled us to understand views of businesses that may be affected by such a provision, and of law firms.

The overwhelming majority of submissions on Australia's Scam Prevention Framework Bill from the private sector, consumer representative groups, and a small business representative group supported the inclusion of a safe harbour provision. One of the concerns raised by submissions was the potential negative effects on legitimate small businesses who could have their website mistakenly disrupted under the guise it was a scam, and potentially suffer loss of sales and impacts to brand reputation[2].

This risk could be mitigated through:

1. the establishment of a 'trusted flagger' regime to support online service providers to make decisions on disrupting suspected scam content, and

[2] Submissions – Parliament of Australia. Submission 26: Australian Small Business and Family Enterprise Ombudsman at page 4.

2. including a condition in the safe harbour that requires online service providers to promptly restore services where they have been mistakenly disrupted.

A legislative safe harbour provision for disrupting digital content has been implemented in some other contexts, for example the Harmful Digital Communications Act 2015. However, a safe harbour provision for disrupting scams in New Zealand would be novel. Australia's Scams Prevention Framework only came into force in February 2025, so it is too early to assess how it is working in practice or what its real-world impacts may be. We are therefore unable to understand the real-world impacts of such a provision.

**I have read the Regulatory Impact Statement and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the preferred option.**

Privacy of Natural Persons

**Responsible Manager(s) signature:**
**Glen Hildreth**
**Manager Consumer Policy**
**22 May 2025**

## Quality Assurance Statement

| | |
|---|---|
| **Reviewing Agency:** Ministry of Business, Innovation and Employment | **QA rating:** Meets |

**Panel Comment:**

The Panel consider that the information and impact analysis summarised in the RIS meets the Quality Assurance criteria. The RIS is clear, concise, complete and convincing. While a full public consultation has not been carried out, there has been a targeted consultation with key stakeholders, and the analysis incorporates results from consultation on a similar Australian proposal.

## Section 1: Diagnosing the policy problem

1. Scam disruption is a fast-evolving policy issue, shaped by rapid technological change, fragmented regulatory responsibility, and increasing consumer vulnerability. Scam-related harm is growing in New Zealand. Scam losses are estimated to be between just under $200 million and $2 billion annually.[3]

2. Scams are increasingly complex and fast-moving, exploiting digital infrastructure like telecommunications networks, social media, messaging apps, and online banking platforms. These scams often rely on multiple touchpoints across different service providers, making coordinated, timely disruption essential.

3. Scam disruption in New Zealand is currently industry-led, without an overarching duty-based legal framework. This light-touch approach has delivered positives to date in the banking sector – where industry has worked closely with government and introduced voluntary measures to provide better protections for consumers. Online service providers, including telecommunication companies, domain name hosts and digital platforms, also have a key role in scam disruption as they can restrict access to or remove scam content.

4. However, online service providers must navigate potential legal risk under contract and tort law if they take steps to disrupt suspected scam content that may later prove legitimate. This creates significant hesitancy to act pre-emptively, particularly in fast-moving scenarios.

5. This concern around liability has been raised by online service providers in Australia during the development of Australia's Scams Prevention Framework. This was addressed by including a legislative defence, called a "safe harbour" into the Bill that would protect the relevant entities from civil liability for any errors made for disrupting suspected scam intelligence. This was designed to remove any barriers that might prevent industry from acting swiftly to disrupt suspected scams, and therefore subjecting more consumers to the same scam. The Australian safe harbour provision has several conditions that must be met to ensure that the interests of legitimate businesses are protected and that the provision is not misused.

6. Under the status quo, Government expects industry to play an increasing role in scam disruption. The New Zealand Anti-Scam Alliance (the Alliance), launched by Hon Simpson on 10 July 2025, is a cross-sector initiative to improve New Zealand's ability to prevent, detect and disrupt scams. It brings together government agencies, banks, telecommunications providers, digital platforms, and consumer groups to coordinate efforts and enhance consumer protection. It aims to improve how scam-related intelligence is shared and acted upon across sectors, update industry codes of practice, raise public awareness, and support businesses and consumers with tools to prevent and respond to scams. MBIE is the coordinating agency for the Alliance.

[3] Data sources: the nearly $200 million figure is based on reported data from Payments New Zealand, released by MBIE as part of the annual Fraud Awareness week campaign in 2024. The $2 billion figure is from the 2024 *State of Scams in New Zealand* report by Netsafe.

7. However, in the absence of legal protection, online service providers may limit their intervention to low-risk, clear-cut scams, or delay action while seeking legal assurance. This is likely to constrain the pace and consistency of disruption responses which may reduce the effectiveness of voluntary action over time.

8. Confidential Advice to Government

**What is the policy problem or opportunity?**

9. Scam disruption is an increasingly urgent policy issue, but providers' ability to act quickly and confidently is constrained by potential liability when disrupting suspected scams. The current legal framework does not create an enabling environment for providers acting in good faith to protect consumers from scams. As a result, voluntary action is often delayed or inconsistent, increasing the risk of harm to consumers from scams.

10. It is difficult to assess the scale of this problem as we cannot determine the quantity of scams that would be disrupted if the safe harbour did exist. Instead, we are relying on anecdotal evidence from online service providers that there are more proactive measures they would be able to take if they had more certainty that they would not be exposed to legal liability for good faith errors. We are also relying on the submissions from industry in Australia that commented on the need for a safe harbour in the development of the Scams Prevention Framework.

**What objectives are sought in relation to the policy problem?**

11. The primary objective is to provide greater clarity and confidence for providers to take timely, reasonable and proportionate action to disrupt suspected scams without fear of prosecution.

**What consultation has been undertaken?**

12. Industry engagement has been ongoing since early 2024 on strategic and coordination issues. Since late 2024, engagement has begun with industry on potential regulatory hurdles and solutions. This engagement has included a range of issues related to scam prevention, including this liability concern raised by industry.

13. Targeted consultation was undertaken in November through an agency-led workshop, and in December 2024 and March 2025 where the Minister convened government, industry and consumer groups to understand problems relating to stopping scam activity (December) and to test a wider set of coordination and regulatory proposals to

address scams (March). More information on the attendees and topics of discussion is set out in Annex 1.

14. No formal public consultation has been undertaken due to the Minister's expressed concern that consultation would incur delays to implementation. In the absence of formal consultation feedback, we reviewed submissions from the Australian select committee's consideration of the Scams Prevention Framework Bill, which included a similar safe harbour provision.

## Section 2: Assessing options to address the policy problem

### What criteria will be used to compare options to the status quo?

15. **Effectiveness** – how well does the option support more confident, proactive scam disruption by providers?

16. **Proportionality** – is the option appropriately targeted to the problem, avoiding unnecessary regulatory burden while still achieving the objective?

17. **Practicality** – how feasible is the option to implement, considering the alignment with existing industry structures, cost and time to implement/operationalise?

18. These criteria will be equally weighted.

### What scope will options be considered within?

19. This RIS considers options that address the specific problem of perceived legal risk faced by online service providers when taking voluntary action to disrupt scam websites. The scope is deliberately narrow, reflecting Ministerial direction to focus on a safe harbour provision rather than a broader regulatory framework.

20. The analysis includes both legislative and non-legislative options that could enable or encourage proactive scam disruption, provided they do not significantly expand government enforcement powers. Options that would shift to a prescriptive or centralised model, such as a mandatory takedown regime, were not considered. These have been ruled out due to concerns about proportionality, implementation complexity, and misalignment with New Zealand's existing regulatory approach in the digital and communication sector which is more supportive of risk-based interventions and industry-led responses. The Government's current focus on reducing compliance burden and enabling private sector innovation also supports a more targeted approach.

21. To shape the options, we considered relevant international models (particularly Australia's Scams Prevention Framework and trusted flagger initiatives in Europe), and New Zealand's Harmful Digital Communications Act 2015 (**HDCA**). Full replication of international models was deemed inappropriate given differences in legal systems, institution responsibilities and levels of government intervention. The preferred approach is targeted, enabling, and industry-led, which is consistent with feedback from stakeholders and the Government's emphasis on light-touch, responsive regulation.

22. As a result, the options assessed in this impact analysis are bounded by:
    - Ministerial preference for a safe harbour provision
    - Industry and agency feedback on practicality and proportionality
    - The need to support voluntary action while avoiding significant compliance or administrative burden.

## What options are being considered?

### Option One – Status quo

23. Under this option, no amendments would be made to existing legislation or operational settings. Online service providers would continue to operate within the current legal framework, which lacks explicit provisions addressing potential liability for mistaken actions intended to proactively disrupt scams. This would continue the current process of online service providers only proactively disrupting scams within their current risk appetite. This may result in ongoing hesitation to act and potentially deterring proactive efforts to protect consumers.

### Option Two – Trusted flagger model

24. This option would establish a framework where designated experts (e.g. a government agency or independent entity) identifies, collects and collates scam reports and recommend to online service providers that they disrupt suspected scam activity. Online service providers typically grant trusted flaggers of harmful online content priority status, which means the online service providers review their recommendations without undue delay.

25. While this option does not remove legal liability from providers when taking action to disrupt scams, it can support more confident and timely decision-making by giving online service providers a credible basis for action. We have heard anecdotally from engagement that having an approved entity flagging online content is useful for disrupting scam content.

26. The trusted flagger mechanism could be implemented through a voluntary arrangement between entities - as is already the case with Netsafe and the New Zealand Police in the online harm space.

### Option Three – Legislative safe harbour provision

27. This option would amend the Fair Trading Act 1986 to establish a statutory defence (a "safe harbour") that online service providers can rely on if they are subject to a civil liability claim because they have mistakenly disrupted online activity by a legitimate business when intending to disrupt a scam; and the business suffered harm as a result. This type of legal defence is incorporated into the Australian Scams Prevention Framework Act. The Australian legislation has a requirement for entities to meet certain conditions in order to rely on the safe harbour. A similar limit on civil liability is also included in New Zealand's Harmful Digital Communications Act 2015 (HDCA). In that context, the defence applies to online content hosts who act on approved takedown requests. The defence offers legal protection where online content hosts act in good faith and follow the statutory process.

28. To ensure that access to justice is not unreasonably interfered with, the safe harbour provision under this option would apply only when specific conditions are met, such as acting in good faith and within defined parameters. This approach aims to provide legal clarity to encourage proactive, industry-led scam prevention measures by reducing the risk of liability in the event of a mistake.

### Option Four – Positive duty to act

29. This option proposes introducing a positive statutory duty for online service providers to take reasonable and proportionate action to prevent scams circulating on their networks. The duty would require providers to establish systems and processes to identify, assess and where appropriate, disrupt suspected scam activity. This model would be broadly based on Australia's new Scams Prevention Framework, which is the first of its kind worldwide and yet to be assessed for its effectiveness but offers a potential precedent for this type of regulatory approach.

30. This model aims to clarify what action is expected of industry and provide protection where those actions are taken appropriately. However, it would likely require a regulator to monitor and enforce the duty.

### Stakeholder feedback on the options

31. As outlined above, MBIE undertook targeted consultation on this proposal. Feedback indicated support for the introduction of a legislative safe harbour provision to support industry to take proactive steps to disrupt scam activity. There was no negative feedback from any stakeholders present. Later feedback from telecommunications sector participants indicated preference for a positive duty to accompany the safe harbour provision. This was to align better with overseas approaches such as those taken in Australia. The telecommunications sector considers that a positive duty would be more persuasive in encouraging industry initiatives. Due to time constraints for both formulating policy and implementation, we consider that a positive duty should not be pursued.

32. The telecommunications industry body and one of its members also supported a trusted flagger-type model as an operational solution, to sit alongside the legislative safe harbour provision.

33. Feedback was positive from businesses and groups, including law firms, that represented their interests during the Australian select committee for the Scams Prevention Framework Bill. Most submitters thought that the introduction of such a provision is a necessary and useful tool to encourage industry-led action. Many submitters on Australia's Bill either have separate New Zealand legal entities of the same name or operate in both jurisdictions (eg banking sector participants, digital platforms). The combination of direct engagement and reviewing Australia's consultation has illustrated support for introducing a legislative safe harbour provision in New Zealand. Most of these submitters highlighted the 'window' of time that the safe harbour provision should apply – for example, 28 days. This would be considered in drafting.

### How do the options compare to the status quo?

| | Option One – Status quo | Option Two – Trusted flagger model | Option Three - Safe harbour provision | Option Four– Positive duty to act |
|---|---|---|---|---|
| **Effectiveness** | 0<br>Maintains perceived legal risk. Providers likely to remain hesitant to act proactively. | +<br>Improves coordination but legal risk for providers persists. Confidence may increase incrementally. | ++<br>Directly addresses perceived legal risk. | 0<br>Creates enforceable obligations. Unclear if this will reduce liability concerns. |
| **Proportionality** | 0<br>No new burdens. No change in disruption capability or protection. | +<br>Flexible and non-regulatory. Accountability remains unclear. | ++<br>Targeted and clear. Enables voluntary action without imposing duties. | +<br>Could impose burdens inconsistent with light-touch regulation. |
| **Practicality** | 0<br>No changes required. Relies on existing frameworks. | -<br>Requires new operational model and likely funding. | -<br>Requires legislation but no operational change. | --<br>Requires legislation and regulatory enforcement capability. |
| **Overall assessment** | 0<br>Does not resolve the problem. Maintains status quo of risk aversion. | +<br>Partial improvement through coordination, but core issue remains. | +++<br>Enables confident, timely disruption. | -<br>Could improve outcomes but higher cost and complexity. |

**Key for qualitative judgements:**

++ much better than the status quo

+ better than the status quo

0 about the same as the status quo

- worse than the status quo

- - much worse than the status quo

**What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?**

34. The preferred approach combines a regulatory tool (safe harbour) and a non-regulatory support mechanism (trusted flagger) because together they offer complementary benefits: reducing legal risk to enable faster action, while also supporting more accurate and coordinated disruption through expert input, without constraining providers' discretion.

35. This combination of these two options is the preferred approach because it most directly addresses the core policy problem: perceived legal risk, which is currently a barrier to timely and proactive scam disruption by online service providers. This uncertainty creates hesitation to disrupt scams, particularly where actions may involve content removal that could later be legally challenged. A trusted flagger regime could support this through greater coordination and as an optional source to support verification of the suspected scam website.

36. The proposed conditional legal protection from civil liability would be available where specific criteria are met. The criteria could include (based on the Australian legislative model), where the action to disrupt the suspected scam website is:
    - taken in good faith
    - the online service provider has a reasonable belief that the content is a scam
    - taken within a certain time and
    - reversed promptly if found to be in error.

37. Combining Options 2 and 3 enables confident, timely action by industry, without imposing new positive duties or broad regulatory obligations on the public. This approach is targeted and risk-based, reflecting the Government's commitment to a light-touch, enabling regulatory approach that supports industry-led solutions and protects consumers.

38. The primary beneficiaries of the proposal are online service providers, who gain greater legal protection in the event they make an error. Consumers also benefit indirectly through improved scam disruption and reduced potential financial harm. No significant adverse distributional impacts are expected, as the safe harbour provision does not impose new obligations on other sectors or groups. There is some risk that legitimate businesses or individuals would be affected if content is mistakenly disrupted. This risk is mitigated by conditions attached to the safe harbour provision. This helps balance the interests of scam prevention with the protection of lawful commercial activity and free expression.

39. We do not anticipate significant impact on business competition in the online services sector, as the safe harbour provision applies broadly to all providers engaging in scam disruption and does not create market advantages for any one online service provider.

40. New Zealand's approach to intermediary liability under the Harmful Digital Communications Act 2015 provides a useful precedent. That framework introduced a legal safe harbour provision for online content hosts who follow a defined complaints-handling process, enabling action to limit harmful content while avoiding undue liability.

41. A similar approach to scam disruption would reduce legal risk for online service providers acting in good faith, while maintaining appropriate safeguards for consumers and businesses.

42. The safe harbour provision is:
    - Highly effective because it removes a key barrier to voluntary disruption efforts
    - Proportionate because the protection is conditional and the online service provider must be able to reverse the disruption if an error is found, and
    - Practical because it does not require a new regulatory body, powers or processes, and would operate alongside existing regulatory structures.

43. The trusted flagger is an optional support mechanism and enables online service providers to both act independently upon their own volition (for example, a telecommunications provider receives internal reports and disrupts a potential scam webpage). Or alternatively, for trusted flaggers to raise an issue with the online service provider for them to act on.

44. This option does not constrain provider discretion. Online service providers may act independently where confident the safe harbour provision conditions are met or seek a trusted flagger's input in cases of uncertainty or where coordination is required.

45. This assessment assumes online service providers will use the safe harbour provision as intended — i.e. in response to scam threats rather than for unrelated content moderation purposes. Benefits are primarily non-monetised but expected to be high, including improved scam disruption rates, reduced financial harm to consumers, and increased industry confidence to act. The benefit-cost ratio is expected to improve over time as scam tactics evolve and reliance on rapid disruption responses grows, increasing the value of a responsive and enabling regulatory environment.

**Is the Minister's preferred option in the Cabinet paper the same as the agency's preferred option in the RIS?**

46. Yes. The Minister supports a safe harbour provision and a trusted flagger model (options 2 and 3).

**What are the marginal costs and benefits of the preferred option in the Cabinet paper?**

| Affected groups | Comment | Impact | Evidence Certainty |
|---|---|---|---|
| **Additional costs of the preferred option compared to taking no action** | | | |
| Online service providers | Minor compliance effort to meet safe harbour provision conditions. One-off adjustment with no ongoing burden. | Low to moderate (non-monetised) | Medium – Based on stakeholder feedback and precedent from the HDCA. |
| Courts (via litigation) | Occasional role in determining if conditions of immunity were met in legal disputes. | Low (non-monetised) | Low – our analysis is based on expected limited volume of cases and alignment with Australian and HDCA precedent. |
| Legitimate businesses (affected third parties) | Risk of revenue loss or disruption if legitimate services are mistakenly disrupted. The frequency of this occurring is expected to be low. The provider must reverse the disruption promptly if an error is found. | Low to moderate (non-monetised) | Low – impact is contingent on error. The conditions will mitigate this risk. |
| Trusted flagger agencies | Some resourcing required to support the trusted flagger function. Cost depends on volume, agency model, and use of existing capacity. Depending on agency/ organisation, it could support existing scams remit. | Low (non-monetised) | Medium – Depends on design choices and operating model. |
| **Total monetised costs** | N/A – monetised costings unavailable. | | |
| **Non-monetised costs** | Low – potential lost revenue for affected legitimate businesses and compliance cost for online service providers to self-assess actions against safe harbour provision conditions. | | |

| | | | |
|---|---|---|---|
| | Low to moderate – compliance effort, possible court use, limited resourcing of trusted flagger role. | | |
| **Additional benefits of the preferred option compared to taking no action** | | | |
| Online service providers | Increased legal protection enables more proactive scam disruption without fear of liability.<br>Trusted flagger gives online service providers an additional data point to inform online disruption activity. | Potentially high (non-monetised) | Medium – Based on stakeholder engagement and safe harbour provision precedent. |
| Consumers | Faster scam disruption reduces financial harm and builds trust in digital systems. Real-world experience from the National Cyber Security Centre's cyber disruption tools shows that blocking scam domains leads to faster disruption with minimal false positives. This builds public trust in digital infrastructure. | High (non-monetised); broad public impact | Medium to high – Supported by scam loss data and consumer surveys. |
| Courts (via litigation) | Nil – some benefit in government providing the defence to support the court's decision-making, but marginal benefit only. | Nil (non-monetarised) | Low – as a similar safe harbour provision in Australia has not yet been implemented. |
| Legitimate businesses with online activity | Clearer position that government supports timely action by regulated groups to disrupt suspected scam websites. More action by online service providers to disrupt scam websites. Could also improve trust and confidence of customers transacting with the business online. | Low-medium (non-monetised). | Medium – Based on submissions from affected businesses and Australia's Scam Prevention Framework Bill. |
| **Total monetised benefits** | Not quantified but likely to reduce financial losses for consumers over time | | |
| **Non-monetised benefits** | High – more confidence for online service providers to disrupt online scams and increased public trust in digital services. | | |

## Section 3: Delivering an option

### How will the proposal be implemented?

47. The proposed safe harbour provision would be implemented through amendments to existing legislation, such as the Fair Trading Act 1986. A trusted flagger mechanism could be developed and operationalised through the Alliance. It would not require new statutory powers or enforcement capability. Two key pillars of the Alliance are 1. Collaboration: focused on increasing data sharing and intelligence and coordination and 2. Disruption: focused on tackling scammers at scale by uniting national efforts across sectors. We consider the Alliance is well placed to develop and operationalise trusted flagger(s).

48. While the safe harbour is the primary regulatory intervention, we have chosen to pair it with a non-legislative trusted flagger mechanism to provide operational support. This combination reflects feedback from stakeholders and industry that legal protection alone may not be sufficient to support timely and confident disruption decisions, and the fact that a broader duty-based framework is out of scope for this work. The trusted flagger mechanism is not a condition for using the safe harbour but offers a flexible tool to aid decision-making – particularly where scam intelligence is complex or contested.

49. The effectiveness of the safe harbour provision (Option 3) does not rely on the trusted flagger (Option 2) being in place. Therefore, if there are delays or risks associated with implementing the trusted flagger mechanism, the legislative safe harbour can proceed independently.

*Responsibility for implementation*

50. The liability limitations would provide a conditional statutory defence, meaning regulated groups are responsible for assessing whether their actions meet the legal criteria for protection. Therefore, there is no need for a new enforcement agency, or an extension of an existing agency's enforcement or regulatory powers. If a dispute arises, courts will determine whether those conditions are met, and the provider would have the onus of proving the conditions under the safe harbour provision. MBIE may play a limited role in issuing non-binding guidance to support interpretation and sector readiness, including through its coordinating role in the Alliance to develop and operationalise trusted flagger(s).

51. Providers may act independently under the safe harbour provision without input from the trusted flagger. The flagger is intended to improve coordination and decision confidence, to provide further intelligence about whether a website or online content is a scam.

*Timing and commencement*

52 Confidential Advice to Government Confidential Advice to Government. The safe harbour provision will not have retrospective effect, meaning it cannot be relied upon by industry for any action taken before amending legislation comes into force.

53. As above, we propose to work with Alliance members to develop and operationalise the trusted flagger roles. We anticipate that the trusted flagger roles could be operationalised by early 2026, to coincide with the implementation of the Alliance work.

*Funding*

54. No additional operational funding is required to implement the safe harbour provision. The proposal does not involve proactive monitoring or administration by regulators. Any cost to government would be limited to policy development and legislative drafting, which is minor and already resourced.

55. An existing entity or the operational scam alliance under development could pick up this role. Should existing entities take on trusted flagger roles, this would need to be funded within baselines, though it is possible that some work would need to be stopped to pick up this role.

*Supporting awareness and compliance*

56. Clear guidance materials and a targeted communications effort will be needed to ensure affected industry bodies and consumer groups understand the purpose, scope and limits of the safe harbour provision.

*Risks and mitigation*

57. The key implementation risk is that providers may misinterpret or overextend the safe harbour provision, leading to unnecessary service disruption or consumer complaints. This risk is mitigated by clearly defined statutory conditions (e.g. good faith, proportionality, reversibility), sector consultation, and supporting guidance.

58. There is also a risk that providers may over-rely on trusted flaggers and delay action while awaiting confirmation. This will be mitigated by guidance clarifying that the safe harbour provision permits proactive, independent action, and that the flagger is a supporting mechanism.

59. Existing systems already enable rapid reversals of erroneous takedowns — usually within hours — which helps mitigate the risk of wrongful disruption. The safe harbour would sit alongside these procedural safeguards.

*Further work*

60. Following passage of legislative amendments, MBIE will support implementation through stakeholder engagement, provision of guidance, and monitoring any early application issues. Further changes to regulatory settings on scams are not anticipated at this stage.

**How will the proposal be monitored, evaluated, and reviewed?**

61. The proposed safe harbour provision would be a conditional statutory defence from civil liability. It would not require ongoing regulatory oversight or administration. Instead, the safe harbour provision would apply only where providers meet clearly defined conditions (such as acting in good faith, proportionality, and within a defined timeframe).

62. There is no proactive enforcement role for regulators. If a dispute arises, it would be for the courts to assess—after the fact—whether the conditions of the safe harbour provision were met. In such cases, the onus would rest on the provider to demonstrate compliance with the statutory criteria. This approach is consistent with the safe harbour provision under the Harmful Digital Communications Act 2015.

63. Impact will be monitored in the following ways:
    - Industry feedback on whether the safe harbour provision is increasing confidence to take proactive scam disruption measures (qualitative)
    - Observable shifts in industry responsiveness - e.g. through voluntary reporting or illustrative case studies (qualitative)
    - The frequency and nature of disputes or legal challenges invoking the safe harbour provision (qualitative)
    - Stakeholder feedback on the use, clarity, or limitations of the trusted flagger model (qualitative)
    - Number of scam reports trusted flaggers provide to industry (quantitative).

64. MBIE will monitor the implementation of both the safe harbour provision and the trusted flagger model, supported by feedback from providers and industry associations. Early insights will be used to assess whether additional operational support, clarification, or adjustment is needed — including any impacts on the efficiency of scam response. This will align with broader stewardship responsibilities under the Fair Trading Act.

## Annex 1: Summary of Industry engagement

Three key engagements have been taken with government, industry and non-government organisations since late 2024. The workshops discussed key ongoing scam issues that industry are experiencing including:

- the lack of data sharing that is preventing the swift disruption of scam material
- the need for a central point of contact across government to ensure efficient communication of anti-scam activities and initiatives
- better industry-led commitments and voluntary codes, particularly from online service providers to ensure all participants are contributing equally to anti-scam activities, and
- barriers both perceived and real that are preventing industry from disrupting scams.

Some participants also directly highlighted the need for a comprehensive legislative intervention, similar to Australia's Scam Prevention Framework Act 2025.

The workshops include:

1. *Government Agencies and Private Sector Scams Data workshop in November 2024*

   Workshop was hosted by the Financial Markets Authority (FMA). Attendees were:

   - Banking and payments sector: BNZ, GetVerified Limited, Payments NZ.
   - Telecommunications sector: 2Degrees, Spark NZ, Telecommunications Forum.
   - Digital sector: Google New Zealand, Domain Name Commission, Meta, Microsoft.
   - Consumer representatives: Netsafe.
   - Government: FMA, MBIE, Commerce Commission, Department of Internal Affairs (DIA), Inland Revenue (IRD), Police, National Cyber Security Centre, Serious Fraud Office.

2. *A workshop in December 2024 to understand problems relating to stopping scam activity*.

   Attendees were:

   - Banking sector: Kiwibank, ASB, ANZ, Westpac, New Zealand Banking Association.
   - Telecommunications sector: Spark NZ, One New Zealand, 2 Degrees, Telecommunications Forum.
     Digital sector: Meta, Apple, Google New Zealand.
   - Consumer representatives: Consumer New Zealand, Netsafe, Banking Ombudsman.
   - Government: MBIE, Police, DIA, IRD, National Cyber Security Centre, FMA, Commerce Commission.

3. *A workshop in March 2025 to test a wider set of coordination and regulatory proposals to address scams*

   Attendees were:

- Banking sector: Kiwibank, ASB, ANZ, Westpac, New Zealand Banking Association.
- Digital sector: Meta, Apple, Google New Zealand.
- Telecommunications sector: Spark NZ, One New Zealand, 2 Degrees, Telecommunications Forum.
- Consumer representatives: Consumer New Zealand, Netsafe, Banking Ombudsman.
- Government: MBIE, Police, DIA, IRD, National Cyber Security Centre, FMA, Commerce Commission.