



New Zealand Anti-Scam Alliance

JULY 2025



MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

Te Kāwanatanga o Aotearoa
New Zealand Government



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI

Ministry of Business, Innovation and Employment (MBIE) Hīkina Whakatutuki – Lifting to make successful

MBIE develops and delivers policy, services, advice and regulation to support economic growth and the prosperity and wellbeing of New Zealanders.

More information

Information, examples and answers to your questions about the topics covered here can be found on our website: www.mbie.govt.nz.

Disclaimer

This document is a guide only. It should not be used as a substitute for legislation or legal advice. The Ministry of Business, Innovation and Employment is not responsible for the results of any actions taken on the basis of information in this document, or for any errors or omissions.

ISBN (online) 978-1-991143-22-8

JULY 2025

©Crown Copyright

The material contained in this report is subject to Crown copyright protection unless otherwise indicated. The Crown copyright protected material may be reproduced free of charge in any format or media without requiring specific permission. This is subject to the material being reproduced accurately and not being used in a derogatory manner or in a misleading context. Where the material is being published or issued to others, the source and copyright status should be acknowledged. The permission to reproduce Crown copyright protected material does not extend to any material in this report that is identified as being the copyright of a third party. Authorisation to reproduce such material should be obtained from the copyright holders.

New Zealand Anti-Scam Alliance

The New Zealand Anti-Scam Alliance brings together government, industry, and consumer organisations in a unified partnership that strengthens New Zealand's ability to prevent, detect, and disrupt scams. By working collaboratively and placing people at the centre, we aim to build trust, reduce harm, and make New Zealand a harder target for scammers.

Background

Scams are having a growing economic and social impact on New Zealanders, challenging the assurances of institutions, businesses, and government. As scam tactics become more sophisticated, a coordinated and large-scale response is essential.

To address this, organisations across the public, private, and not-for-profit sectors have committed to forming the **New Zealand Anti-Scam Alliance**. This alliance will lead the design and delivery of a national anti-scam work programme focused on disrupting scams, protecting individuals and communities and making New Zealand a harder target for scammers. This alliance is built on shared objectives, a commitment to collaboration, and a joint approach to shaping the work programme through a design phase. This will lay the foundation for future operational collaboration and long-term impact.

Success for the Alliance will look like:


- › We (government, industries and non-profits) share information and insights to take a coordinated and targeted approach to prevent, detect and disrupt scams.
- › We are connected with international counterparts to pursue scammers and tackle scams that affect New Zealanders.
- › Consumers and businesses know how to protect themselves from scams, and where to go for help.
- › Banks, telecommunications companies and digital platforms put in place stronger protections for their customers against scams.

Guiding Principles for the Alliance

This alliance is grounded in a shared commitment to collaboration that strengthens, rather than replaces, the work of individual organisations and agencies. It takes an ecosystem approach with people at the centre. The aim is to amplify the collective impact of our anti-scam efforts to deliver better outcomes for individuals and communities across New Zealand. This alliance will be guided by the following principles:

- › **People-centred approach:** Efforts are designed around the needs of individuals and communities.
- › **Aligned for impact:** Government and industry collaborate with clear roles and shared objectives to deliver a coordinated and effective response to scams.
- › **Leverage existing strengths:** This alliance builds on existing capabilities, avoids duplication, and draws on unique experience and infrastructure of each Member; and
- › **Driven by intelligence and international insights:** Our actions will draw on data, intelligence, and proven examples of local and international approaches to deliver targeted response to scams in New Zealand.

Alliance Objectives



COLLABORATION

- › **Data Sharing & Intelligence:** to increase the sharing of anti-scam data and intelligence between not-for profit organisations, the public sector and the private sector. The objective is by sharing this information, it will provide insights that support scam prevention, detection and disruption.
- › **Coordination:** to organise and run collaborative anti-scam programmes of works across and between industries and in the not-for profit, public and private sectors.

Next steps


To achieve Government objectives, agencies, industry and not-for-profit organisations will develop a detailed work programme building on the key existing initiatives and activities across the sector ([see Annex](#)). The key activities include:

Data Sharing & Intelligence

- › To build on existing anti-scam data sharing initiatives and introduce new actions where needed.
- › Agree minimum standards for security and data quality for anti-scam data sharing activities to ensure that those activities comply with applicable laws.

Coordination

- › Use insights derived from shared anti-scam data sharing activities to inform anti-scam work programmes for Members, including through a ‘trusted flagger’ initiative to support timely scam disruption¹. Work programmes will be based on the Strategic Pillars.




DISRUPTION

- › **Nationally:** to tackle scammers at scale by uniting national efforts across and between Government, law enforcement, not-for-profit organisations, regulators and the private sector.
- › **Internationally:** to engage with other international anti-scam organisations to tackle scams that impact New Zealand and other countries.

Next steps

To achieve Government objectives, agencies, industry and not-for-profit organisations will develop a detailed work programme building on the key existing initiatives and activities across the sector ([see Annex](#)). The key activities include:

- › Agree and prioritise work programmes across and between industries and in the not-for profit, public and private sectors to deliver against a National Anti-Scam Strategy.
- › Create industry work programmes to drive innovation and co-ordinate industry specific roadmaps for anti-scam initiatives.
- › Deliver and operationalise centralised capability and tooling to enable enhanced collaboration across Members.



EDUCATION AND AWARENESS

- › **Consumers:** raise awareness of and educate the New Zealand public about scams, including prevention and what to do when a scam occurs; and
- › **Businesses:** educate New Zealand businesses on how they can prevent and respond to scam risks, including through cyber security practices.

Next steps


To achieve Government objectives, agencies, industry and not-for-profit organisations will develop a detailed work programme building on the key existing initiatives and activities across the sector ([see Annex](#)). The key activities include:

Consumers

- › Provide advice on how individuals can protect themselves from becoming a victim of a scam.
- › Establish a main point of contact for reporting scams and inform victims on how they can receive support.
- › Campaign for better awareness of scams, including making lists of known scams publicly available.

Businesses

- › Develop training programmes for New Zealand businesses on how they can investigate and respond to scam risks.



VOLUNTARY CODES

- › **Industries:** drive change at level by supporting New Zealand industries to implement voluntary codes of practice which set standards for the prevention and detection of and response to scams.

Next steps

To achieve Government objectives, agencies, industry and not-for-profit organisations will develop a detailed work programme building on the key existing initiatives and activities across the sector ([see Annex](#)). The key activities include:

- › Support industry bodies in the formulation and uplift of voluntary sector codes which set standards for the prevention, detection of and response to scams.
- › Consider alignment between sector codes.





For clarity, the scope of alliance activities will not include victim redress.

This shared alliance will work together to develop a National Anti-Scam Strategy that can be implemented through each of the four pillars.

¹ A “trusted flagger” is a term used to refer to agencies who have preferential access and/ or trusted status with Members to refer on scam intelligence for consideration.

Strategic Pillars and Participation

The organisations listed below form the core of the Alliance and will play a leading role in shaping and contributing to the detailed work plan. We welcome other organisations to become involved.

STRATEGIC PILLARS:	   			
	COLLABORATION	DISRUPTION	EDUCATION AND AWARENESS	VOLUNTARY CODES
Co-Ordinating Lead Agency	Ministry of Business, Innovation and Employment			
Co-leads of strategic pillars	Bank of New Zealand + Department of Internal Affairs	Tele-communications Forum + Police	ASB Bank + National Cyber Security Centre	MBIE
Industry Participants	Tele-communications Forum Westpac Meta Google NZ ASB Bank	ANZ, Westpac Meta Google NZ ASB Bank Kiwibank	Westpac Tele-communications Forum Meta Google NZ Kiwibank	Tele-communications Forum ANZ, Westpac Meta Google NZ
Government Participants	Police Financial Markets Authority Inland Revenue Department National Cyber Security Centre Commerce Commission	Financial Markets Authority Department of Internal Affairs National Cyber Security Centre Commerce Commission	MBIE Commerce Commission Financial Markets Authority	Commerce Commission
Other Bodies	Netsafe (three months)		Netsafe (three months) Banking Ombudsman Scheme Consumer NZ	Banking Ombudsman Scheme Consumer NZ

Timelines



ANNEX: Anti-scam actions already underway



COLLABORATION

Google now requires financial service providers to complete verification before advertising on its platforms. This will reduce the occurrence of unlicensed financial service providers when searching online. [Financial Services Verification - New Zealand - Advertising Policies Help](#)

The **telecommunications sector** is planning to establish a Memorandum of Understanding with **digital platforms** to participate in and share information to block scam phone calls and texts to protect New Zealand customers.

The **Department of Internal Affairs** and the **telecommunications sector** have implemented early phishing domain detection through the '7726' reporting number. This has enabled the telecommunications sector to provide near real-time scam intelligence for prevention. **Apple** has also collaborated with the **Department of Internal Affairs** to enable scam and spam reports to be sent directly to the Department of Internal Affairs, to further support collaborative scam prevention efforts.

The **banking** and **telecommunications sectors** are sharing information about potentially malicious websites. These websites are blocked by telecommunications sector if they are found to facilitate scams or fraud.

Netsafe chairs the Oceania chapter of the Global Anti-Scam Alliance. The **Telecommunications Forum** and **Meta** sit on the board. Several **government agencies** participate in this forum.



DISRUPTION

The **banking sector** is continuing to target mule accounts. These accounts are used to store and siphon funds scammed from victims. The sector has also introduced a Confirmation of Payee (account to name matching software) for customers.

The **Domain Name Commission** can suspend suspicious scam websites using the '.nz' domain name to prevent fraudulent companies.

Inland Revenue is rolling out compulsory Multi-Factor Authentication (MFA) on myIR. This will improve security on customer's online accounts, reducing the risk of account takeover by a scammer. Roll out is phased and began in April.

The **Financial Markets Authority** issues public warnings about investment scams and some pyramid schemes. Warnings are shared with banks to support wider scam prevention and disruption efforts. See here: [Scams | Financial Markets Authority](#)

Meta and the **banking sector** have been working to commence reporting of scam URLs on Facebook and Instagram to Meta through an appropriate aggregator, such as the Australian Financial Crimes Exchange.

The **telecommunications sector** has implemented rules to restrict scammers being able to swap SIM cards to take control of consumers' mobile accounts. In addition, consumers must now actively verify their identity and provide consent when they switch from one mobile provider to another. This helps to protect against scammers accessing the consumer's personal information.

The **telecommunications sector** uses scam prevention tools across their network to help identify and disrupt scam activity. These tools help block international fraudulent calls and scam text messages to protect consumers and avoid scammers impersonating New Zealand companies and government agencies.



EDUCATION AND AWARENESS

Many **government** agencies post online guidance and information on how to spot scams, and what to do if you've been scammed. If you are ever unsure, you should stop communication immediately and call the agency back on its listed number.

The **government** regularly runs anti-scam awareness campaigns, such as the annual Own your Online and Fraud Awareness Week campaigns that help consumers spot scams early. Other educational content includes the Serious Fraud Office's Fraud Film Festival that produces engaging anti-fraud related content.

NZ Verify and all of Government App: the Department of Internal Affairs has begun work on an All-of-Government app that will improve the way New Zealanders interact with their government. When you receive an email or text message claiming to be from a government agency, it can be hard to determine whether the message is legitimate. This App will enable government agencies to send authentic and verified messages to New Zealanders.

The **banking sector** regularly publishes useful tools and resources online to help customers better protect themselves from scams.

Digital platforms deliver scam awareness campaigns in New Zealand, including partnership with Netsafe.

Online anti-scam resources can be found here:
[Own your Online](#)
[Netsafe](#)
[Consumer Protection](#)



INDUSTRY CODES

Digital platforms are commencing discussions around the development of a voluntary New Zealand Online Scams Code. This will provide guiding non-binding obligations on platforms around anti-scam protections. More information on the Australian code at: [SCAMS | DIGI](#)

The **telecommunications sector** recently announced it is reviewing its Scam Prevention Code. The review will ensure the Code is still fit for purpose and incorporates the new anti-scam initiatives that telecommunications providers are implementing today.

The **banking sector** has announced stronger consumer protections through changes to its Code of Banking Practice, in late 2025. The changes will introduce pre-transaction warnings, identification and response to high-risk transactions, 24/7 reporting, scammer account information sharing.



Te Kāwanatanga o Aotearoa
New Zealand Government