



COVERSHEET

Minister	Hon Andrew Bayly	Portfolio	Commerce and Consumer Affairs, Small Business and Manufacturing
Title of Cabinet paper	Proposal for an all-of-government approach to address online financial scams	Date to be published	4 December 2024

List of documents that have been proactively released

Date	Title	Author
17 October 2024	Proposal for an all-of-government approach to address online financial scams	Office of Hon Andrew Bayly
23 October 2024	ECO-24-MIN-0234 Minute	Cabinet Office

Information redacted

YES / NO (please select)

Any information redacted in this document is redacted in accordance with MBIE's policy on Proactive Release and is labelled with the reason for redaction. This may include information that would be redacted if this information was requested under Official Information Act 1982. Where this is the case, the reasons for withholding information are listed below. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Some information has been withheld for the reasons of confidential advice to Government

In Confidence

Office of the Minister of Commerce and Consumer Affairs, and Minister for Small Business and Manufacturing

Cabinet Economic Policy Committee (ECO)

PROPOSAL FOR AN ALL-OF-GOVERNMENT APPROACH TO ADDRESS ONLINE FINANCIAL SCAMS

Proposal

- 1 To set out my proposed approach to an all-of-government approach to address online financial scams.

Relation to government priorities

- 2 This proposal supports our priority to rebuild the economy by enabling legitimate businesses and consumers to confidently transact online.

Executive Summary

- 3 Online financial scams are a growing problem in New Zealand. Last year, New Zealanders lost approximately \$200 million to scams, 15 per cent more than the previous year. It is estimated that only one in five scams are reported to authorities, so the real losses to New Zealanders are significantly higher.¹
- 4 Government, industry (banking, telecommunications, and digital platforms) and consumers all play a role in addressing this issue, but the status quo is not working. There is no clear overarching direction or coordination.
- 5 My engagement with government agencies, industry, consumer groups, and international counterparts has identified that efforts in New Zealand to combat online financial scams are fragmented and unsophisticated.
- 6 Based on this engagement it has become clear there is a need for a single government agency to lead the coordination of activity within government and across industry. There is also a need for a centralised system for reporting, triaging and tracking scams. There is an opportunity to better leverage overseas expertise to New Zealand's advantage where such models have proven to be highly effective.
- 7 To do this, I propose to:
 - 7.1 work with ministerial colleagues and lead the development and implementation of a strategy to detect, prevent and respond to reduce online financial scams in real time;

¹ Data gathered from eleven of New Zealand's largest financial institutions.

- 7.2 convene a reference group with government and industry participants, including from the banking, telecommunications, and social media sectors, to better understand the breadth of activity and agree cross-sector collaborative solutions;
- 7.3 report back to Cabinet by April 2025 with a proposal for how to better coordinate government activity in the areas of prevention, reporting and mitigation; and
- 7.4 take responsibility for leading collaboration with relevant international government agencies and ministerial counterparts, particularly those in Australia and Singapore, to develop cross-border strategies for combatting scams.

Background

- 8 As Minister of Commerce and Consumer Affairs, I have a strong interest in protecting consumers. As Minister for Small Business and Manufacturing, I want to ensure New Zealand businesses have the tools and capabilities to conduct business effectively with trust and confidence.
- 9 Kiwis experienced more scams in 2023 than ever before, with 62 per cent encountering a scam at least once a month.² Many of these were scam text messages, with over 333,000 referred to the Department of Internal Affairs (DIA) each month between January and September 2023.³
- 10 It is estimated only one in five scams are reported to authorities, so while reported losses were approximately \$200 million, losses could be as high as \$1 billion.⁴ Without intervention, this problem will only worsen. These scams are largely carried out by sophisticated organised criminals who work across borders.
- 11 Online financial scams are a discrete and distinct subset of fraud. While there are processes in place to deal with fraud, online financial scams are frequently not pursued by enforcement agencies. They are prevalent, regularly harm consumers and erode trust and confidence in legitimate business activity. Overseas jurisdictions, including Australia, Singapore and the UK, have recognised this harm and have set-up regimes specifically targeting scams.
- 12 I propose a New Zealand approach to scams as a distinct subset of fraud and organised crime, in line with international practise. There is real opportunity to focus on industry-led solutions and to improve coordination to help Kiwis transact with confidence.

² Netsafe and the Global Anti-Scam Alliance; *The state of scams in New Zealand 2023*.

³ From a representative sample of scam messages actually sent within New Zealand.

⁴ Data provided from Google New Zealand, Netsafe and the Global Anti-Scam Alliance.

- 13 Action in Australia and Singapore has shown that with sufficient focus on scams, the dial can be shifted. Australia has seen a 47 per cent drop in investment scam losses within a year, largely from the work of the Australian National Anti-Scam Centre and the bank-led Australian Financial Crimes Exchange.
- 14 Earlier this year, Australia announced plans to establish mandatory scam codes for key sectors, including social media as part of its wider efforts to combat scams.

It is difficult to get any remedy for scam victims

- 15 Online financial scams take many forms. The National Cyber Security Centre can assist victims of cybercrime when there is a cybersecurity component. However, it is often difficult to recover victims' funds, as funds paid to scammers are often siphoned offshore.
- 16 In some instances, banks have taken responsibility for reimbursing scam victims' lost funds. This typically happens for unauthorised payment scams, although exceptions apply, such as when a victim shares their PIN in a non-secure way.⁵
- 17 Banks do not routinely reimburse victims of authorised payment scams, as these transactions are technically approved by the account holder.⁶ However, I have directed banks to investigate a voluntary reimbursement system for these types of scams, in line with leading international practice. The banking sector provided me with a draft proposal on how to apply these lessons in the New Zealand context and I expect to receive a more detailed proposal by the end of November.

Understanding where scams originate

- 18 Scammers often act across borders. Analysis from Meta has found many scams originate in Nigeria and South-East Asia.
- 19 Scammers mainly reach their victims through telecommunications companies' systems, including text messages and phone calls, or online through email, social media, messaging applications and fraudulent websites.
- 20 Poor controls over website creation and content moderation on online platforms means that scams circulate freely. Scammers often take out advertising to promote scams and to impersonate legitimate services, while digital platforms have limited incentives to stop scams circulating in these ways.
- 21 Most scams last year circulated on digital platforms and emails like those offered by Meta (Facebook, Instagram and Whatsapp) and Google.⁷ Scammers can buy SIM cards over-the-counter and use "SIM-bots" - machines that rapidly push out scam

⁵ In unauthorised payment scams, scammers access bank accounts without the victim's consent, often through phishing or remote access scams.

⁶ Authorised payment scams occur when a person is manipulated into making a payment to the scammer themselves, believing they are sending money for a legitimate reason. Common authorised scams include online romance scams, investment scams, impersonation scams and payments for goods or services that are never delivered.

⁷ Netsafe and the Global Anti-Scam Alliance; *The state of scams in New Zealand 2023*.

texts through telecommunications networks. If a scam is removed by a platform or blocked by a telecommunications provider, it is very easy for the scammer to create new scams, resulting in platforms and agencies chasing up reactively, rather than coordinating a strategic and proactive approach.

- 22 This is why a systemic solution that deals with the whole scam ecosystem is required. Combatting individual scams as they appear is ineffective.

Government agencies have been taking action to address online financial scams, but the landscape is complex and inefficient

- 23 As described below, government activity to address online financial scams has evolved in a reactive and uncoordinated manner. The landscape is complex and rife with duplication across a number of government agencies with different roles and responsibilities.

Multiple agencies undertake awareness-raising activities to prevent scams

- 24 The Ministry of Business, Innovation and Employment (**MBIE**), the National Cyber Security Centre and the Financial Markets Authority (**FMA**) all have information on their websites and run regular awareness campaigns to educate, warn and remind consumers, businesses and investors about how to protect themselves from cyber-attacks and scams. With the private and non-government sectors also undertaking similar activities, it is timely to review our contribution and consider whether it could be better targeted.

Detection and disruption activity is focused on certain parts of the scams landscape

- 25 The National Cyber Security Centre operates services that are focused on detecting and disrupting cyber security threats, which may include scams.
- 26 DIA provides secure identity verification services to prevent the misuse of identity information in transactions with government agencies and some businesses.
- 27 The Police and the Ministry of Justice look at the issue from a transnational organised crime lens, while the Reserve Bank engages with banks on the links between money laundering, terrorist financing and fraud and scams.

There are too many places to report scams which makes it difficult to get a complete picture of what is happening

- 28 The siloed nature of reporting makes it difficult for consumers to know where to go to get help, and government agencies can miss crucial information that could help them respond to the scam activity. People can report:
- 28.1 fraud and scams to Police's non-emergency '105' number;
 - 28.2 cyber security incidents to the National Cyber Security Centre;

- 28.3 email spam and text scams to DIA;
 - 28.4 pyramid schemes to the Commerce Commission; and
 - 28.5 investment scams and ponzi schemes to the FMA.
- 29 Outside of government, reports can also be made to banks and Netsafe, an online safety charity.
- 30 The National Cyber Security Centre is creating a cyber incident reporting service: 'Report Cyber'. This is designed to handle reports of cyber security issues but may receive reports of other scam activity which are referred to the correct agency.
- 31 Agencies have begun working together to improve scam reporting processes and data and information sharing. However, this work is in the early stages.

Overlapping remits across enforcement agencies further complicates the picture

- 32 DIA and the FMA work with industry partners to remove scam websites and block malicious phone numbers that send scam messages. However, this process is often slow, and it is compounded by the difficulty of getting digital platforms and social media companies which host these websites to respond quickly.
- 33 The Police investigate and prosecute fraud offences (including scams) under the Crimes Act 1961, and the Serious Fraud Office investigates and prosecutes serious or complex financial crime. This activity can miss smaller, more prevalent scams.
- 34 Sometimes, scam activity crosses agency remits. While government agencies sometimes work together to undertake investigations into scam and fraud activity, resulting in criminal convictions, there have also been instances where this has not happened.

Government activity is fragmented and leaves gaps for scammers to slip through

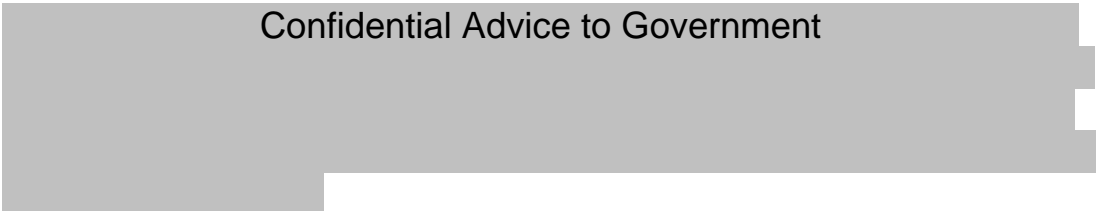
- 35 The current structure means each agency is responsible for a section of the scam ecosystem. There are multiple reporting lines, no clear lines of responsibilities and work is siloed and disjointed. The fast evolving, sophisticated nature of scams means it is impossible to effectively prevent, detect and respond without government using its collective power.
- 36 There are pockets of collaboration occurring across government, and within the private sector. On behalf of the Council of Financial Regulators, the FMA is leading collaboration between relevant agencies to develop practical initiatives to disrupt scam activities. However, there is no single lead agency with responsibility for all scams and there is a lack of awareness of the initiatives underway across government and industry.

Existing channels for sharing information about scams are unsophisticated

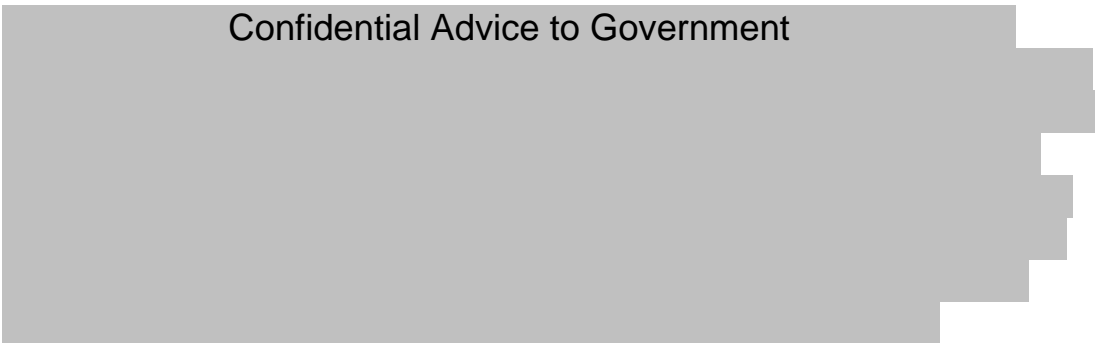
- 37 There is also no form of instantaneous communication between agencies and industry participants to report, triage and track scams. Government agencies and industry currently rely on unsophisticated methods to share intel about emerging scams. This gap is hindering agencies ability to respond to emerging scams swiftly and coordinate their actions.
- 38 There is a clear need for enhanced digital communication systems to enable faster and more effective information sharing and tracking of scams. Without a single real-time system for reporting scams, agencies and industry will continue to work in silos.

Relationship to other government work to combat crime

39 **Confidential Advice to Government**



40 **Confidential Advice to Government**



I propose to lead a coordinated approach to addressing online financial scams

- 41 I propose three key pillars to coordinate activities to address authorised and unauthorised online financial scams, which I would lead;
 - 41.1 **Coordination across portfolios and public sector agencies** with improved information and data sharing. This will streamline agency work and use resources more efficiently.
 - 41.2 **Coordination with industry** to address scams on their networks and systems. By working with industry, we can be more effective at blocking scams before they reach consumers and bring an all-of-government approach to work already underway. This will involve better coordination within specific industry sectors (e.g. banks) and between different sectors (e.g. information sharing between telecommunications and banks).

- 41.3 **Work closely with Ministerial counterparts**, including Australia and Singapore, to enhance information sharing and coordinate our national approaches to improve regional security.

Pillar One: Coordination across portfolios and public sector agencies

- 42 I have already started taking action to address scams in my Commerce and Consumer Affairs portfolio. I wrote to the banking sector in February this year to encourage them to improve bank processes and consumer protections on scams. Separately in June, I encouraged them to fully integrate with the Australian Financial Crimes Exchange to better align anti-scam efforts with Australia. This has led to the banks accelerating work to implement a confirmation of payee system. A confirmation of payee system enables consumers to check the name of the account they are paying into and is effective at preventing investment scams where individuals are misled into paying money into fake business bank accounts. Confirmation of payee will be fully operational by the first half of 2025.
- 43 I am also progressing open banking to enable consumers and businesses to share their data safely and securely, better protecting them from potential scams.
- 44 In my Small Business and Manufacturing portfolio, one of the main barriers to digitisation is a concern about cybersecurity and fraud. MBIE is working with the National Cyber Security Centre to develop cybersecurity training for small businesses. I am also exploring options to enable the New Zealand Business Number to be a 'business trust anchor' to increase business credibility and make online transactions safer.
- 45 As part of this work, Cabinet has agreed to add bank account names to the New Zealand Business Number register, to sit alongside bank account numbers. This will complement the banks' confirmation of payee functionality, which they will begin rolling out in November.
- 46 However, action in my portfolios alone will not be enough. The Police, Associate Police, Justice, Media and Communications, Internal Affairs, Government Communications Security Bureau and Digitising Government portfolios also all have an important role in addressing scams.

I am seeking agreement to lead work to address online financial scams

- 47 I propose to work closely with Ministers responsible for the above portfolios to set strategic direction to combat online financial scams, consider new initiatives, and coordinate international engagement to drive change. We have already met as a ministerial group once, and I propose we meet as required.
- 48 This will be the first time that coordinated government action, led by Ministers, has been taken to address online financial scams in New Zealand.

49 MBIE has recently convened a working group made up of officials from the respective portfolio areas and it is proposed that this group will continue to support Ministers.

50 **Confidential Advice to Government**

Pillar Two: Coordination with industry

51 My engagement with banks, telecommunications companies and digital platform providers has highlighted that all industry players need to take action. Industry is taking some steps to address online financial scams, including the banking sector by targeting mule bank accounts, and telecommunications companies working with banks and government to disrupt text scams.

I am seeking agreement to establish an industry reference group

52 I propose to bring industry representative groups together as soon as possible to discuss industry-led counter-scam initiatives, as well as the gaps and opportunities for industry-government collaboration. I would look to test proposals with this group and encourage cross-industry collaboration.

53 There is also an opportunity to put in place a voluntary industry scam code for digital platforms. Digital platforms have just agreed to such a code in Australia, modelled on a United Kingdom code. Meta indicated this is something it would support.

Pillar Three: International coordination and collaboration

54 This year, I visited Australia and Singapore to learn about their approaches to combatting scams. These visits showed strong appetite from New Zealand, Australia, and Singapore to work together more closely on anti-scam initiatives at industry and Ministerial levels. **Confidential Advice to Government**

I propose to leverage connections and international approaches as we develop our own approach to combat online financial scams

55 I intend to leverage our international relationships to consider how we can better work together to identify scams, adopt leading practice and get the agreement of social media platform providers to act quickly and appropriately to address new threats as they arise. By way of example, Australian Assistant Treasurer Hon Stephen Jones is visiting New Zealand later this year. He has responsibility for scams in Australia and I have asked him to brief the ministerial group.

56 Finally, I will monitor the implementation of recent Singapore-led regulatory initiatives, and draft Australian mandatory scam code work, to see if there are opportunities to leverage these in New Zealand.

Cost-of-living Implications

57 There are no cost-of-living implications associated with either the release of this Cabinet Paper or the workplan contained within it. The coordinated anti-scams portfolio approach may lead to policy proposals that have an indirect positive impact on New Zealanders cost-of-living.

Financial Implications

58 There are no financial implications associated with this Cabinet Paper, as work will be progressed with existing agency resources. I will report back to Cabinet on the financial implications of any proposal to better coordinate and address online financial scams.

Legislative Implications

59 There are no legislative implications resulting from the workplan of this Cabinet Paper. The coordination of ministerial portfolios may result in policy proposals to amend legislation to Cabinet in the future.

Impact Analysis

60 Regulatory impact analysis does not apply to the proposals in this paper as no regulatory change is sought.

Climate Implications of Policy Assessment, Population Implications and Human Rights

61 This paper does not seek policy decisions and therefore there are no climate implications. The proposals of this Cabinet Paper have no direct population or human rights implications.

Use of External Resources

62 There have been no use of external resources arising from this paper.

Consultation

63 The following agencies have been consulted: DIA, Department of Prime Minister and Cabinet, the National Cyber Security Centre, Serious Fraud Office, New Zealand Police, Reserve Bank New Zealand, Ministry of Justice, FMA, and the Commerce Commission.

64 I have engaged with many industry groups and consumer representatives. These include The New Zealand Banking Association, the Telecommunications Forum, Google, Meta and Consumer New Zealand.

Communications

65 I intend to issue a press release shortly after this paper has gone to Cabinet. As noted above, I will also convene an industry reference group.

Proactive Release

66 The contents of this paper will be proactively released within proactive release guidelines with appropriate redactions if needed.

Recommendations

The Minister of Commerce and Consumer Affairs recommends the Committee:

- 1 **note** that scams are a growing issue in New Zealand, with New Zealanders last year losing approximately \$200 million to scams;
- 2 **note** that levers to address scams sit across government, industry, and individuals;
- 3 **agree** to a government approach to address online financial scams around three pillars: coordination across government portfolios, working with industry, and collaboration with international counterparts;
- 4 **agree** that the Minister of Commerce and Consumer Affairs be the lead Minister to coordinate and drive action to address online financial scams;
- 5 **agree** that the Minister of Commerce and Consumer Affairs will work with Ministers responsible for the Government Communications Security Bureau, Internal Affairs, Police, Associate Police, Media and Communications, and Justice portfolios to lead an all of government coordinated response;
- 6 **agree** that the Minister of Commerce and Consumer Affairs instruct the Ministry of Business, Innovation and Employment to convene an industry reference group;
- 7 **agree** that the Minister of Commerce and Consumer Affairs will collaborate with international counterparts to join up work and develop regional strategies for addressing online financial scams;
- 8 **direct** the Minister of Commerce and Consumer Affairs to report back to Confidential Advice to Government with a proposal for how government and industry can work together more effectively to prevent, detect and deter scams, Confidential Advice to Government

Hon Andrew Bayly

Minister of Commerce and Consumer Affairs
Minister for Small Business and Manufacturing