Independent Research Solutions

The crime of the future that's here today

A REPORT ON SCAMS AND WHAT NEW ZEALAND NEEDS TO DO

Acknowledgments

This report was made possible by the New Zealand Crime and Victims Survey Contestable Fund. It was also supported by Ministry of Justice staff, notably Tianying Chu, Charlie Russell and Anna Kasperczyk, who were among the most supportive people we've ever worked with.

Great thanks to all of the people who took time to be interviewed. We trust we have been faithful in capturing your views.

We also acknowledge the expertise and help of our research oversight committee, which included Rob Pope, Ruth Money, and Bridget Doell. Each cast informed and critical eyes over the work and were invaluable. While we could not be more grateful to them, the findings and recommendations contained in this report – and any errors – are ours.

Jarrod Gilbert and Ben Elley

January 2025

Contents

Acknowledgments 2

Introduction 4

Methods 5

Definitions 6

Executive summary 7

- The present and future of scams in New Zealand 10
- The scale of scams in New Zealand 10
- Scams affect everyone 15
- The serious impacts of scams 15
- Scams have not been taken seriously 16
- Cyber scams will grow in volume and sophistication 18
- Anti-scam approaches remain largely untested 19

The reporting system is broken 21

- The underreporting of scams 21
- The reporting process is complex and confusing 23
- Police are poorly equipped to deal with scams 25
- No right door 26
- Some victims do not want to make a full report 27
- Recommendations 28
  - Lead agency needed 28
  - Unified reporting channel needed 28
  - Victim support needed 29

Public education 30

- Public education campaigns 30

Simple tricks for scam prevention may not be helpful 31
Public education campaigns are not a substitute for scam prevention 32
Does a focus on education serve other interests? 33
The private sector 34
Fraudsters target weaknesses in systems 35
New Zealand's consumer protections are weak 35
Existing anti-scam efforts in the private sector 36
Banks 37
Telcos 38
Tech companies 39
Other countries are enacting significant consumer protections 42
Multinational tech companies may be highly resistant to regulation 45
Recommendations 45
The fairest approach is one where companies bear the cost of scams that occurs through their systems 45
The government can be an enabler of private sector communication 47
SIM card registration rules needed 47
Establishing an effective response 49
A combined anti-scam centre is the best approach 49
Public-private partnership is required 50
Current models of communication may not be a good basis for effective collaboration 51
Fast intelligence processing and response is essential 52
Scam prevention is a matter of data 53
Privacy Act changes may be needed 54
Allowing New Zealand's scam response to languish will lead to New Zealanders being targeted 54

Introduction

The latest cycle of the New Zealand Crime and Victims Survey (NZCVS) estimates that 437,000 adults experienced instances of 'fraud and deception' victimisation within the last 12 months. That this immense wave of scams has landed upon New Zealand so quietly, and largely without public outcry, is shocking but also unsurprising.

The large majority of these scams are cyber scams. As information technology has become pervasive in our lives, it has opened vast new avenues for exploitation, often by scammers who live on the other side of the world. Cyber scams, once seen as the crime of the future, are now a reality of everyday life.

This type of scam, though highly prevalent now, can be expected to grow in sophistication and harm, both to individuals and the economy.

The issue has largely been ignored until very recently, and scam reporting, policing, and intelligence sharing systems are largely unfit for purpose.

When this research project began in early 2024, scams were not identified as a priority for the New Zealand government. This has recently changed with a series of announcements by Minister of Commerce and Consumer Affairs, Andrew Bayly, who will be taking the new role of Anti-Scam Minister and coordinating a combined effort across government.

This research is designed to aid that effort. Developed through interviews with 40 experts and victims, it establishes the key issues of scams, and lays out the key steps New Zealand needs to take to bring our response up to the international standard.

This is a global issue, and in fact many of the countries that we normally compare ourselves to have pulled ahead in regard to tackling scams. This places us in a vulnerable position: if we allow ourselves to fall behind, we will be seen as a soft target for fraudsters operating transnationally. Swift and firm action is required, and this research provides the outline for an approach that will place New Zealand at the forefront.

Methods

This research is based on data from the NZCVS, in-depth interviewing and a review of academic literature, with the goal of building a clear understanding of scams as an issue, from which recommendations can be made.

NZCVS data was used from reports published by the Ministry of Justice, but also from previously unused data from NZCVS surveys.

In-depth interviews were conducted with a total of 40 participants. The majority of these were fraud and scam experts working in government and the private sector, as well as victim advocates, non-government organisations, and academic experts. We also spoke to 12 victims of scams of various kinds.

Interview questions varied depending on individual roles and expertise, but included a set of standard questions about current issues in scams, present weaknesses in New Zealand's system and approach, and what the ideal scam prevention system might look like. Interviews followed a semi-structured conversational format that encouraged participants to offer insights even if they did not correspond to specific questions.

While scams are a field of criminology that has been significantly under-studied so far, the findings of the interviews were developed through a review of academic literature, with a focus on international best practice and victim experiences.

Definitions

Research on scams is significantly hampered by uncertainty around definitions of relevant terms such as fraud, scam, and cybercrime. There are a range of definitions used for these terms, which appear to vary in use across borders, potentially because of varying ways that fraud and scams are treated in law.

For simplicity, here, we have used the term ‘scam’ throughout, because it matches the language used in recent government announcements (including the appointment of an anti-scam Minister), and in public education efforts.

When we use the term scam, we refer specifically to any case where a person was tricked or deceived, or their information or documents stolen, in order to obtain money, goods, or services. This matches the approach used by the NZCVS to identify scams,[1] which uses the following questions:

> In the last 12 months, has anyone tricked or deceived you, in order to obtain money, goods or a service?
>
> - Exclude unsuccessful attempts to trick or deceive, such as scam calls or emails where you didn’t respond or supply any information.
> - Include when this happened in person, by telephone or online.
> - Include when you have lost money, goods or a service as a result of somebody tricking or deceiving you

> In the last 12 months, has anyone used or attempted to use, a bank card, credit card, cheque or other document belonging to you, without your permission, in order to obtain money or credit, or to buy goods or services?
>
> - Exclude when this was done innocently, for example by a family/whānau member or friend.
> - Include when the person gained access to your bank or credit card details and used these to buy things, even if they did not steal your actual card.
> - Include when the person took the card, cheque or other document, with a plan to obtain money or credit, or to buy goods or services, but did not actually attempt to obtain anything.

This captures all cases where a person was deliberately tricked in order to extract some sort of gain from them. It does not distinguish between whether the person made a payment directly, or whether they provided their details to an offender who then used those details to steal from them.

[1] The NZCVS refers to this category of offending by the broad term ‘fraud and deception’.

Executive summary

The present and future of scams in New Zealand

- New Zealanders experienced 541,000 instances of 'fraud and deception' in the last NZCVS cycle, making it the most common category of crime.
- Fraud and deception have risen substantially in the last few years, with the proportion of New Zealand adults who have been the victim of fraud and deception offending each year almost doubling from 5.3% to 10.3%. The growth, and overall problem, is now driven by cyber fraud.
- There are a variety of data regarding the amount of money lost to scams each year in New Zealand, but the most useful is provided by the NZCVS, which estimates fraud and deception losses at $397 million.
- Contrary to expectations, scams in New Zealand affect people of all demographics, and is not disproportionately clustered among the elderly. Those who earn over $100,000 are significantly more likely to be victimised than those who do not, however.
- Despite its scale, the issue of scams has not received the government or public attention that is needed. This is particularly noteworthy when compared with other forms of offending.
- Scams can be expected to grow in both volume and sophistication as technologies mature and the process of shifting social and economic activity into the digital realm continues.
- Because they are largely a recent phenomenon, cyber scams have not been well-studied, and there is little empirical evidence regarding best practices for combating it.
- Despite this, there are things New Zealand can and must do. If we act quickly and decisively, the effort itself will act as a deterrent through target hardening.

Recommendations:

- The issue of scams must be recognised as a priority by the state and private sectors.

The reporting system

- Only 11% of scam victimisations are reported to Police.
- Some 60% of scam victimisations are reported to banks, who generally do not pass reports made by customers on to Police.
- For those who do report scams, the process can be confusing and overly complex. There are eight places that scams can be reported in New Zealand, as well as banks, telecommunications companies, and technology companies. While some have unique criteria, many reporting channels also overlap.
- Agencies that take reports do so under the reasoning that there should be 'no wrong door' for those reporting scams. This is admirable in intent, but adds to the confusion of the reporting process.
- Scam reporting is complicated by the fact that many victims do not want to make a full report to Police. Reporting systems need to be designed with this in mind.

Recommendations:

- A single, unified channel that offers a front door for all types of scam reporting is needed.
- A lead agency that is ultimately responsible for scams should be appointed. The logical place for this is Police.
- Acknowledging the particular harms that can be associated with scams, tailored victim support options are needed.

Public education

- New Zealand's anti-scam approach has so far largely relied upon public education.
- A common trope in public education is to give simple advice for recognising scams. This advice does not always match well to the realities reported by victims, however, and reinforces ideas about scams that may actually make people more vulnerable.
- While public education is an important pillar of an effective response, victim narratives reveal there are many scams that simply cannot be prevented this way.
- It has been suggested that private interests see an education-first approach as a way to deflect responsibility for scam prevention onto the consumer and away from the private sector.

Recommendations:

- Public education is important, but must not be relied upon on its own. It should be considered one pillar of approach that also includes effective hardening of financial and communication systems against scams.
- Future public education campaigns should be assessed to ensure that they align with the realities of scams, and do not present a picture of scams or victims that simplifies it into harmful stereotypes.

The private sector

- Scams are a crime that target and exploit vulnerabilities in systems. In New Zealand, the primary systems that it exploits are privately owned.
- New Zealand's consumer protection rules are weak in this area, particularly in relation to tech companies.
- Banks are engaged in significant scam prevention measures, but did not prioritise key elements until the government recently threatened to intervene. There are still weaknesses in key areas.
- Tech companies – and in particular, social media – are widely neglecting their responsibilities in terms of scam prevention.
- Other countries are enacting significant consumer protection measures that show considerable promise.

Establishing an effective response

- Internationally, countries are moving toward anti-scam centres that centralise intelligence collection and analysis. This appears to be the best way forward for New Zealand as well.
- An anti-scam centre must be built around collaboration between the private and public sectors, because both sectors hold important data and expertise.
- Scam prevention is first and foremost an exercise in data analysis, and a key part of an anti-scam centre would be fusing the data and intelligence sources available into a workable whole.
- If our scam protection falls behind that of other countries, we risk being specifically targeted by transnational organised crime.

Recommendations:

- An anti-scam centre that combines reporting, analysis, and public education functions should be established. This should be a physical centre that is designed around collaboration between public and private sectors.

The present and future of scams in New Zealand

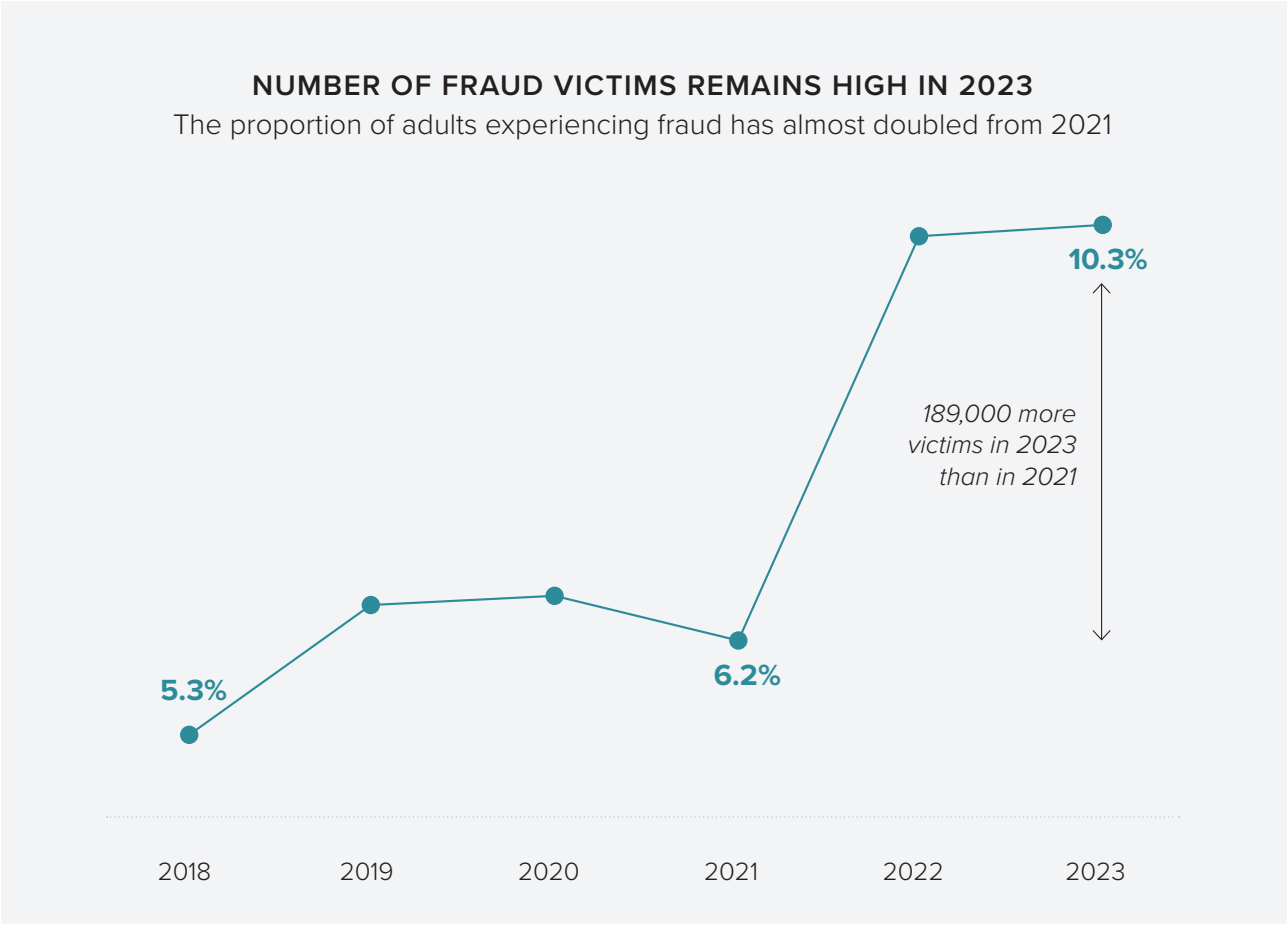
- New Zealanders experienced 541,000 instances of 'fraud and deception' in the last NZCVS cycle, making it the most common category of crime.
- Fraud and deception have risen substantially in the last few years, with the proportion of New Zealand adults who have been the victim of fraud and deception offending within the last year almost doubling from 5.3% to 10.3%. The growth, and overall problem, is now driven by cyber fraud.
- There are a variety of data regarding the amount of money lost to scams each year in New Zealand, but the most useful is provided by the NZCVS, which estimates fraud and deception losses at $397 million.
- Contrary to expectations, scams in New Zealand affect people of all demographics, and is not disproportionately clustered among the elderly. Those who earn over $100,000 are significantly more likely to be victimised than those who do not, however.
- Despite its scale, the issue of scams has not received the government or public attention that is needed. This is particularly noteworthy when compared to other forms of offending.
- Scams can be expected to grow in both volume and sophistication as technologies mature and the process of shifting social and economic activity into the digital realm continues.
- Because they are largely a recent phenomenon, cyber scams have not been well-studied, and there is little empirical evidence regarding best practices for combating it.
- Despite this, there are things New Zealand can and must do. If we act quickly and decisively, the effort itself will act as a deterrent through target hardening.

The scale of scams in New Zealand

The latest cycle of the NZCVS showed that New Zealanders experienced 541,000 instances of 'fraud and deception' within the last year, making it the most common category of crime during that period.[2] For comparison, the next largest category, physical offences (assault and robbery) contained only 255,000 incidents.

NZCVS results show clearly that scams have risen sharply in recent years: since the survey began in 2018, the proportion of New Zealand adults who have been the victim of fraud and deception offending per year has almost doubled from 5.3% to 10.3%, with the largest rise being between 2021 and 2022.

[2] Ministry of Justice (2024). NZCVS Key Stories 2023 (Cycle 6). Results drawn from Cycle 6 of the New Zealand Crime and Victims Survey. Wellington: Ministry of Justice.



This rise mirrors a rise in cyber scams globally, which have been driven in particular by the COVID-19 pandemic, which greatly accelerated the already-ongoing shift of day-to-day societal functions into the online realm.[3] Remote work and social distancing measures saw both individuals and businesses transition to online platforms rapidly and on a large scale,[4] and these changes have largely not reversed after the pandemic ended. Mass adoption of online platforms for everyday activities has provided fraudsters with a range of avenues through which to deceive others, and an unprecedented degree of access to potential victims.[5] [6]

The large majority of the scams that occur in New Zealand is either cyber-enabled or dependent. The most recent NZCVS results show that 86% of frauds occurred "online (including text messages and emails".[7]

The Banking Ombudsman has also recorded an enormous increase in the number of scam cases handled by their office, rising from only two cases in 2014 to 904 in 2024 so far.

---

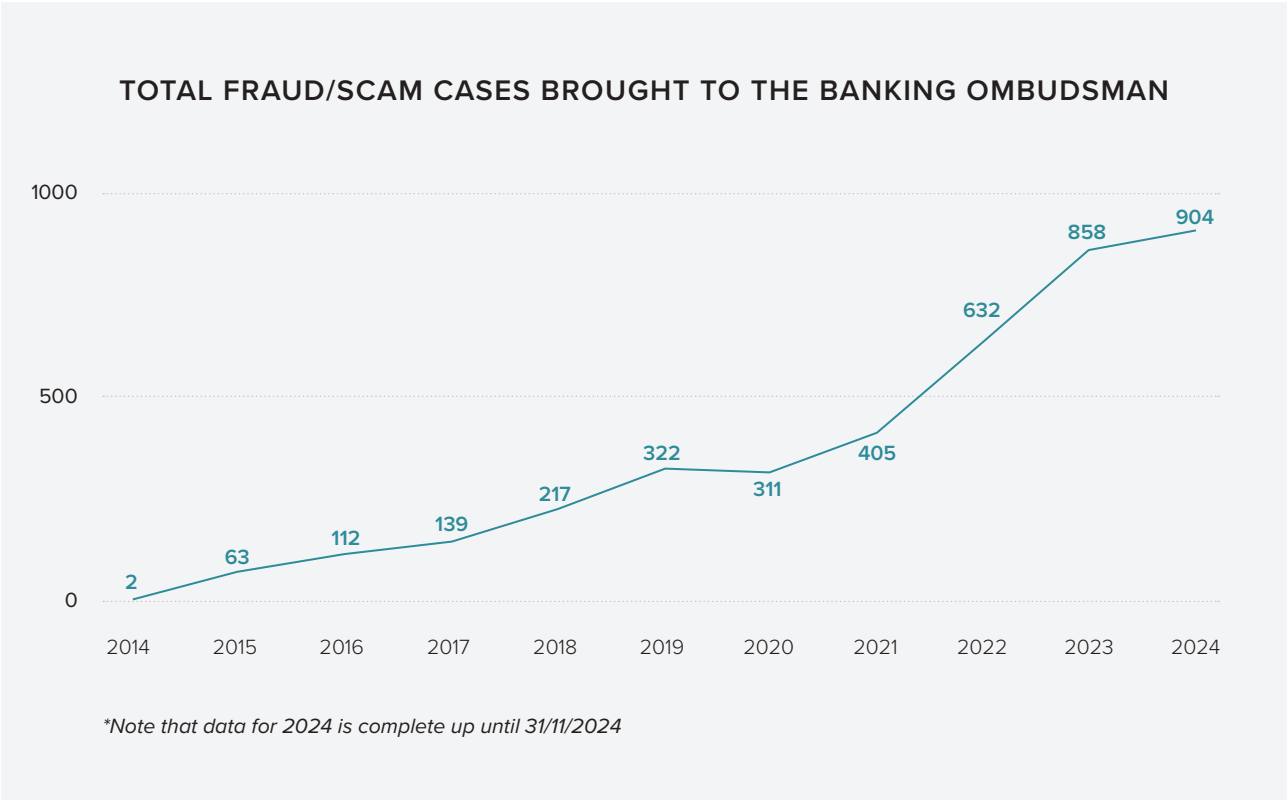
[3] Ma, K. W. F., & McKinnon, T. (2022). COVID-19 and cyber fraud: Emerging threats during the pandemic. *Journal of Financial Crime*, 29(2), 433-446. https://doi.org/10.1108/JFC-01-2021-0016

[4] Whittaker, J. M., & Button, M. (2020). Understanding pet scams: A case study of advance fee and non-delivery fraud using victims' accounts. *Australian & New Zealand Journal of Criminology*, 53(4), 497-514.

[5] Richardson, S. V. A., & Gilmour, N. (2015). Cybercrime and national security: A New Zealand perspective. *The European Review of Organised Crime (EROC)*, 1(1), 51-70.

[6] Cross, C. (2020). Reflections on the reporting of fraud in Australia. *Policing: An International Journal of Police Strategies & Management,* 43(1), 49-61. https://doi.org/10.1108/PIJPSM-08-2019-0134

[7] Ministry of Justice (2024). NZCVS Key Stories 2023 (Cycle 6). Results drawn from Cycle 6 of the New Zealand Crime and Victims Survey. Wellington: Ministry of Justice.



Assessing the amount lost to scams in New Zealand

While it is evidently substantial, the amount of money lost to scams by New Zealanders remains the subject of some dispute.

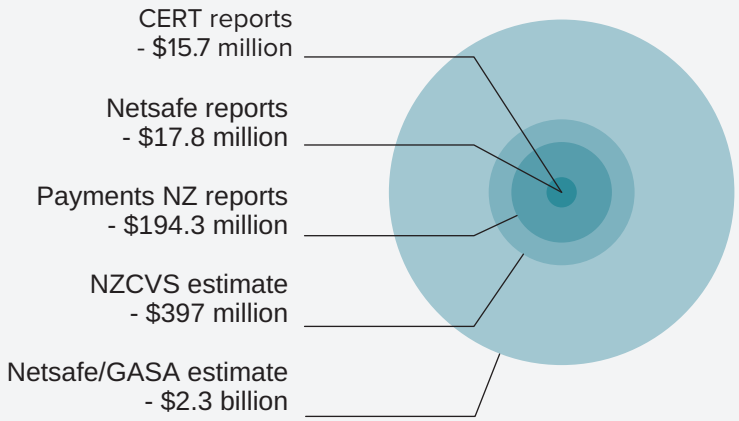
There are two categories of information that are available: numbers derived from scams reported to authorities, and numbers extrapolated from surveys of victims. Numbers of each type are published by a variety of sources.

SOURCE	TYPE OF DATA	LOSSES
CERT[8]	Reports	$15.7 million
Netsafe[9]	Reports	$17.8 million
Payments NZ	Reports	$194.3 million
NZCVS	Extrapolation from representative sample	$397 million
Netsafe/GASA	Extrapolation from non-representative sample	$2.3 billion

[8] CERT NZ (2024). *2023 Report Summary.*

[9] Netsafe (2023). Annual Report 2022/2023.

FRAUD AND SCAM LOSSES: REPORTS AND ESTIMATES



While numbers generated by reports of scams are more certain, the very low reporting rate for scams means that they represent only a portion of actual losses. In the case of CERT and Netsafe, it is also unclear how many reports were made to only one or the other, and how many were duplicated across both. The most useful of these numbers is the $194.3 million figure provided by Payments NZ., which is the payments processing system jointly owned by New Zealand's major banks. This figure represents all of the losses reported to the 11 financial institutions that use Payments NZ, but does not include those reported to companies that do not use Payments NZ, or scams that were not reported to banks, which NZCVS results find to be 40% of cases. Despite representing an incomplete picture of scams, this figure is the one that has been most often cited by government sources describing the recently announced all-of-government anti-scam response.[10]

Extrapolation from victimisation surveys represents a method that, while less concrete, can provide a better overall picture of the problem. This approach takes a sample of the population and asks them directly what types of offending they have experienced within the last 12 months, thereby capturing offending that has gone unreported.

The first of these is the NZCVS, which uses a very large sample (n=7,134 in cycle 6) with a highly robust sampling methodology designed to ensure a representative sample.[11] The question that it uses to code for fraud and deception is well-calibrated to accurately capture the full range of frauds and scams. This appears to offer the clearest picture of scam victimisation in New Zealand. The latest NZCVS cycle found that 10.3% of the adult population has been the victim of scams in the past 12 months, with an average loss of $734 per incident, for a total of $397 million extrapolated across the country. Due to its methodological robustness, this is the estimate of scam losses that can be considered most accurate.

[10] Ministry of Business, Innovation & Employment (2024, December 4). Proposal for an all-of-government approach to address online financial scams.

[11] Ministry of Justice (2024). *NZCVS Methodology Report*. Wellington: Ministry of Justice.

The NZCVS, critically, has recently been evaluated externally.[12] While the evaluation did not look specifically at its assessment of scam numbers, it did find that the NZCVS system overall is well-designed and implemented, and uses best practice survey methodology.

One widely-reported estimate of scams may be unreliable

The outlier among these estimates comes from survey results published by the Global Anti-Scam Alliance (GASA) and Netsafe.[13] This survey asks a sample of the population about their experiences with scams, and extrapolates the results across the country's population. The survey was conducted by GASA, and mirrors an approach that GASA has taken in overseas as well. This estimate has been widely cited in media recently,[14] [15] [16] and was often mentioned by experts working in the sector that we spoke to.

This survey finds that 20% of its sample of 1000 New Zealanders have experienced scams of some sort in the past 12 months, and lost an average loss of $3105. Extrapolated across the population as a whole, this means a loss to scams of $2.3 billion annually, which is 0.6% of the country's GDP.

These extrapolations, which imply a scam problem that is twice as prevalent as that reported by the NZCVS, and many times as costly as any other estimate, do not appear to be methodologically sound, however. While the researchers took a large sample of the population (1071), they do not appear to have taken steps to ensure that this sample is representative. The limited demographic section of the report does show an even mix of men and women, but distributions of age and education level do not appear to match those of the census. Other demographics – most notably ethnicity – are not covered in the report. The demographic profiles presented in reports using the same methodology in other countries are similarly, and in some cases more obviously, non-representative.[17] [18] [19] [20]

No information about how the sample was gained (i.e. how they found people to take the survey) is included in the report and it simply cannot be validated. Given the high prevalence of scam victimisation and loss, it appears likely that the sample was drawn, at least in part, from people who had some form of contact with GASA already. If this is the case, then the data are not suitable for extrapolation in this way, and the $2.3 billion figure cannot be considered valid.

We reached out to GASA with these questions, but have not received a response.

There are elements of this methodology that can still yield useful information. As a survey of scam victims, this methodology is still valid, if not necessarily ideal. It is only the extrapolation across the population as a whole – which is unfortunately the result that has been widely reported – that does not appear to be trustworthy.

---

[12] Solasta Evidence Consulting (2024). Evaluation of the New Zealand Crime and Victims Survey: Final Summary Report.

[13] Global Anti-Scam Alliance (2024). *The State of Scams in New Zealand 2024.* Netsafe and GASA.

[14] The New Zealand Herald (2024). Kiwis lose $2.3b to digital scams, Government readies three big moves.

[15] The Post (2024). Which scam loss number should we believe: $200 million or $2.3 billion?

[16] Radio New Zealand (2024). Revealed: How much money Kiwis have lost to scams this year.

[17] Global Anti-Scam Alliance (2024). *The State of Scams in Australia 2024.* GASA.

[18] Global Anti-Scam Alliance (2024). The State of Scams in the United States of America 2024. GASA.

[19] Global Anti-Scam Alliance (2024). The State of Scams in the United Kingdom 2024. GASA.

[20] Global Anti-Scam Alliance (2024). *The State of Scams in Canada 2024.* GASA.

Scams affect everyone

While widely believed stereotypes characterise scam victims as predominantly elderly, the demographic results of the latest NZCVS paint a significantly different picture, showing a rate of victimisation that is much more evenly spread across demographics than might be expected.

Older New Zealanders do not appear to be disproportionately victimised at all: those 65 and over experienced scams at a rate of 10%, while those aged 30-64 were scammed at a rate of 12% per year. Those 15-29 experienced the lowest rate at 6%. This may be because older people are less likely to use digital technology – something that is already in the process of changing. Younger people, while online more, may be less vulnerable to many scams simply because they have less money to spend.

Scams defy other expectations around victims of crime as well. European New Zealanders are the ethnic group most likely to suffer scams, with 11% of Europeans reporting an experience of scams within the last 12 months. Asian people were the next highest at 10%, and Māori and Pacific Peoples, who in other categories of crime are often the most victimised, were the lowest at 9% and 8% respectively.

Unlike most other crimes, scam victimisation is also weighted toward those with more money. Those earning over $100,000 a year were most likely to suffer scams at 16%, those earning $70,001-$100,000 a year at 11%, and those earning less than $70,000 a year at 9%.

Not only are people with a personal income over $100,000 the most likely to suffer scams, rates of victimisation among that group have risen more than any other group since the first cycle of the NZCVS, leaping from 6% to 16%. This may suggest an increase in fraudsters' ability to construct scams that target those with money to invest, such as investment and cryptocurrency frauds.

Victimisations of Asian people have also risen precipitously, from 2% in 2018 to 8% 2024. One Chinese victim that we spoke to reported a feeling that people of their ethnicity were being specifically targeted by certain types of scams because the community's lower rates of English fluency, and greater vulnerability to scams that leverage anxieties about immigration. This is a subject that may merit future research.

The serious impacts of scams

Scams can have devastating effects on its victims, reaching far beyond mere financial loss. Research has shown that it often leaves individuals feeling violated and distrustful, eroding their confidence in both digital and personal interactions.[21] The emotional toll can be profound, leading to anxiety, stress, and even depression as victims grapple with the betrayal and the daunting process of reclaiming their identity and funds. Moreover, the ripple effects can extend to their families, businesses, and communities, highlighting the critical need for robust protections and support systems to prevent and address scam comprehensively. The microeconomic harms created by scams can, therefore, have wider negative impacts on the economy as a whole.

We spoke to a number of investment scam victims who had lost amounts over $100,000 to fraudulent investment schemes. In all cases, the money lost was most or all of their life savings, which was particularly crippling for those who were at or nearing retirement.

An outcome that many victims did not expect was the judgement that was attached to being taken in by a scam. This was despite very few of the victims we spoke to having fallen victim to scams that

[21] Button, M., Lewis, C. & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal* 27 36–54.

they might reasonably have foreseen or prevented. One reported that the spiral of shame and guilt brought on by the scam led them to lose their business.

This culture of shaming significantly exacerbates the harm of scams, and can lead to scams not being reported, and to victims choosing not to seek help.

> [I have dealt with victims] who didn't tell anyone because they were completely shamed and embarrassed that they had fallen for the scam. This happens a lot, which means that they're not supported… And then that leads to them kind of withdrawing from their life.
> *Victim advocate*

Another important consequence of many cyber scams is fear and loss of confidence. Several victims we spoke to reported that they found themselves afraid to use technology again because they were not sure if they could avoid being scammed again.

> I'm afraid to touch anything on my phone or tablet now, in case I do something wrong again.
> *Victim*

Experts we spoke to described this as a common but unmeasured outcome of scams.

> I've got people who are victims of this type of crime where they now can't bank online… they've got nothing on their devices. [They've become very] financially insecure. I think people underestimate how once you have been a victim of something so invasive, it's very difficult for you to then trust those systems and those processes again.
> *Victim advocate*

This has been identified in research as well: BNZ's 2024 scam survey found that one in four New Zealanders over the age of 65 are hesitant to go online due to fear of scams.[22]

This represents a significant handicap in the modern world: electronic devices and the internet are fundamental parts of how we engage with the world, and are required for everything from managing money to connecting with friends and family. As the number of victims grows, the impact of this digital anxiety on the country's economy and productivity will grow as well.

Scams have not been taken seriously

Despite affecting one in every ten New Zealanders each year, scams have largely been ignored until very recently and is still not receiving the attention it requires.

As will be discussed in the next section of this report, no government agency is fully responsible for combating scams, and fraud offending has been found to be treated essentially as an afterthought by Police.[23]

While there have been some calls for change, it was only in late 2024 (shortly before the completion of this report) that the government announced its intention to coordinate a multi-agency response to scams, which will seek to increase agency and regional collaboration under the leadership of a newly created position of anti-scam Minister.[24] The specifics of how this will be achieved have yet to be decided.

---

[22] BNZ (2024). A quarter of older NZers fear going online due to scam concerns.

[23] Independent Police Conduct Authority (2022). *Review of Police management of fraud allegations.* Government: IPCA.

[24] Bayly, A. (2024). *Better coordination of anti-scam efforts*. Wellington: Beehive.co.nz.

Private companies whose systems are targeted by fraudsters have developed scam prevention systems, and often employ dedicated scam protection teams, but these efforts are piecemeal, and have not been well supported by government, despite their relevance to law enforcement. Work in this regard has varied considerably between sectors, and in some areas has been deeply lacking. New Zealand's scam protection has been allowed to become almost entirely reliant on the private sector, despite their efforts having been developed with little government coordination or direction.

This lack of interest has not been because scams are a new issue, or because their significance was unknown. Scams have been known to be occurring in their hundreds of thousands for at least as long as the NZCVS has been running - its first iteration in 2018 recorded 273,000 instances, and the upward trajectory of victimisation has been apparent since then.

A key reason behind this lack of focus is the perception that fraud and scams are dominated by small offences with limited losses. While it is true, however, that many individual scams result in relatively small losses, many are also in the tens or even hundreds of thousands of dollars, and are personally devastating for victims. Even the average amount lost ($734 according to the NZCVS) can have a significant financial impact for many people. Moreover, because of the sheer scale of the problem, it means that the overall cost of scams to victims, and to the country's economy in general, is nevertheless substantial.

To provide context for the degree to which scams have been ignored, an important contemporary comparison can be found in the example of 'ram raids' – a form of burglary where a vehicle is used to smash through the wall or door of a closed shop. This crime came to the forefront of public attention in 2022, when a small[25] but highly visible increase in ram raid offending became apparent. Despite numbering only a few hundred offences a year (433 at their peak),[26] ram raids became the subject of debate in media and parliament, and resulted in both the proposal of new legislation (the Ram Raid Offending and Related Measures Amendment Bill 2023), apportionments from the Proceeds of Crimes Fund for preventative measures, and considerable behind-the-scenes work in justice agencies.

A number of the victims that we spoke to made the comparison between how the government has responded to ram raids and how it has dealt with scams, feeling that retail crime has been firmly prioritised and scams rather ignored.

No official figures were ever published on the amount lost to victims through ram raids, but it cannot be doubted that scams, which occur at annual rates around a thousand times higher, generate much greater loss and general harm. There is good reason to believe that scams result in greater harm for every dollar lost as well. Where money and goods lost to burglary largely remain in New Zealand, and continue to be part of the economy – for example, cash stolen in a robbery is likely to be spent on goods and services within New Zealand – money stolen by scammers is highly likely to be sent overseas and therefore lost to the New Zealand economy. The impact on individual victims may also be greater: retail crime victims are likely (or at least able to be) insured, although costs are high.[27] No insurance or protection schemes for many types of scams exist, save for the efforts of banks to recover lost funds, which are rarely successful,[28] and for reimbursement policies that cover only unauthorised fraud.

---

[25] New Zealand Police (2022). *Scanning report: Ram Raids* NIC / SR / 22-01-26. New Zealand Police.

[26] Radio New Zealand (2024). Ram raids down 80 percent compared with same time last year.

[27] Radio New Zealand (2023). Keeping business alive 'may not be possible' as ram raids hike up insurance.

[28] Global Anti-Scam Alliance (2024). *The State of Scams in New Zealand 2024*. Netsafe and GASA.

Ram raids appear to have declined substantially in 2024, with analysis in June finding that rates of offending are down 80% from the year before.[29] Undoubtedly targeted policing and the efforts to install prevention measures have aided in this, but it also appears clear that the crime itself, which showed every outward sign of being an internet-driven fad among a small number of young offenders, simply became less popular.

The reasons for the vastly contrasting responses to these two types of crime likely come down to narrative: where ram raids present a clearly sympathetic victim and the familiar trope of wild young criminals that need to be restrained, scams are an issue that cannot be so easily rendered in black and white. There is a common perception, however wrong it may be, that scam victims are defrauded because they fell victim to their own incompetence or greed, and the offenders, who largely reside overseas, are not easily understood or imagined.

This is something that must be overcome, however, because the current boom in cyber scams cannot be expected to recede as quickly as ram raids did.

Cyber scams will grow in volume and sophistication

Cyber scams has grown dramatically in recent years, and can be expected to continue to grow in the future as new technologies are integrated into existing scam methodologies.

A key vector repeatedly highlighted by experts in the area is Artificial Intelligence (AI) technology. AI tools designed for legitimate use have improved vastly in sophistication and capability in the last few years, and have now reached the point where they are able to aid and imitate the work of humans remarkably effectively. These same technologies are rapidly being co-opted for illicit applications as well.

As an example, AI technologies can be deployed on an individual basis to increase the believability of some scams through methods such cloning (or 'deepfaking') of voices and likenesses. Examples of this include using the appearance of public figures or real investment professionals in order to lend credibility to an investment scam, or copying the voice of a person's family member to solicit funds using a fake emergency. These technologies can be deployed in real time conversations, and have reached a level where they are likely to be very difficult to detect by a person who is not already suspicious and well-versed in what to look for. Scammers are already using these tools, however, they do not yet appear to be regularly used against New Zealanders.

AI technology can also be used to facilitate the delivery of mass scam approaches by automatically tailoring scam messages to suit information that is known about a list of targets. Where previously a scammer sending a mass scam message would have to create a message that was applicable to the broadest possible range of potential victims, AI tools can be used to gather publicly available data about potential victims, and to craft an approach – such as a phishing message – that appears more genuine, for example by imitating a company that they are known to have an account with. Beyond this, it is also possible for AI tools to automate scams by using a chatbot, either via text or

[29] Radio New Zealand (2024). Ram raids down 80 percent compared with same time last year.

[30] Richet, J.L. (2022). How cybercriminal communities grow and change: An investigation of ad-fraud communities. *Technological Forecasting and Social Change*: 174.

[31] Jung, B. R., Choi, K. & Lee, C. S. (2022). Dynamics of Dark Web Financial Marketplaces: An Exploratory Study of Underground Fraud and Scam Business. *International Journal of Cybersecurity Intelligence & Cybercrime*: 5(2), 4-24.

using a simulated human voice. While current voice simulation technology is unlikely to be convincing – particularly in an extended conversation – technology in this area is rapidly advancing, and this cannot be expected to remain the case.

These technologies are developed and distributed between fraudsters through communities on the 'dark web' – the portion of the internet that is obscured from search engines.[30] [31] Anti-scam experts that we spoke to were concerned that the levels of collaboration and information sharing within this community could outstrip that of those working to prevent scams.

> But [fraudsters are] constantly developing, they're sharing intel the same way that we're sharing intel [through] the dark web. They've got all these secure communication channels, and they can share techniques and things at the same speed we can as well... they're able to propagate their new trends faster as well.

AI technology notably has considerable value in scam prevention as well, in areas that potentially include enhanced scam detection measures, allowing Police to better triage scam incidents, and targeting potential victims for education measures. The value of AI tools in these areas is as yet unknown, but is undoubtedly being tested already in other jurisdictions. AI technology is the subject of enormous commercial investment, and is improving rapidly, meaning tools that were ineffective even a year ago may now be substantially more capable. It remains unclear whether AI will ultimately provide a greater benefit to fraudsters or scam prevention efforts: while anti-scam work is likely to be better resourced, fraudsters have the advantage of being able to deploy new tools more rapidly, and without extensive testing.

Anti-scam approaches remain largely untested

While we can – and should – look to other countries for examples of what to do and what to avoid, it is important to acknowledge that the contemporary growth in cyber scam offending is very recent, and not something that can be closely matched to any historical patterns of crime. The field of cyber scam criminology has, as a result, only begun to develop, and is doing so only slowly. Scams are a crime that has traditionally been ignored in research, much as it has in policing, for reasons that include its lack of appeal relative to other offending (many experts described it as an "unsexy" crime), and its variable and sometimes confusing definition as an umbrella term that covers many different methods of defrauding people. More recently, the practical difficulty inherent in understanding, solving, and prosecuting crimes that are rarely reported, and which often occur across borders, has also been a significant contributor. It has been in this absence of attention that an epidemic of cyber scams has been able to spring itself upon New Zealand, and the world, seemingly out of nowhere.

There are significant elements of the cyber scam problem, both internationally and in New Zealand specifically, that are not fully understood, and about which we are currently forced to rely on assumptions and the anecdotal experience of those working in the area. These include:

- What proportion of scams is committed by domestic offenders, and what proportion belongs to transnational offenders?
- If a significant portion of scams is being committed or enabled by domestic offenders, what is the profile of those offenders?

---

[32] Prenzler, T. (2020), "What works in fraud prevention: a review of real-world intervention projects", *Journal of Criminological Research, Policy and Practice,* 6 (1), 83-96.

- How much of the money that is lost to scams is sent overseas, and therefore lost to the New Zealand economy?
- How does the economic impact of scams compare with other types of crime?
- What prevention and policing measures actually reduce scams?

The most important of these questions is the final one. Because the crime itself is new, and efforts to combat it are largely in their infancy, we simply do not know for certain what works to reduce scams.[32]

Dr David Buil-Gil, a quantitative criminology researcher who studies cyber fraud, describes cyber scam research as a field that is only just emerging, and where the evidence required to establish a clear idea of what works is simply not yet available.

> I think that one of the conclusions of any review on the topic is we know very little. There's some research that has been done around different countries, but at the best we can call it soft evidence. There's very little hard scientific research and literature examining what works in prevention and what works in detection.
> *David Buil-Gil, University of Manchester*

Key to this is evaluating the efforts that are being set up now. Robust evaluation measures are a critical part of any novel approach to crime prevention because they allow us to measure whether the approach is working, identify the elements that are performing well and those that are not, and to more efficiently prioritise spending on future initiatives.

Systems of evaluation must be built into an approach during its design phase, with clear metrics by which to judge the success of its goal. Evaluations done after a programme has already begun operating are less efficient, and can struggle to establish a clear picture of success or failure when establishing measures retroactively.

Acknowledging the lack of empirical evidence for best practice, there may be a temptation to delay action, and to await further examples from overseas. It is important that this is avoided.

Scammers are growing in sophistication and capability, and if New Zealand's defences are allowed to stagnate – and therefore to decline relative to those countries that are taking action – we will become a target.

With that in mind, what we can do is look to the methods that are being developed overseas, and assess them in light of the strengths and weaknesses of our own current regime.

The reporting system is broken

- Only 11% of scam victimisations are reported to Police.
- Some 60% of scam victimisations are reported to banks, who generally do not pass reports made by customers on to Police.
- For those who do report scams, the process can be confusing and overly complex. There are eight places that scams can be reported in New Zealand, as well as banks, telecommunications companies, and technology companies. While some have unique criteria, many reporting channels also overlap.
- Agencies that take reports do so under the reasoning that there should be 'no wrong door' for those reporting scams. This is admirable in intent, but adds to the confusion of the reporting process.
- Scam reporting is complicated by the fact that many victims do not want to make a full report to Police. Reporting systems need to be designed with this in mind.

Recommendations:

- A single, unified channel that offers a front door for all types of scams reporting is needed.
- A lead agency that is ultimately responsible for scams should be appointed. The logical place for this is Police.
- Acknowledging the particular harms that can be associated with scams, tailored victim support options are needed.

The underreporting of scams

Despite its impact on New Zealanders, scams are rarely reported to Police. Low reporting of this type of crime has remained consistent throughout all NZCVS cycles, with Cycle 6 finding that only 11% of fraud and deception crimes were reported to Police.[33] This is echoed in research by Netsafe and GASA, who found that only 29% of New Zealanders who were the victim of a scam reported that scam to law enforcement.[34]

The NZCVS finds that most reporting of scams begins and ends with the victim's bank. Some 60% of victims said they reported their scams to their bank, with most reporting to no other authority. Many of the victims that we spoke to assumed that banks would carry their report on to Police, but this is not the case. Banks generally do not pass details of scams reported to them by customers on to any other authorities, primarily because Privacy Act rules prevent them from doing so, and instead simply recommend that the customer make that report themselves.

[33] New Zealand Crime and Victims Survey. (2024). NZCVS key stories 2023 (cycle 6). Ministry of Justice.

[34] Global Anti-Scam Alliance (2024). *The State of Scams in New Zealand 2024*. Netsafe and GASA.

> ...when we talk to them, we recommend that they do take that to Police, but we don't do that on their behalf. That's a privacy issue... There's limitations around what we can and can't do, and sometimes customers don't want that to be mentioned to the Police. I would imagine most banks would encourage the victim to ensure that they are letting the Police know about that and it is appropriately tracked.
> *Bank scam expert*

Data from the NZCVS provides further insight into victims' reasons for not reporting fraud and deception offending to Police. As shown in the graph below, the most significant reasons for not reporting fraud to Police were that it had been reported to other authorities (presumably banks) already, that Police were unlikely to be able to do anything about the scam, and that they had dealt with the matter on their own.

Data from NZCVS cycle 6. Note that participants were able to select more than one answer.

Many of these reasons relate to a general sense that minor scams, and cases where no resolution is likely, are not worth reporting. This represents a problem of messaging and public awareness: while this may be true in terms of recovering funds or seeing the offender punished, it ignores the importance of data in scam prevention. Scam prevention is significantly reliant upon having access to up-to-date information about what scam methodologies are being used, and failure to report minor cases can result in them being allowed to proliferate.

[35] Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology* 21 (2).

While few NZCVS participants selected shame or embarrassment as a direct reason for not reporting, experts that we spoke to regarded shame as a significant broader influence on non-reporting patterns. This is a factor that has been identified in research as well.[35] In this sense, feelings of shame may drive a victim to decide to deal with it on their own, or to conclude that Police are unlikely to be able to do anything.

> ...many people don't disclose because of the shame. And also, you know, it's very whakamā, I guess is the appropriate term there. But also the institutional response also means you're feeling more shame if you do choose to disclose... they say, why did you transfer that money? Why didn't you check it with us first? There's a lot of victim blaming.
> *Victim advocate*

Research found that some scam methodologies – such as romance scams or those involving sex work – may be designed specifically to create shame as a means of isolating their victim and preventing them from going to the authorities.[36]

The reporting process is complex and confusing

There are at least eight government or government-funded agencies and websites that accept reports of fraud and scams in New Zealand. This makes for a needlessly confusing and user-unfriendly experience for victims that is undoubtedly contributing to low rates of reporting.

Groups and agencies that accept reports of scams in New Zealand include:

- Police
- The Financial Markets Authority (FMA)
- The Serious Fraud Office (SFO)
- The Department of Internal Affairs (DIA)
- The Commerce Commission
- Computer Emergency Response Team (CERT)[37]
- Own Your Online (operated by CERT)[38]

Outside of government, reports can also be made to:

- Netsafe

Where the scam occurred through their systems, it can also be reported to the following types of companies:

- Banks
- Telecommunications companies
- Social media and technology companies

---

[36] Button, M., Nicholls, C. M., Kerr, J., Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, 47(3), 391–408.

[37] CERT was recently folded into the Government Communications Security Bureau's National Cyber Security Centre, but remains a separate brand within that entity.

[38] While Own Your Online is operated by CERT, it is (or at least appears to be) a separate reporting tool from the one on the CERT NZ website.

Some government channels will only accept reports of specific types of scams: the FMA receives reports of investment fraud, the DIA takes reports of scam texts and emails, the Commerce Commission takes reports involving fraudulent business activities, and the SFO takes only the most serious or complex cases of fraud and corruption. Police, CERT, Own Your Online, and Netsafe, however, will all accept reports of almost any report of scam.

Participants of all kinds – both victims and experts – expressed frustration with the variety of avenues for reporting scams in New Zealand, and the lack of clarity as to which one was the 'right' one for victims to go to.

> ...the most common concern, other than [the scam itself], would be that victims just don't know who to talk to about it, where to report it, and certainly how to get any help with it. It's a very fragmented landscape, and it is certainly a very difficult process for the victims to navigate.
> *Victim advocate*

While all of the various reporting avenues available provide valuable services, it is rarely made immediately obvious to victims what each one can do for them, or what they can expect and whether reporting to only one is likely to be sufficient.

This lack of clarity was so significant that members of an association of investment scam victims we spoke to reported that one of the most valuable services that collective could provide was giving new victims a frank and honest roadmap of reporting avenues, along with an explanation of what they could expect to get from each one. This is something that some reporting avenues such as Netsafe and CERT should be able to provide also, but no victims that we spoke to reported receiving this kind of advice from any reporting avenue.

Victims who were eager to see a tangible resolution to their case (primarily those who had lost significant amounts of money) said that they found themselves making reports to all of the agencies and groups listed above, in the hopes that any one of them might prove useful. This creates an excessive burden on those in this position, and was described as a confusing and demoralising process.

> I just I mean, I tried everybody, but I just felt like I was hitting my head against the brick wall with everybody, everything.
> *Victim*

Indeed, even when victims could point to elements of the process that had worked well, their frustration with the confusion and perceived futility of most of their reporting methods left them frustrated with the system overall.

A further issue with the variety of reporting avenues available is that it muddies the data available on how much scams are occurring in New Zealand. As noted earlier, both CERT and Netsafe, for example, regularly publish figures showing data points such as how many reports have been made to them, and how much has been reported lost, but it is impossible to know what proportion of these cases are unique to each reporting system, and how many have been reported to both.

The confusion of the reporting process may be an outward sign of a deeper internal issue in how scams are handled. Victims consistently described a sense that in an environment where many groups and agencies were somewhat responsible for aspects of scams, no group was truly responsible for it at the end of the day.

> I just felt like I was going around in circles. Nobody actually really gave a shit to be honest, they were just like, "Oh, yeah, we've seen this before." It's like, but how is there not anyone doing anything about this?
> *Victim*

Victims also said their reports did not tend to be treated with any urgency, and would often take a while to be addressed, if they were addressed at all. This is despite the importance of quick intervention in many scam cases, where delays may allow the fraudster to create more victims.

Similar issues with the process of reporting of scams have been acknowledged in other jurisdictions as well, including Australia,[39] [40] the UK,[41] [42] [43] and Europe.[44] The issues in these processes are generally consistent across these jurisdictions,[45] although some countries, most notably the UK, have taken steps toward streamlining their scam reporting systems as a result.

Police are poorly equipped to deal with scams

NZCVS data show that Police were alerted in only 11% of scam cases, despite being the agency responsible for investigating the large majority of scams.

There is reason to believe that there are significant issues with the way that Police currently handle scams. A 2022 investigation by the Independent Police Complaints Authority (IPCA) found Police management of fraud reports to be "inadequate" and identified widespread and fundamental institutional failures when it came to dealing with fraud.[46]

The report found that unsatisfactory Police handling of scam cases is the result of four key issues:

- variable and inadequate processes for receiving, categorising and prioritising fraud investigations both between and within districts;
- poor and inconsistent investigation structures and processes;
- a lack of victim focus; and
- inadequate expertise and training.

The investigation found that scams were not taken seriously within Police in general, and was perceived to be of low impact and importance – a belief that is entirely out of step with the devastating impact that scams can have on victims. Those who report scams were found to have considerable variation in experience depending on what part of the country they reported it in, and on who they reported the offending to.

Reflecting this low prioritisation of scams, experts we spoke to in the private sector who were frequently responsible for passing information about suspected fraudsters to Police reported that there was considerable variation in the response across cases. While all of the reports that they sent to Police were in their assessment actionable, some were simply never followed up on, and others would be left for a long time before being addressed, allowing the fraudster to continue operating. It was also

---

[39] Cross, Cassandra. (2019). Reflections on the reporting of fraud in Australia. *Policing: An International Journal,* 43(1), 49–61.

[40] Morgan, A., Dowling, C., Brown, R., Mann, M., Voce, I., Smith, M. (2016). *Evaluation of the Australian Cybercrime Online Reporting Network.* Australian Government: Australian Institute of Criminology.

[41] Levi, M., Doig, A., Gundur, R., Wall, D., Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: themes from UK research. *Crime, Law and Social Change*, 67 (1), 77-96.

[42] Scholes, A. (2018). *The scale and drivers of attrition in reported fraud and cyber crime*. UK Home Office.

[43] Button, M., Whittaker, J. (2021). Exploring the voluntary response to cyber fraud: From vigilantism to responsibilisation. *International Journal of Law*, Crime, and Justice 66.

[44] Kemp, S., Miró-Llinares, F. & Moneva, A. (2020). The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research* 26, 293–312.

[45] Cross, Cassandra. (2019). Reflections on the reporting of fraud in Australia. *Policing: An International Journal*, 43(1), 49–61.

[46] Independent Police Conduct Authority (2022). *Review of Police management of fraud allegations.* Government: IPCA.

reported that having personal contacts within Police was the only truly reliable way to be certain that a report of fraud would be prioritised, and therefore addressed.

> A lot of the time, if you know somebody and you have a connection, and you can get in front of the right person. Then you know, [the response] can be a lot more effective or efficient. But not everybody has those sorts of connections, you know?
> *Telecommunications company fraud expert*

One important feature that the IPCA report discussed, and which was confirmed by experts that we spoke to, is that new Police recruits were not given any specific training in how to deal with fraud, and as a result many officers are unaware of how to investigate fraud cases, or how to escalate reports to international authorities when the fraudster is outside of New Zealand.

The report also found that Police often ask scam victims to do their own evidence-gathering and analysis, a practice that "does not occur with any other type of crime". This was echoed by two victims of high-value investment scams that we spoke to, who reported that they had to hire private investigators to track the people who had defrauded them.

> [The fraudster] continued to do it till I got a private investigator, and we interviewed him for 45 minutes... I gave [the video] to Police. So every week I was giving more and more evidence to Police. It still took them seven months to take him down.
> *Victim*

There is a widespread perception among victims and those working in the area that Police simply do not have the resources or manpower to properly deal with scams.

> I mean, we know they are under resourced. They've got problems.
> *Victim*

Police staff that we spoke to pushed back on this, however, and suggested instead that the primary issue was a general lack of awareness among Police staff of how to deal with scams, which led to fraud cases falling to the bottom of officers' list of priorities. This is mirrored in the IPCA report's findings, which highlight organisational and cultural issues that lead to low prioritisation of scams – and therefore poor resourcing – rather than simply an overall lack of funds and people.

The report found that "it is clear to us that Police need a fundamental overhaul of their processes for recording and investigating fraud". No such overhaul has occurred, but in the two years since its publication work has been undertaken within Police, some changes have been made, including ongoing efforts to provide officers with relevant training. A more extensive programme of changes was planned, but was deprioritised after the change of government in 2023.

No right door

Among reporting agencies there was a consistent feeling that there should be 'no wrong door' for those needing to report a scam, meaning that they could come to any agency (sometimes including some that do not have a formal role in reporting scams at all) to make their report, and that the information they provide could then be passed on to other relevant agencies as needed, thereby ameliorating the issue of multiple reporting avenues. Based on the accounts of victims, however, this does not appear to occur reliably. This is unsurprising: there is no combined system for registering scam cases with all of the relevant agencies, or for passing case notes between them.

Information sharing between government agencies can often be difficult. Because different agencies use different computer and data storage systems and do not always have the ability to proactively

share information covered by the Privacy Act, sharing of information generally has to be done manually, one agency at a time, sometimes person-to person, or by using public-facing reporting tools. This is an issue that is widely reported across all types of crime prevention, but is especially pronounced here because of the number of agencies involved. Exactly how the Privacy Act applies, and what types of measures might be considered to enable better information sharing, are issues that are best addressed by legal scholars.

Some working in the area noted that this system is one that is often dependent on relationships between individuals within agencies, rather than operating through standardised channels. While all described good relationships with the relevant people, and a shared desire to achieve the best possible results for victims, this leaves room for inconsistency across cases.

One potential issue with a 'no wrong door' system also is that victims have no way of knowing if their case has really been passed on to other agencies or not, leading to further erosions in confidence. When many reports of scams go nowhere, a victim who does not receive any further contact from other agencies cannot be sure that their case has indeed been referred, or if the person they have dealt with simply forgot. This was described by several victims we spoke to, and needlessly creates uncertainty and mistrust of the system among those who deal with it.

Notably, information sharing is something that New Zealand government agencies should be well-placed to do effectively, when compared with their international counterparts. New Zealand has a small population, a relatively small number of agencies (in many countries there are tens or even hundreds of separate police forces, for example), and does not have the issue of friction or competition between agencies that is often present elsewhere.

Some victims do not want to make a full report

Some victims that we spoke to were not interested in making a full report to authorities. This appears to represent a large portion of those who suffer scams, particularly those who lose smaller amounts of money. Given the data-driven nature of scam prevention, however, encouraging minor reports is important, so any changes to the reporting system must be designed with this in mind.

As noted earlier, many of the reasons given by NZCVS participants for choosing to not report scams are related to a feeling that reporting is unlikely to be worthwhile, both because a resolution is unlikely, and because the process is expected to be too arduous for a complaint perceived as minor. Victims that we spoke to who were in this position said that an online reporting tool – such as those offered by CERT, Netsafe, and Own Your Online – would have been a good option for them, as long as it was simple and straightforward, had they felt that there was a benefit to reporting. This highlights a key concern: to achieve higher rates of reporting, victims must be convinced that there is a reason for reporting scams that goes beyond the resolution of their own case.

Another contributing factor in this is shame: because victims often feel that they are at fault for falling for a scam, going through a reporting process that likely involves speaking to another person and going through what happened in detail can feel like an unwelcome proposition, especially if the case is one that they feel is unlikely to be meaningfully resolved. Again, online reporting tools are important here. Another promising approach that Netsafe has been trialling for this is to its AI chatbot Kora to take scam reports. This is an approach that has been utilised by governments and NGOs internationally as well.[47]

[47] USAgov. (2019). *Breaking into Artificial Intelligence: Meet Our USAGov ChatBot!*

Recommendations

Lead agency needed

An immediate response needed is the appointment of a 'lead agency' to deal with scams in the first instance, and to be ultimately responsible for scam cases to ensure that they do not 'fall through the cracks'.

As noted earlier, there is a widespread feeling that many scam cases are not addressed properly because the wide range of players involved in the area means that nobody is truly responsible for any given case. A logical solution to this is to ensure that there is a lead agency on whom this responsibility rests. There is also a need for leadership within this space in general.

> We have aggressive adversaries, and we have a disjointed, haphazard, piecemeal approach to protecting our citizenry from the threat.
> *Jon Duffy, Consumer NZ CEO*

As the primary responsibility for investigating most cases of fraud, and the one with the greatest resourcing and number of personnel available, the most logical agency in this case would appear to be Police. That the Police should be the lead agency for developing a combined response to scams was also a conclusion of the 2022 IPCA report into fraud.[48] Given that the findings of that report identified important deficiencies in Police handling of scams, however, this would need to come with a significant redevelopment and improvement of their scam reporting approach.

Unified reporting channel needed

There is a clear need for the confusing and impractical multi-channel reporting system currently in use to be replaced with a single channel for reporting scams. The current system is confusing for victims, and exacerbates issues of poor data collection and lack of responsibility. If a single agency is responsible for taking all initial reports, and for passing the report on to other agencies as relevant, these major issues can be considerably reduced. Once this single front door is decided upon, all other reporting avenues must be closed.

The best way to approach this is through the creation of a separate fraud-only reporting channel. This approach is used in the UK, where scams – whether successful or simply attempted – can be reported to Action Fraud.[49] Action Fraud is operated by the City of London Police, which is the UK's national policing lead for economic crime. This platform accepts reports of fraud and scams at all levels, ranging from simple email spam scams through to serious fraud. A similar service, ACORN,[50] takes reports of cybercrimes (including scams) in Australia.

A channel of this nature would likely work best when operated by Police, given that the majority of reports would go directly to them, and that we recommend they are made the lead agency for dealing with scams overall. This may also serve to counter the issue of reporting of crimes outside of scope, which is a concern that has been raised in similar services overseas,[51] which could simply be referred to the correct place internally within Police.

---

[48] Independent Police Conduct Authority (2022). *Review of Police management of fraud allegations*. Government: IPCA.

[49] https://www.actionfraud.police.uk/

[50] https://www.cyber.gov.au/report-and-recover/report

[51] Cross, Cassandra. (2019). Reflections on the reporting of fraud in Australia. Policing: An International Journal, 43(1), 49–61. doi:10.1108/pijpsm-08-2019-0134

Having the reporting channel notionally separate from Police (i.e. operating under different branding, as Action Fraud does) may encourage reports by those who are currently uncomfortable making reports to Police because of feelings that their report is too minor, or concerns that they are wasting Police resources.

While it is preferable for all reports to come through a single 'front door', it may be worth offering a variety of ways of making reports within that service, such as by providing a telephone number, an online form, and potentially a chatbot service, as is currently available through platforms like CERT and Netsafe. This allows for maximum accessibility, as well as making it easier for those who are uncomfortable reporting to a person directly.

We note that some government experts noted that considerable work has already been done toward establishing a single reporting channel within CERT, but that this work appears to have been shelved as CERT has been moved to reside within the GCSB.

Victim support needed

As noted earlier, the effects of scam victimisation on an individual can be considerable and long-lasting, but this is not currently addressed as part of the reporting process.

The 2022 IPCA report into fraud also concluded that support for victims of scams needed to be enhanced.[52]

One option for minimising these harms is the provision of financial grants for victims. In New Zealand, victims of serious crimes can currently receive grants and funding through the Victim Assistance Scheme (VAS) to allow them to remedy the immediate harms of the crime and its investigation, as well as to receive counselling support. These are made available immediately after the offending, without waiting for an offence to be proven in court. It may be worthwhile to consider offering tailored options through the VAS scheme to the victims of scams. Given the volume of scam victims in New Zealand, selective eligibility criteria – such as those suffering significant loss – will need to be considered.

Counselling support may be particularly valuable. As noted earlier, some victims of scams can be affected in lasting ways that include feelings of shame, guilt, and fear of being victimised again. In extreme cases, this can lead to a degree of withdrawal from society, and economic impacts that go beyond those of the scam itself. Offering counselling support tailored to victims struggling with these feelings may be a useful way to prevent these feelings from developing in ways that produce long-lasting – and more costly – outcomes.

A key area for possible funding that applies to some scam cases is the provision of malware removal services. While most scams will not involve the installation of malware on a victim's phones or computers, some do, and victims may be afraid to use their devices when they are unsure if others may still have access to them, significantly limiting their ability to participate in society. Cleaning a computer or mobile phone of malware is a commonly available service that can cost around $100-200, but potentially offers substantial benefits in terms of enabling victims to confidently return to participating in society and economic activity.

[52] Independent Police Conduct Authority (2022). *Review of Police management of fraud allegations.* Government: IPCA.

Public education

- New Zealand's anti-scam approach has so far largely relied upon public education.
- A common trope in public education is to give simple advice for recognising scams. This advice does not always match well to the realities of scams reported by victims, however, and reinforces ideas about scams that may actually make people more vulnerable.
- While public education is an important pillar of an effective scam response, victim narratives reveal there are many frauds that simply cannot be prevented this way.
- It has been widely suggested that private interests see an education-first approach as a way to deflect responsibility for scam prevention onto the consumer.

Recommendations:

- Public education is important, but must not be relied upon on its own. It should be considered one pillar of approach that also includes effective hardening of financial and communication systems against scams.
- Future public education campaigns should be assessed to ensure that they align with the realities of scams, and do not present a picture of scams or victims that simplifies it into harmful stereotypes.

Crime is commonly controlled by attempting to modify the behaviour of criminals. In the case of fraud, where the offender is separated from us by distance and digital anonymity, this is often impossible. We have largely turned, instead, to attempting to control scams by modifying the behaviour of victims through public education campaigns.

Raising public awareness of scam methodologies is an important part of hardening the country's defences. It is important to recognise the limitations of the approach, however, and carefully consider whether all of the messages that have often been the focus of these campaigns are necessarily helpful or responsible.

Public education campaigns

In New Zealand, scam prevention advertising focuses on educating the public about common scams and how to avoid them. Campaigns are run by various organisations, including the government, consumer protection agencies, banks, and telecommunications companies. These ads emphasise the importance of being vigilant, verifying unexpected contacts, and using security measures like two-factor authentication. These are conducted through media of all kinds. Outside of advertising, articles about fraud and scams often appear in the media, and are frequently concluded with a list of basic warnings about how to recognise scam attempts. Anti-scam messaging reaches its peak in Fraud Awareness Week every year, during which a wide variety of groups release messages relating to scams.

These education campaigns appear to be reaching the large majority of the public: a recent survey by BNZ found that 96% of New Zealanders over 65 reported seeing scam awareness messaging recently.[53]

Experts we spoke to universally agreed that public education is an important part of defending against scams, when it is delivered well, but can only ever be one part of a combined strategy that also needs to include effective prevention and policing measures.

Simple tricks for scam prevention may not be helpful

While the majority of scam education work occurring in New Zealand is good, there have been aspects of public education efforts so far that fail to reflect the realities of scams, and that perpetuate unhelpful attitudes about who victims are and how they become victims.

The most prominent example of this is the often-repeated truism that "if it's too good to be true, it probably is" – a phrase we have seen widely used as part of advertising campaigns, Fraud Awareness Month press releases, and as part of the standard package of scam prevention advice added to media articles on the topic.

This advice aligns with ideas of widely known and famously crude scam methodologies like the 'Nigerian prince' emails that were common in the past, but does not reflect most modern scams in any meaningful way. No scam victim that we spoke to reported being ensnared by an offer that could reasonably be called 'too good to be true' – even those who lost large amounts of money to investment scams reported that the fraudulent company they invested with was offering rates only very slightly better than those offered by legitimate companies. There may be some cases where deals that are 'too good to be true' are relevant, such as online product scams, but these represent only a subset of scams, and any advice targeted specifically at them needs to be labelled as such.

This condescending advice perpetuates an image of scam victims as greedy fools who deserve to lose their money. This type of implicit victim blaming was widely identified as an issue by both experts and victims as something that needlessly increased the suffering of victims, and ultimately undermined the goal of scam prevention.[54] [55]

Victims described feeling shamed and alienated seeing their experience so frequently mischaracterised this way.

> No one wants to listen to us. It's blaming. They keep on blaming victims and shaming us.
> *Victim*

This serves only to increase the feelings of shame that are an important driver of poor reporting rates.[56]

By presenting an overly simplistic image of what a scam might look like, this type of messaging suggests that scam attempts, when they do occur, will be easy to identify. This has the effect of reducing vigilance and unduly increasing confidence – ultimately achieving the exact opposite of what was intended. Similarly, other anti-scam public education messaging also often focuses on not making elementary mistakes such as giving out passwords or allowing someone to take remote control of their device – something that no victims we spoke to reported doing.

---

[54] Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology* 21 (2).

[55] Nataraj-Hansen, S. (2024). 'Should've known better': Using Lerner's Belief in a Just World to understand how the Fraud Justice Network observe victims of online romance and investment frauds. *International Review of Victimology*, 30(1), 192-215.

[56] Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology* 21 (2).

> It wasn't too good to be true. I had no pressure on me. It wasn't a cold call. You know, all those things that people assume you have to have done [to get scammed]. I didn't give out any passwords, or any you know, data that I shouldn't. We all feel frustrated by [that sort of messaging]. I just look at them sometimes and shake my head.
> *Victim*

The difficulty here is that these messages are obviously lessons that people do need to learn – if people do not know not to give out their passwords, for example, scammers would exploit that fact – but focusing on the simplest possible advice, and positioning it as the core things that people need to know, is equally problematic.

Better approaches include:

- Offering frequent and up-to-date examples of current scam methodologies, presented without simplistic advice, in order to develop a more nuanced understanding of how scams actually work.
- Focusing on explaining what to do if a person is scammed, and emphasising that it can happen to anyone. Real victim stories may be helpful for this.
- Ensuring that messaging clearly explains what type of scams it applies to.
- Building scam awareness by reminding people why it is important to report scam attempts they encounter. This encourages people to think about scams that they see, and builds anti-scam buy-in among the public.

Although it was widely identified as an issue by scam experts, there remains little research on how best to craft anti-scam messaging to avoid issues of victim blaming. This is something that would be worth further investigation.

Public education campaigns are not a substitute for scam prevention

While some of those better educative approaches are beginning to emerge, they should not distract from other critically important initiatives. Prior to the push that included appointing an anti-scam Minister in late 2024, the government's efforts relating to fraud and scams have largely been focused on public education. The level of public education campaigning being undertaken has noticeably increased in recent years, while actual scam prevention work has languished.

> And they've sort of taken the path of least resistance in a lot of ways, and said, well, the easy option is to teach people how to avoid fraud, rather than improving the systems behind the scenes that might prevent it.
> *Victim advocate*

It is important to recognise that while public education is a pillar of an effective scam response, the system will fail if it is not also supported by effective prevention at the banking and communication technology level, and meaningful policing of offending.

Experts we spoke to emphasised that many scams could not be prevented by better educating the victim, because many scam victims are not in a position to identify that they are being victimised in the first place. As fraud researcher Mark Button explains, victims of complex scams are often fully aware of the signs of fraud, but are unable to see how they apply to their situation, usually because the fraudster has created a relationship of trust with them.

> Lots of victims just think well, "this is a real lover. It's not a fraudster," so no matter what you tell them about romance fraud, as far as they're concerned, that's other people, you know.

> This is their lover, or this is a real investment. There's obviously all those fake ones, but what I've got is a real investment, I'm going to put more money in it.
> *Prof. Mark Button, University of Portsmouth*

Similarly, in cases of simpler fraud such as scam texts, the goal is not necessarily to find a credulous person who does not know how to spot a scam text, but to catch someone at a vulnerable moment when they are too busy, tired, or stressed to think critically. One victim we spoke to, for example, described falling for a scam message after an exhausting day in hospital with a family member. They were not unaware of how to spot a fraud attempt, but were too tired and overwhelmed on that one occasion.

> The reason [spam texts] have success is that if they can get a campaign out, they only need one in a hundred or one in a thousand, or one in ten thousand people to actually fall for it.
> *Telco fraud expert*

In this sense, public education can only ever be part of an effective scam response. While ensuring the public are able to recognise scams reduces the public attack surface, there will always be vulnerabilities that cannot be closed this way.

Does a focus on education serve other interests?

While the experts we spoke to consistently described good quality public education as an essential part of an effective fraud response, there was some concern that it could be deployed in ways that do not align with the public good. As noted earlier, campaigns that focus on how to avoid scams can carry with them implicit characterisations of the victims themselves as being responsible for fraud.

> And that element of things seems quite victim blaming to me as well... everything is about how not to fall for things, rather than how to deal with it when people inevitably do. Because that's just how it works. It's like running a campaign to say to girls, "don't walk around in short skirts."
> *Victim advocate*

It was widely suggested by participants that narratives framing scam victimisation as a personal failure of judgement and care are being promoted by private enterprise as a cynical attempt to avoid being held financially responsible for scams.

Banks and the New Zealand Banking Association (NZBA) were described as a primary driver of this narrative of personal responsibility, suggesting that shifting culpability onto victims – and therefore away from the systems in which the scam occurred – was a strategy designed to head off suggestions that the banks should be required to reimburse scam victims as they do in the UK. While we cannot speak to their intentions, it is notable that this has been a consistent theme in NZBA comments in media, and in their interview with us.

> To hear the Banking Association talk, its victim blaming. It's saying, "Hey, consumers, you need to take responsibility to protect yourselves, using the systems that we put in front of you. We have no responsibility here. It's up to you."
> *Jon Duffy, Consumer NZ CEO*

This was identified by overseas experts as a strategy that had been used by the banking industries in the UK and Australia as well.

As will be seen in the next chapter, conceptualising scams as a matter of personal responsibility ignores the fundamental role of the systems of communication and finance that it takes place in.

The private sector

- Scams are a crime that targets and exploits vulnerabilities in systems. In New Zealand, the primary systems that it exploits are privately-owned companies.
- New Zealand's consumer protection rules are weak in this area, particularly in relation to tech companies.
- Banks are engaged in significant scam prevention measures, but did not prioritise key elements until the government recently threatened to intervene. There are still weaknesses in key areas.
- Tech companies – and in particular, social media – are widely neglecting their responsibilities in terms of scam prevention.
- Other countries are enacting significant consumer protection measures that show considerable promise.

Recommendations:

- To motivate change, companies need to be held more accountable for scams that occur through their systems, via regulatory bodies and codes of practice.
- In return, the government should work to enable and support private sector scam prevention through a combined anti-scam centre.
- Rules requiring identification for the registration of SIM cards are needed.

Technology is the primary enabler of the boom in scams that New Zealand is currently experiencing. Scams often work by exploiting the weaknesses of complex systems, and an increasingly large proportion of modern life is conducted within realms of social, communications and financial technologies that are vulnerable to exploitation. These systems are almost entirely privately-owned, so effective scam prevention efforts must, to varying degrees, recognise, collaborate with, and impose itself upon the private sector.

There are three key industries that have a role to play in the ecosystem of scams in New Zealand. These are banks, telecommunication companies (telcos), and tech companies (including, but not limited to, social media). Companies in all of these three spheres have been engaged in scam prevention efforts of various kinds, with varying degrees of commitment, but these efforts have so far been piecemeal and often in isolation. While some of these efforts have been working, many others are well below the standard that should be considered acceptable.

There is a clear need for the government to provide leadership in this area by setting clear and firm standards for what is expected from each of the industries involved and holding them accountable for failures, as well as working to build systems for collaboration and information sharing that multiply the value of the efforts that are already taking place.

Fraudsters target weaknesses in systems

Scams are very rarely a crime of opportunity. Government and private sector experts we spoke to described the process of planning a cyber scam as one of identifying a vulnerability in a system and working backwards to exploit it for profit.[57] Successful scams may often involve the exploitation of several vulnerabilities in multiple different systems, and be repeated at scale until one of the vulnerabilities is closed. In very real ways, the individual victim themselves is simply a soft element upon which the wider exploitation of the system may turn. Transnational organised crime groups have been increasingly identified as targeting New Zealand institutions this way, using their broad knowledge of international digital systems to recognise gaps in our defences, and potentially re-using approaches that are no longer viable overseas.

In this respect, the most important element of safeguarding New Zealand against scams are to protect the systems – primarily banking, telecommunication, and technology – that can be exploited for profit by fraudsters. In contemporary New Zealand, these systems are all privately-owned, meaning that improvements in this area must be cultivated through consumer protection and public-private partnership.

New Zealand's consumer protections are weak

In terms of scams, New Zealand's consumer protection laws are weak in comparison to those in the countries we might normally compare ourselves to. This applied across all three of the key industries.

> Urgent action is required to establish an effective consumer protection framework that prevents, detects and responds to scams and addresses the harms being done.
> *Nicola Sladden, Banking Ombudsman*

While banks have received the largest share of criticism recently, it must be noted that – largely owing to their longer history as an institution – the banking industry is in fact where consumer protections relating to scams are strongest, although they are still limited. These are determined primarily through the Code of Banking Practice, which is developed and overseen by the NZBA.

Banks and credit cards will refund losses to unauthorised payments – i.e. payments made using stolen credit card details – but generally not for authorised payments, meaning those where a person is tricked into deliberately making a payment themselves.

There are limited cases where banks may be made to refund authorised payment fraud, primarily in cases where the bank has been negligent in some way, such as when it has been warned about a particular fraudster but still allowed payments to go through, or where a bank has failed to recognise an obviously suspicious pattern of payments or other activity. Banks may choose to offer refunds of this type proactively, but many cases are adjudicated through the Banking Ombudsman.

Critics have argued that the criteria for when a bank can be considered negligent are overly narrow, and constructed to the benefit of banks.

The Banking Ombudsman has acknowledged that these criteria no longer reflect society's understanding of what a bank should be doing for its customers, and called for changes to legislation and banks' code of conduct that would allow them to hold banks accountable in a wider range of scam cases.

---

[57] Choo, KK.R., Smith, R.G. (2008). Criminal Exploitation of Online Systems by Organised Crime Groups. *Asian Criminology* 3, 37–59.

Some critics have noted, in particular, that it appears to be more difficult to hold banks accountable for frauds where an authorised payment is made online, suggesting that the general shift toward online banking has had an unintended consequence of eroding consumer protection. This was an assertion that banks and the Banking Ombudsman pushed back on, however.

These protections may be set to change in the near future. In February 2024, Andrew Bayly, the Minister of Commerce and Consumer Affairs, published an open letter to the banking industry recognising the growing issue of fraud and scams, and asking it to update the Code of Banking Practice to provide greater consumer protection, and to investigate a voluntary reimbursement scheme for authorised payment fraud victims.[58] The banks have not yet issued a response on the subject of reimbursement.

The Banking Ombudsman also echoed wider calls for an ecosystem-wide approach that acknowledges the other systems that also contribute to scams, primarily the telecommunications sector and social media platforms.

Telecommunications in New Zealand is guarded by a range of consumer protections, but few have direct applicability to scams. The telecommunications industry is regulated primarily by the Telecommunications Act 2001, which establishes a Telecommunications Commissioner through the Commerce Commission, as well as the Telecommunications Forum (TCF), which is an industry group responsible for enacting policy set by the commissioner through industry codes. One of these codes is the Code for Scam Calling and Scam SMS Prevention, which is a voluntary code that entered use in 2018, and which "formalises a process and minimum standards between industry participants, to identify and block Scam Calling and Scam SMS activity, and to work proactively and collaboratively with the relevant external bodies to mitigate the risks to end users". This code is notably considerably more detailed than the portion of the Code of Banking Practice that governs scams, but does not contain any obligations for telcos to provide redress to victims of scam activity on their networks. The TCF does not have the ability to sanction companies who fail to meet their obligations under this code, but can refer them to the Commerce Commission for enforcement action. What this might look like in practice is unknown, because it has never been tested.

Social media, and tech companies in general, are subject to very little regulation in New Zealand, and much of what does exist was drafted before the advent of the modern internet. This was acknowledged in the DIA's recent Safer Online Services and Media Platforms (SOSMP) review, which found that the current legislation and is no longer fit for purpose, difficult to navigate, and does not protect consumers sufficiently.[59] This review recommended the creation of codes of practice for social media companies, to be enforced by a new industry regulator that is independent from government, in an arrangement similar to that used by the telecommunications industry. Major social media platforms have signed on to the Aotearoa New Zealand Code of Practice for Online Safety and Harms,[60] following the Harmful Digital Communications Act 2015, but this includes no provisions for scams.

Existing anti-scam efforts in the private sector

With limited consumer protections in place, scam protection within these three systems is strongly reliant on the anti-scam efforts conducted by industries, and by individual companies.

---

[58] Hon Andrew Bayly (2024). Strengthening bank processes and consumer protections against scams – Open letter to the New Zealand banking industry.

[59] DIA (2023). *Safer Online Services and Media Platforms.* Government: Department of Internal Affairs.

[60] https://thecode.org.nz/

This section is not an exhaustive list of the anti-scam measures used in each industry, but highlights some key areas of importance.

Banks

The majority of banks' anti-scam efforts can be summarised as data-driven work to flag and map fraudulent activity by analysing information including profiles of customers' payment activity and habits of accessing bank services (such as the devices and locations they normally use). These systems are proprietary to each bank, and largely kept secret for reasons of operational security, so it is difficult to establish whether they have any significant weaknesses.

One significant limitation of this system is that while there is some information sharing between banks, each bank largely has visibility over only its own system, which inhibits their ability to establish patterns of behaviour.

> ...if you think of it as a system with lots of nodes and data moving between those nodes, and that's like the payment system, or the payments infrastructure across any given environment. And then you think of that system from a New Zealand perspective, and then you multiply it multiple times and start to add the international system, you can start to see it gets quite complex quite quickly for each of the banks, what they see is one node of that system, right? So they see what's happening in their environment, but they don't see what's happening necessarily in all the other banks in New Zealand, let alone all the other banks internationally... Technology wise, the challenge exists in visibility of things that are occurring out of your ecosystem.
> *Technology expert, major bank*

In New Zealand, banks established a joint anti-scam centre in late 2023, which aims to better centralise anti-scam efforts through information sharing.

Bank technology experts we spoke to said that while this system is highly effective at detecting unauthorised payment fraud, it struggles considerably with authorised payment fraud. In the case of an unauthorised payment, for example a stolen credit card, patterns of use often diverge visibly from those of the card's legitimate owner, allowing for payments to be quickly flagged as suspicious. In the case of authorised payment fraud, however, because the payments are made by the account's legitimate owner, they do not display any of the signs of anomalous access that they might ordinarily look to as a sign of scams.

Some participants took a more cynical view of the reason for this difference, however, suggesting that it was at least partly because unauthorised payment fraud are an area where the Code of Banking Practice requires banks to reimburse victims in most cases.

> Where [fraud protection is] strong, is 'card not present' fraud because banks are on the hook. So the systems for detecting anomalous card use and alerting on that are excellent.
> *Jon Duffy, Consumer NZ CEO*

Following Minister Bayly's letter in early 2024, New Zealand banks are currently working to institute Confirmation of Payee (COP) systems, which checks the name entered when making a payment online against the details of the recipient account, displaying various warnings if the two do not match. This will make things difficult for fraudsters, who can currently ask victims to make payments to accounts under names that bear no relation to the account they are actually using, allowing them to disguise personal accounts as the accounts of businesses or other entities.

COP is important not only because it will provide a valuable check against scams, but also because the widespread presumption that it already exists is currently enabling scams. Many people presume that because banks ask for details of the payee, those details are checked against the receiving account, but this is not currently the case. We spoke to several victims who said that the assumption that the payee details would be matched gave them a false sense of security that the payments they were tricked into making must be being sent where they had been told.

> ...if that confirmation of payee was in place I wouldn't have been scammed because it wasn't going to [name] it was going to some other guy. I said to them, why are you even asking for the name and the account number if you don't care who it's going to?
> *Victim*

While the measure is unequivocally a good thing, banks have faced significant criticism for not having the system in place already, and for only moving to create one under pressure from the government. This is perhaps instructive of the pressure needed to be put on banks (and others) to go further.

While it must be noted that COP is not as ubiquitous internationally as it is sometimes characterised as being – Australia, for example, is expecting to have its own COP system in operation after New Zealand's, and the USA has shown no indication of an intention to set one up – COP systems have been in place in some (mostly European) countries for a number of years, including the Netherlands since 2017, and the UK since 2020.

Banks have also promised to stop sending text messages to customers containing URL links to websites, because phishing scams can easily imitate these messages but replace the link with a fraudulent one. Progress on this seemingly elementary change has been surprisingly slow, however.

Telcos

Preventing scams through telecommunication systems is primarily related to the detection and blocking of fraudulent text messages and calls.

The most significant component of this is preventing 'spam' texts, where large numbers of people are targeted at random with messages that often imitate a government institution or company. This is accomplished in part by screening for suspicious behaviour, such as multiple text messages with the same content being sent repeatedly from one device.

A key issue identified by telco scam experts is the speed at which potential scams have to be identified, assessed, and blocked from the network. Tools that allow messages and calls to be made en masse, such as 'SIM boxes', which accept a large number of SIM cards at once, have become much more widely available at low cost in recent years, meaning that a scammer can often send thousands of messages in a very short space of time.

Telcos can also block fraudulent URLs from being accessed on their network. As well as those identified through their own spam prevention efforts, telcos receive lists of these URLs from the DIA, and through industry information sharing. One telco scam expert that we spoke to noted that they can sometimes be wary of blocking URLs because of the damage that could be done if they accidentally blocked one used by a legitimate business, and were eager for a system where government could audit blocked URLs, or where the telco's liability in cases where they incorrectly identify a legitimate site as a scam might be reduced.

> It would be really good if it could be overseen by the government... The concern is if we block something on our network, but it's actually legitimate, then what's the risk? There's liability.
> *Telco scam expert*

One notable weakness in the telecommunication industry's scam prevention methods that was identified by experts in government is the general absence of any identity verification mechanisms when registering new SIM cards. Because SIM cards can be bought in bulk, and there are no significant barriers to getting quickly onto the network at present, and returning immediately after a given SIM card is blocked.

> We're having these conversations [with telcos] now, and we're saying, "Hey, we just got 10,000 SIM cards from you, from an offender. We've got 2000 from this one. That's, you know, you guys are part of the problem as well as being part of the solution."
> *Government scam expert*

Tech companies

Experts reported that while banks and telecommunications companies have largely been making a genuine effort to combat the issue of scams through their services, the piece that has thus far been missing is that of technology companies.

Tech companies in this context include social media companies like Meta (Facebook, Instagram, and WhatsApp), Twitter/X, Snapchat, and TikTok, as well as companies with a variety of offerings such as Microsoft, Apple, and Google, and smaller local companies like Trademe. Scams are possible through any service that allows one person to communicate with another; a range that includes an enormous number of companies in this sphere. Because of the sheer quantity of communication that takes place through their systems, however, social media is of particular interest here.

The ways that these companies' systems can be used for scams are many and varied, but the key vectors include messages delivered through messaging services (which may be spam or tailored to the victim), ecommerce scams, websites imitating those of legitimate companies, and fraudulent advertising.

All major tech companies have processes through which fraudsters operating on their platforms can be reported, and presumably removed, and staff working to track and pre-emptively remove fraudulent accounts. The element of concern, however, is whether those processes are actually a match for the problem of scams occurring through these platforms. Many experts we spoke to were of the opinion that for most of the major tech platforms, they are not.

> I think the platforms have a huge degree of culpability in this, because they're actively taking money to promote scams. Their checks and balances are virtually non-existent.
> *Jon Duffy, Consumer NZ CEO*

There are no publicly available evaluations of how effective these reporting tools are, and nor are there likely to be: outside of their own internal processes, tech companies rarely make data on the activity of their platforms available to researchers.

Government experts and others working in the space were broadly of the opinion that most big tech companies, and in particular the social media companies, do not have a culture that is inclined towards genuine engagement with efforts to police the activity on their platforms.

> The platforms don't even engage. They just pretend it's not happening. Don't answer the phone, you know.
> *Jon Duffy, Consumer NZ CEO*

> ...many of the big social media companies, their trust and safety groups have been run down recently. You know, they've lost staff. Like some of them, scam pages that are brought to their attention and they're not removed. So it's one thing to say that you're willing to do something about it, but when in practice, you're not seeing that, then it doesn't have a lot of meaning.
> *Government scam expert*

This is not entirely surprising: there are significant disincentives for social media companies to meaningfully engage with the issue of scams on their platforms. Because they do not charge users any fees, and instead rely on the value of the data that they produce, most tech companies operate on business models that require very large numbers of users engaging with their systems through entirely automated processes to be profitable. Effective scam prevention requires extra processing of data, as well as human reviewers to check flagged content, all of which adds additional costs that threaten to overwhelm a strained system if applied alongside other requirements such as moderating extremism, blocking the distribution of child abuse material, and removing hate speech. This is notably an issue of the business model in question, rather than any criticism of the importance of these tasks.

Since their first boom in the 1990s, multinational tech companies have often enjoyed freedom from regulation, and been able to operate in ways that would not have been possible for a conventional non-tech company operating similar services, both because their novel nature often separates them from existing codes, and because of the widespread view of the internet as a 'place apart', where laws and norms do not necessarily apply. Even as the internet has matured into a ubiquitous part of ordinary life, this belief has persisted: a recent review by the DIA concluded that criminal activity of all kinds is often taken less seriously in the online space, and not seen as being as 'real' as equivalent offending in the 'real world'.[61] Many tech companies have been founded in explicitly laissez faire libertarian ideals that have until relatively recently gone entirely unchallenged, and have found themselves poorly equipped to deal with their now fundamental importance in many of society's everyday functions.

One example of this can be seen in social media platforms' broad failure to properly respond to the rise of far-right extremism on their platforms. While it was abundantly clear in the mid-2010s that social media's systems and algorithms were driving and amplifying far-right radicalisation among a portion of their userbase,[62] [63] social media companies declined to take steps to curb these issues, seemingly because it would be unprofitable to do so.[64] It was only following events like the 2019 Christchurch mosque shootings, which was live-streamed on Facebook, that some limited action began to be taken, but far-right extremism on these platforms remains a significant issue,[65] as does extremism of other kinds.[66] [67]

The tendency among big tech companies is often toward reducing user protections, rather than improving them. A particularly emblematic example, which we explored with victims in this research, can be seen in Facebook's launch of its Marketplace service in 2016. Facebook Marketplace is a

---

[61] DIA (2023). *Safer Online Services and Media Platforms*. Government: Department of Internal Affairs.

[62] Scrivens, R., Amarasingam, A. (2020). Haters Gonna "Like": Exploring Canadian Far-Right Extremism on Facebook. In: Littler, M., Lee, B. (eds) *Digital Extremisms. Palgrave Studies in Cybercrime and Cybersecurity*. Palgrave Macmillan, Cham.

[63] Hutchinson, J., Amarasingam, A., Scrivens, R., & Ballsun-Stanton, B. (2021). Mobilizing extremism online: comparing Australian and Canadian right-wing extremist groups on Facebook. *Behavioral Sciences of Terrorism and Political Aggression*, 15(2), 215–245.

[64] Lauer, D. (2021). Facebook's ethical failures are not accidental; they are part of the business model. *AI Ethics* 1 (4), 395-403.

[65] Marko, K. (2022). Extremist language in anti-COVID-19 conspiracy discourse on Facebook. *Critical Discourse Studies*, 21(1), 92–111.

[66] Sharma, S. (2023). Online Radicalisation: How Social Media Is Promoting Islamist Militancy. *South Asian Survey*, 30(2), 189-209.

[67] Choudhary, P., Mourya, B.R. (2024). The Role of Social Media in Cyber Terrorism: Recruitment, Radicalisation, and Propaganda. *Library Progress International* 44(3), 22991-22997.

peer-to-peer ecommerce platform that allows users to sell goods to one another in a style similar to Trademe or eBay. Critically, Facebook Marketplace has chosen not to include key features that allow users to judge the trustworthiness of buyers or sellers such as public transaction histories and positive and negative feedback, relying instead on Facebook's existing social media profile system, and its much more opaque processes of user verification.

While much of the discussion in this regard has focused on social media, it is important to recognise the significance of technology companies outside of social media as well. Research by Netsafe/GASA finds that email is the most common vector through which people receive scam attempts,[68] although notably this may be more a measure of how easy it is to send large numbers of scam emails than how many people are actually defrauded by scams delivered through email. Key companies in this area are Google and Microsoft, who provide widely used email services (Gmail and Outlook), and therefore have the ability to control what messages reach their users, and how those messages are presented (i.e. whether messages are flagged as potential phishing, whether links are enabled, etc.). Email addresses hosted privately – for example business emails – are notably outside of this, and are subject to scam protection measures only if the company operating the server chooses to apply them.

Dating sites and apps are also important – while the number of people who report receiving scams through this vector is relatively low (8% according to Netsafe/GASA), romance scams, where a person is tricked into a fictitious relationship and then manipulated into sending the scammer money, can be particularly costly and personally devastating,[69] and have seen an increase in prominence internationally since the pandemic.[70]

Search engines can also be a key vector for scams. Scams that are able to reach victims through search engines can be particularly effective because of the presumption of legitimacy that comes with their presence in search engine results – especially if they are one of the promoted links that appear at the top of the page.

Search engine processes for removing fraudulent links from their searches do not appear to be working well. Both victims and experts described frustrating attempts to get search engines to take down links to websites, in which the search engine was extremely slow, or even refused, to remove sites posing as legitimate banks and investment companies.

> I've heard of bank CEOs who have gone to those search engine companies and asked for those sites to be taken down, and it takes literally months and months for that to occur when it's a known scam, fraudulent site. And so it's very frustrating, because banks can't tell a social media or big tech company what to do, but government can, so that's why we need that intervention.
> *Roger Beaumont, New Zealand Banking Association CEO*

> I also reported it to Google. I told Google that this was a fake [website]. They didn't take me seriously. They said they were being paid for it, so why would they take it down?
> *Victim*

---

[68] Global Anti-Scam Alliance (2024). *The State of Scams in New Zealand 2024.* Netsafe and GASA.

[69] Cross, C., Dragiewicz, M., Richards, K. (2018). Understanding Romance Fraud: Insights From Domestic Violence Research, *The British Journal of Criminology,* Vol 58 (6), 1303–1322.

[70] Buil-Gil, D. and Zeng, Y. (2022), Meeting you was a fake: investigating the increase in romance fraud during COVID-19, *Journal of Financial Crime*, Vol 29 (2), 460-475.

Other countries are enacting significant consumer protections

Internationally, there has been a considerable push toward providing greater consumer protections for scams in recent years. The best example of this is in the United Kingdom, which has been a leader in consumer protections, but we can also look to the example of measures that are currently being developed in Australia.

These laws can be expected to significantly harden those countries against scams, causing transnational organised crime groups to look elsewhere for vulnerabilities to exploit. It is important, then, that New Zealand seek to keep up with these developments: if we allow ourselves to fall behind, we may risk becoming a significant target.

The United Kingdom's scam reimbursement system

One of the key directions in Minister Bayly's letter to the banking industry is that the banking industry investigate a voluntary reimbursement system for victims of authorised payment fraud. This is a direct reference to a system that has been in operation in the United Kingdom for the last five years. This system is unique to the UK, but similar models are being investigated elsewhere, including Australia.

A reimbursement scheme represents a means of making the systems that enable scams directly and proportionately responsible for harms that occur through them, while also greatly enhancing outcomes for consumers. While the UK model only requires reimbursement from banks, models proposed elsewhere extend this liability to other systems that enable scams as well.

The UK's voluntary Contingent Reimbursement Model Code (CRM Code) was introduced in May 2019 to provide a framework for reimbursing victims of Authorised Push Payment (APP) scams. Under the CRM Code, Payment Service Providers (PSPs) that signed up voluntarily committed to reimbursing customers who were not at fault in relation to a scam. Some banks, particularly smaller institutions, chose not to sign up to the CRM Code, but the large majority, including all of the country's major banks, are signatories.

While this code was notionally voluntary, UK-based victim advocate Janine Starks reports that this was not something banks would have signed up to if they felt they had a choice.

> …our banks won't do anything voluntarily in the UK. They succeeded with a voluntary reimbursement scheme, but you need to understand the law here to realize there's nothing really voluntary about one arm behind your back and a gun to your head.
> *Janine Starks, victim advocate*

As a result of the CRM Code, rates of reimbursement for scam victims in the UK are high. The most recent Crime Survey for England and Wales, which is a self-report survey similar to the NZCVS, found that of the approximately 2.7 million scam incidents where victims lost money, "the victim was fully reimbursed in 1.9 million of these incidents".[71] While no comparable statistics exist in New Zealand (the Netsafe/GASA survey, for example, asks about money recovered, which may not cover reimbursements, particularly in the longer term), rates of reimbursement can be expected to be much lower.

---

[71] Office for National Statistics (2024). *Crime in England and Wales: year ending June 2024*. UK Government: Office for National Statistics.

[72] This was reduced from an initial proposal of £415,000 in a decision made in September 2024, two months before the scheme entered force.

In 2024, the CRM Code has been updated with the introduction of a mandatory reimbursement scheme, which entered operation in October. This scheme makes reimbursement mandatory across the entire banking sector, with the cost shared equally between the sending and receiving banks. The reimbursement cap is set at £85,000,[72] although banks may choose to reimburse beyond that level.

While it has been suggested by banks that the UK's reimbursement system is at risk of creating a situation where customers are reckless about potential scams because they know they are likely to be refunded, there remain significant guardrails against claims by those who have been 'grossly negligent' in making a payment, for example if a bank has given them a targeted warning that they are likely sending money to a fraudster. In cases of gross negligence by the victim, the bank is unlikely to be forced to reimburse.

The outcome of the CRM Code, according to experts, has been a precipitous increase in scam-protection efforts by banks.

> Suddenly we have the most amazing fraud technology here [in the UK], because [banks] don't care about protecting customers, but they will protect the shareholders. So if they've got a liability for the fraud, they need to protect the shareholders from that, and they will invest in all the tech that they need to.
> *Janine Starks, victim advocate*

> You've got that pressure [on banks to prevent fraud]. And what I've noticed is that has made the banks take fraud much more seriously and introduce a lot more initiatives to try and prevent fraud.
> *Prof. Mark Button, University of Portsmouth*

Many experts took a cynical view of the private sector's motivation to combat scams, and felt that the CRM Code had been an effective tool because it directly targets the primary motivations of banks as profit-driven companies.

> If the banks don't have to reimburse, then what is their interest in doing more to prevent fraud? It doesn't matter to them.
> *Prof. Mark Button, University of Portsmouth*

This view would appear to be borne out by the New Zealand banking industry's visibly increased interest in anti-scam measures following Minister Bayly's letter.

UK fraud expert, Professor Mark Button, reported that while the UK's voluntary reimbursement scheme had been in his assessment a very significantly positive move for scam prevention, the fact that many banks had not entered into it, and that the amount they would reimburse varied considerably between banks, produced a system that was inconsistent and not as victim-friendly as it could have been. He describes this as a key pitfall to avoid when setting up a similar system in New Zealand, and a major reason why the UK has now shifted to a mandatory industry-wide scheme.

> If it's voluntary, then you guys will get what we've had, and up until now you get some banks that will reimburse some won't, then you get some banks that will reimburse in some situations and not others.
> *Prof. Mark Button, University of Portsmouth*

[73] Button, M., Hock, B., Shepherd, D., Gilmour, P. (2023).

Importantly, the impact of these measures on rates of scam itself remains essentially untested. Somewhat surprisingly, we are aware of no evaluations of the outcomes of the voluntary reimbursement scheme. UK scam experts consulted said that while the scheme has been active for a number of years now, its inconsistency of application across the banking sector means that its impact on scams is unclear. While the UK has not seen the same leaps in scam rates in recent years that New Zealand has (although they did rise precipitously during the pandemic), this may not be meaningful because their rates of scams have been high for longer.[73] The UK government has committed to building evaluation measures into its mandatory reimbursement scheme, however, so some results can be expected in coming years.

The United Kingdom's Online Safety Act and Online Fraud Charter

Recently, the UK has made significant moves toward preventing scams through social media. In 2023 the Online Safety Act entered law, mandates that tech companies remove illegal content, including child sexual abuse, hate speech, and terrorism, from their platforms. Companies found to be in breach of the Act can be fined up to £18 million or 10% of their worldwide revenue, whichever is greater, criminal action can be taken against senior staff, and in serious cases access to UK payment providers can be revoked, preventing the company from making money in the UK.[74]

The UK government and major technology companies have also recently adopted an Online Fraud Charter.[75] Signatories include Facebook, Microsoft, Google, eBay, Amazon, and TikTok. This charter binds signatories to adopt a variety of mechanisms to combat scams on their platforms, including intelligence sharing, providing effective reporting tools, liaising with law enforcement, and verifying the legitimacy of advertisers on their service.

Australia's proposed Scams Prevention Framework

The Australian government has announced its intention to introduce new laws to combat scams and enhance protections across relevant sectors. These measures are called the Scams Prevention Framework (SPF), which was introduced as a bill in November 2024.

The SPF bill would allow for the relevant sectors (such as banks, telcos, and tech companies) to be designated as "regulated sectors", and requires those sectors to take actions to prevent, detect, report, disrupt, and respond to scams. Each sector's responsibilities would be defined in sector-specific codes of practice.

The bill mandates businesses to report scam activities to the Australian Competition and Consumer Commission (ACCC), implement detailed governance policies, and establish internal and external dispute resolution processes. Non-compliance could result in significant civil penalties, with fines reaching up to $50 million for serious breaches.

Additionally, consumers can seek compensation through external dispute resolution mechanisms or directly initiate legal proceedings for damages. This is not an automatic requirement for reimbursement, but if a regulated entity fails to meet its obligations under the SPF, there is a presumption that the entity will compensate the victim for their scam losses. Liability for this reimbursement can be divided among multiple parties through a single resolution process.

---

[74] Gov.UK (2023). What the Online Safety Act does. Government of the United Kingdom.

[75] Government of the United Kingdom (2023). *Online Fraud Charter.*

[76] DIA (2023). *Safer Online Services and Media Platforms.* Government: Department of Internal Affairs.

Multinational tech companies may be highly resistant to regulation

While banks and telcos are subject to tailored regulation governing their activities in relation to scams, tech companies are not. As concluded recently by the DIA,[76] there is a need for regulation, and potentially for a regulatory body, in this area.

International tech companies have generally been resistant to efforts impose regulation on their activity, particularly those that impose costs on their operations, and have frequently employed the threat of simply leaving a given market rather than accepting regulation. A characteristic example can be found in recent efforts to introduce laws requiring technology companies to pay media outlets for linking to their articles through their news services. In early 2021, Google and Meta threatened to withdraw their services from Australia over proposed media laws that would require tech giants to pay news publishers for their content.[77] In Canada and New Zealand,[78] Google and Meta also threatened to stop linking to news articles in response to similar laws. In Australia and Canada neither Google nor Meta have followed through with these threats, although it appears that Meta is in the process of ending the deals it had initially struck with Australian media companies. In New Zealand, the Fair Digital News Bargaining Bill has not yet entered law, and has been described as being 'in limbo'.[79] Big tech companies have recently threatened to leave the UK[80] and EU[81] over other types of proposed laws as well.

It is important to be aware, then, that strong scam protection laws – particularly those that impose significant financial costs on technology companies – may be expected to result in similarly forceful bargaining efforts from tech companies. Given the comparatively small size of New Zealand as a market, companies may be willing to push these threats further than they have elsewhere.

One possible means of circumventing this issue is to seek to enact measures as part of regional partnerships with other nations, rather than simply approaching them in isolation.

Recommendations

The fairest approach is one where companies bear the cost of scams that occurs through their systems

The loss of consumer trust, and the harms done to significant numbers of people through scams, have thus far not been sufficient drivers for improvement. While it must be acknowledged that there is good work happening in many areas, banks began working on key measures only after being directly prompted by Minister Bayly, and tech companies have, as an industry, generally shown little genuine concern for the issue. Any new measures, it must be concluded, need to include penalties for private companies that fail to protect their customers from scams.

Systems of fines and sanctions, while preferable to nothing, are not an ideal approach, however. They are reliant upon the government to remain highly vigilant to the issues in relevant industries, and to have the investigation and enforcement resources available to deliver sanctions, both of which are likely to come at considerable cost. They may also produce hills and valleys of consumer protection,

[77] BBC (2021). Google threatens to withdraw search engine from Australia.

[78] Radio New Zealand (2024). Google threatens to stop linking to NZ news sites if bill passes.

[79] Radio New Zealand (2024). Fair news bargaining bill in limbo as minister says it is not ready.

[80] BBC (2023). Why US tech giants are threatening to quit the UK.

[81] Cory Doctorow (2024). Big Tech to EU: "Drop Dead". Electronic Frontier Foundation.

where efforts improve after interventions by government, but then decline with time. Moreover, they may encourage companies to do only as much to prevent scams as they need to do in order to avoid being sanctioned.

The most effective approach, then, is one where companies whose systems have been leveraged to enable scams are required to reimburse victims. This would ensure that cost to companies is directly proportional to the amount of loss suffered by victims, and creating a tangible and immediate incentive for companies to invest in scam protection systems that work as well as possible. Such a system would greatly reduce harm to victims, and would also require considerably less investment in enforcement efforts from government.

It is clear that there is a need for a system of reimbursement that goes beyond only the banks, and to include other systems that are exploited by fraudsters as well, as is intended in Australia. The ratio at which this might be divided up in each case is beyond our ability to consider here, but reimbursement need not necessarily be split evenly.

Following existing practice, this is likely best achieved through codes of practice for each industry. As noted earlier, these codes, and the regulatory bodies needed to establish and administer them, already exist in the case of the banking and telecommunications industries, but are absent in the tech and social media space.[82] A tech company regulator and code of practice is needed as a priority. Following the experience in the UK, these codes are likely to need to be made mandatory, otherwise there is a risk of inconsistency of outcomes for consumers.

Any system that involves multiple parties potentially liable for reimbursement will need a 'single door' through which victims can apply for reimbursement. In Australia's upcoming SPF, this is to be accomplished through the Australian Financial Complaints Authority (AFCA), which is an ombudsman system for financial complaints. The AFCA will divide the cost of reimbursement between banks, digital platforms, telecommunications companies, and others.

As an alternative, consumer and victim advocates suggested that the most practical and victim-friendly approach would be one where victims can claim full reimbursement of scam losses from banks, through a system similar to that used in the UK, but where banks then have the ability to seek a portion of those losses from other platforms that may carry a degree of fault, such as tech and telecommunications companies. This would significantly reduce the burden on the victim, minimising their engagement with a painful process that may otherwise draw out their revictimisation, and place it on companies better equipped to handle it.

> The analogy I use is the Consumer Guarantees Act: when your blender breaks you take it back to Briscoes, and if Briscoes chooses to, they then go to Breville and say, "hey, this is the fifth blender of this week that we've had returned. We want you to do something about it." And they've got the resources and the buying power to do that, whereas the consumer doesn't.
> *Jon Duffy, Consumer NZ CEO*

An important advantage of a bank-first system is speed: in the UK, banks are required to provide reimbursement very quickly, and in the majority of cases do so within five days.[83] Ombudsman-based systems can be expected to take much longer, particularly if blame must be argued and apportioned between multiple parties – creating a situation of ongoing uncertainty, stress, and revictimisation that

---

[82] DIA (2023). *Safer Online Services and Media Platforms*. Government: Department of Internal Affairs.

[83] Atkin, Michael (2024). The federal government is cracking down on scams. How does Australia compare to other countries? ABC News.

[84] Banking Ombudsman (2024). Frequently Asked Questions.

is undoubtedly a negative for victims. Cases heard by the Banking Ombudsman in New Zealand, for example, are usually resolved within three months,[84] but more complex cases can take considerably longer, and some of the investment scam victims we spoke to reported cases that took over a year to reach a resolution.

The government can be an enabler of private sector communication

If the government is to expect that the private sector reimburse victims of scams, as we argue it should, it must in turn work to enable private sector scam prevention to be as effective as possible.

A fundamental issue reported by private sector scam teams we spoke to was that of information sharing. Even when they are using everything at their disposal, it can be difficult for private sector scam prevention professionals to access the information that is outside of their company or industry's area, limiting their ability to draw the crucial connections that allow them to prevent scams. Any system that can unite these data into a coherent whole can be a powerful force multiplier for existing scam protection systems.

An approach that was endorsed by all of the private sector experts we spoke to was that of an anti-scam centre run by the government in partnership with banks, telcos, and tech companies. A key part of this would be a fusion centre that could draw information together from the wide variety of available sources and combine it into a shared resource.

The value of a combined anti-scam centre is discussed further in the next section of this report.

SIM card registration rules needed

Scam text messages are currently made easier to send by the lack of any rules requiring customers to prove their identity when buying or setting up new SIM cards. Many comparable countries, such as Australia and the nations of the European Union, require ID checks of various kinds in order to purchase or activate a SIM card, ensuring that any phone that is used for illicit purposes is tied to a person's identity. While there are several comparable countries that do not require identification for SIM purchases, such as the UK and USA, it is common practice for telcos in those countries to choose to require identification anyway.

The current ease of purchase for new SIM cards is a direct enabler of spam-based scam practices that are currently popular among fraudsters. Many text scams are sent using SIM box devices, which is a device used in telecom for routing calls and SMS messages via multiple SIM cards. It functions like a mobile phone that contains several SIM cards, allowing it to send out a spam message in large quantities quickly and from different phone numbers, potentially skirting automated blocking measures. When SIM cards are inevitably identified as being used for spam and blocked, fraudsters can simply remove the blocked card and insert another, allowing them to continue for as long as they have access to new SIM cards. Requiring identification would significantly restrict that supply of new cards, largely making this particular method of delivering spam untenable.

This would not prevent text spam entirely – fraudsters will always work to find new ways to gain a supply of SIM cards, or to send text scams using other methods – but does close a particularly broad gap in New Zealand's scam defences. DIA staff that we spoke to theorise that lax requirements around SIM card availability – and the closing of similar gaps overseas – may be a reason why they have identified cases of transnational organised crime groups recruiting individuals in New Zealand to operate text spam scams using these methods.

While a blanket legal requirement for identification is preferable, it is also possible for telcos to introduce identification policies for new SIM cards on their own. It is unclear why telcos have not already chosen to institute this themselves, although the answer is likely one of cost, and potentially the unwillingness of any given company to be the first one to introduce a measure that creates a barrier to entry new customers. As noted earlier, it is common practice for telcos overseas to require identification, even in countries where there is no legal requirement. This would need to be done consistently on an industry-wide level, however, because if any telcos choose not to collect ID, or had more relaxed requirements, fraudsters will simply focus on that company.

In terms of steps that can be introduced immediately, restricting bulk purchases of SIM cards to verified legitimate customers would also be of clear benefit. Many telcos allow SIM cards to be purchased in bulk, allowing spam scammers easy access to an essentially endless supply of SIM cards.

It has been noted that the movement towards embedded SIM cards (eSIMs) may reduce opportunities for this type of scam. eSIMs are built-in digital SIM cards that remove the need for a physical card to be placed within the device, and are believed to be less vulnerable to abuse because of the difficulty of changing a device from one eSIM to another, which requires the input of the telco. Given that eSIMs cannot be used on older devices, it is unlikely that telcos will be in a position to stop selling physical SIM cards at any point in the near future.

Establishing an effective response

- Internationally, countries are moving toward anti-scam centres that centralise intelligence collection and analysis. This appears to be the best way forward for New Zealand as well.
- An anti-scam centre must be built around collaboration between the private and public sectors, because both sectors hold important data and expertise.
- Scam prevention is first and foremost an exercise in data analysis, and a key part of an anti-scam centre would be fusing the data and intelligence sources available into a workable whole.
- If our scam protection falls behind that of other countries, we risk being specifically targeted by transnational organised crime.

Recommendations:

- An anti-scam centre that combines reporting, analysis, and public education functions should be established. This would work best as a physical centre that is designed around collaboration between public and private sectors.

Alongside advances in consumer protection, international anti-scam efforts are moving toward the use of centralised anti-scam centres that draw together the resources of the public and private sector in a physical location. This represents the best approach for New Zealand as well, because it recognises that scam prevention is a data-driven problem that spans across a multitude of privately-owned communication technology systems.

There is considerable demand and enthusiasm for such a centre, and it was recommended by experts of all kinds.

A combined anti-scam centre is the best approach

To achieve a truly effective response to scams, we recommend that the government establish a combined anti-scam centre that brings together government agencies and private sector partners in a shared physical location.

This approach was recommended by all of the experts that we spoke to as a priority, and is well established in advanced overseas approaches.

This centre would ideally incorporate and centralise the following elements:

- Management of a scam reporting system
- Collecting information on the latest scams and distributing this to both public and private sector agencies
- Assigning scam cases to relevant agencies
- Analysis and fusion of scam data (from both internal and external sources)

- Maintaining lists of bank accounts, phone numbers, and other identifying details believed to be used by scammers
- Liaison and information sharing with international anti-scam centres
- Public education around scam prevention, awareness, and current methods

A combined anti-scam centre would take reports of scams and process them, and fuse and analyse data from sources such as the private sector and anti-scam agencies overseas to direct the law enforcement response. As a result of this up-to-date oversight of scam patterns, it would also be well placed to coordinate public education work that best aligns with the realities of scams. The actual investigation and policing of fraud cases would still likely need to be undertaken by local Police and other relevant agencies due to the volume of cases.

A centralised response is important because scammers do not limit themselves to single methodologies or approaches. As defences in one area are strengthened, or as a new vulnerability becomes available, scammers will move toward targeting areas of weakness, regardless of whether that means engaging victims through text messages, social media, or through other methods. An approach where different arms of scam prevention (i.e. banking, telecommunications, and so on) are separated, therefore risks failing to identify larger patterns of activity.

Anti-scam centres of various types exist in Australia, the United Kingdom, and Singapore, with Singapore's being widely regarded as the gold standard. The Singapore Anti-Scam Centre (ASC) was established by the Singapore Police Force under the Commercial Affairs Department in 2019. The ASC serves as the nerve centre for investigating scams, combining government agencies with stakeholders in the private sector in a shared physical location. A key strength of Singapore's system is that it has enabled reports and data to be processed and analysed very quickly. This is vitally important for scam prevention because of how rapidly cyber-enabled fraudsters can work to defraud people. Fast responses mean that harm is limited much more quickly, as fraudsters' phone numbers, email addresses, and websites can be blocked before more victims come into contact with them.

As noted earlier, there are not yet any best-practice approaches to scam prevention that are empirically proven, because the problem is simply too new, and international responses are in their infancy. While the approach taken in Singapore is very promising, this applies to the creation of combined anti-scam centres as well.

It does appear clear, however, that the particular problems that scams present are logically best addressed through a system that prioritises speed, collaboration, and data fusion – all of which a combined anti-scam centre is best placed to deliver.

Public-private partnership is required

To be truly effective, this centre must include representatives of the private sector companies that run their own anti-scam teams, such as banks, telcos, and tech companies. As outlined earlier, these companies are critical because it is their systems that fraudsters target, and through which scams occur. Failing to include these experts – and the streams of data that they have oversight of – at the core of the scam prevention system would needlessly limit New Zealand's ability to analyse data effectively and quickly.

Critically, buy-in among private companies is very high. All of the private sector professionals we spoke to were enthusiastic about the idea, and strongly emphasised that a combined approach would work better than the piecemeal approach currently in use, where different parties are largely operating in silos.

> There's a lot of people in fraud teams like the one I'm in at other telcos, ones at other banks that have really good knowledge, and I think it's just getting that all together and pulling together in one place [would be very helpful]. I think that that would be one of the benefits of if we could have a scam centre, just sheer intel collection, just being able to sort of harness that data, to then be able to analyse it and look for things that maybe we're not seeing [on our own], or maybe we didn't know.
> *Telco scam expert*

> I think it has to be central... For scam prevention, at the moment, there's little bits here, little bits there, and it's not lined up. If you're not joined up, it's not working towards a common goal... and that helps the criminals, essentially.
> *Telco scam expert*

As noted earlier, banks in New Zealand set up a combined anti-scam centre in 2023, but this centre is solely between banks, without any government partnership or public-facing elements. The NZBA has called upon the government to consider using their anti-scam centre as the basis for a combined public-private centre, however.[85]

> When you look around the world, the jurisdictions that have been the most effective in combating scams have been countries where it's been a government led initiative, where government have recognized that actually, there are so many players involved and so many government agencies that have a responsibility and part to play that actually no single industry can take that leadership position and provide that coordination. So it is a matter of government stepping up and providing that.
> *Roger Beaumont, NZBA CEO*

There are potentially considerable efficiencies to be created by drawing private sector efforts together into a single operation. Work appears to be being replicated across different companies in various areas. One example is in the blocking of scam URLs by telcos: because there can be liability involved if a legitimate link is blocked by accident, telco staff spend time analysing each one before blocking it. If a government run anti-scam centre was able to publish a list of identified scam URLs to a system that could block them for all telcos automatically, as is currently being trialled in relation to child exploitation material, considerable delay could be avoided.

Current models of communication may not be a good basis for effective collaboration

The government has recently suggested that a decentralised anti-scam centre like approach can be achieved simply through building effective communication channels within agencies. This may be possible, but current interagency communication does not appear to present a strong base to build upon.

Government agencies appear to overestimate the effectiveness of existing information sharing practices. All of the government and NGO staff that we spoke to emphasised that there are already established channels of communication between them and other agencies, and that they regularly pass information through those channels. Government staff working in the area have regular Teams meetings on the subject of scams, during which they exchange details about current trends, events, and concerns. Their assessment of this system's effectiveness is generally positive.

---

[85] Beaumont, R. (2024, April 12). L*etter to Minister of Commerce and Consumer Affairs.* New Zealand Banking Association.

Non-government stakeholders who have been involved in these systems were not impressed with them, however.

> We've previously been on the interagency fraud working group, but quit in January because we were sick of it being a talk fest, and just nothing really happening.
> *Brent Carey, Netsafe CEO*

Moreover, it is clear from the extremely high rate of scams occurring in New Zealand, and the fact that the boom in this offending has largely gone unrecognised, that these systems are not working.

Accessing the wealth of information and expertise held by the private sector is also currently difficult. Government and private sector staff we spoke to reported that despite being aligned in goals, and with many good working relationships between individuals, there is considerable separation between the two.

Private sector staff described government as something of a black box, into which reports and information would flow, with little coming back.

Government staff also report that even though private sector groups are notionally aligned with government against scams, government staff we spoke to noted that gaining access to the information they hold can be difficult and time-consuming with current systems, often requiring formal search warrants even in cases where the bank itself is a victim.

Fixing these misaligned relationships and intelligence sharing systems will require formal information sharing agreements, but also the type of deep collaboration that is difficult to establish and maintain remotely. If collaborative relationships are to be built quickly, as is necessary here, the best approach appears to be a centralised one.

Fast intelligence processing and response is essential

Experts consistently emphasised that response speed is critically important when dealing with scams. Because scams are often undertaken repeatedly and quickly, failing to act on information immediately is highly likely to result in more scams taking place. The Netsafe/GASA survey found that 46% of scams are completed within 24 hours of first contact with the fraudster, and more than a quarter within only a few minutes.[86]

New Zealand's government agencies were widely reported to be unable to deliver the type of quick response that that this offending requires.

[In Australia] they get alerted to or their own investigation detects a suspicious ad for an investment scam or for a website posting a potential scam, and they're analysing it within 24 to 48 hours and then initiating a takedown, and notifying all the other relevant players in the ecosystem… which means, if Banks continue to not act on red flags indicating that you know that that scam has been accessed by a customer, they may have some liability.

> What do we have in New Zealand? [The DIA] might put something up on its website after six weeks or something like that. Everyone's been done by then, the horse has bolted.
> *Jon Duffy, Consumer NZ CEO*

[86] Global Anti-Scam Alliance (2024). *The State of Scams in New Zealand 2024*. Netsafe and GASA.

A combined and physically centralised anti-scam centre would appear to be the best way to ensure that New Zealand's processing of scam reports and intelligence is as quick as possible. As noted earlier, speed of processing and analysis has been noted as a critical strength of the Singaporean anti-scam centre.

Scam prevention is a matter of data

As a crime that occurs through manipulation of information technology systems, the pathways of fraudulent activity are marked with clear digital footprints in the form of calls, emails, bank transfers, and more. These footprints are how fraudsters can be discovered, investigated, and locked out of the system. Even when detection begins through a human factor – i.e. a report by a victim, or report of a fraudulent message – it is through analysis of data that the scam operation itself can be mapped out.

At the moment, data is a critical weakness. There is a lot of data available, but it is siloed in private companies and difficult to access. Even within government, there are multiple sources of data working independently of one another, with exchange taking place simply through human relationships. There is also a wealth of important data available from anti-scam centres overseas.

Making good use of data is not only a matter of having access to it, but of being in a position to understand it and draw connections between points. Law enforcement agencies are able to request access to data from all of the relevant sources already, but without visibility across those sources, that ability is very difficult to use. Enough information to paint a clear picture of a scam operation may be present across these various sources, for example, but because no individual or automated detection system sees more than a single data point, the connections are never drawn.

This issue is not unique to New Zealand by any measure, but is something that other countries are responding to by centralising their scam prevention measures.

A crucial role of an effective scam response is fusing the data that are available into a cohesive and useful combined system. What this might look like is beyond our ability to consider here, but fusion centres of this type are widely used in other areas of data-driven law enforcement,[87] and would be a fundamental part of any anti-scam centre.

> We have fusion centres set up for other crime types like child exploitation, and you have multiple agencies, including government and NGOs, working together there effectively. And it's probably a really good practice model in terms of creating a national response to a particular problem.
> *Government expert*

In some cases, transnational organised crime intelligence fusion centres are operated regionally, rather than by individual countries. Given the role that transnational criminal groups are believed to play in scams, this may be an approach that is worthy of consideration. The Five Eyes[88] intelligence alliance may be a valid basis for such an approach, given that all five countries are likely to be targeted by similar groups, although the sharing of information fused at a high security classification may pose challenges.

---

[87] Carter, J.G., Carter, D.L., Chermak, S., McGarrell, E. (2017). Law Enforcement Fusion Centers: Cultivating an Information Sharing Environment while Safeguarding Privacy. Journal of Criminal Psychology. 32, 11–27.

[88] Five Eyes is an intelligence alliance between Australia, Canada, New Zealand, the United Kingdom, and the United States.

Beyond accessing and combining the data that already exists, there is also a critical need to generate more data though improving the scam reporting system, as already discussed. This means making it easier for people to report scam, as well as fostering an understanding of why reporting scams (including those that are not successful) is important in the first place.

Privacy Act changes may be needed

An important hurdle to effective information sharing identified by many working in the area of scam prevention is the Privacy Act.

The Privacy Act 2020 is an important law that governs how organisations collect, use, store, and share personal information. It ensures that individuals know when their information is being collected, that it is used and shared appropriately, and that it is kept safe and secure. This can make it difficult or impossible for agencies and private companies to share information when it contains personal details.

> I think one of the problems is, and obviously for good reason, the privacy restrictions can be quite prohibitive when it comes to this sort of intelligence sharing.
> *Telco scam expert*

It is not unusual for agreements to be made between entities to allow for the sharing of this kind of data to take place under certain circumstances, and it appears that this is likely to be required for a scam centre to work.

Given that the companies involved do hold a large amount of personal data about New Zealanders, this would need to be done with extreme care to ensure that the data involved is kept safe, and not misused.

Allowing New Zealand's scam response to languish will lead to New Zealanders being targeted

As a crime that can be committed entirely through communication technology, scams present a unique opportunity for criminals to work transnationally in a way that is almost unprecedented.

Many scams occurring in New Zealand are believed to be perpetrated by criminals working transnationally, often as part of organised criminal groups. Even in instances where the offender operating scams in New Zealand, government experts reported that they are sometimes working with, or in the employ of, transnational organised crime groups that provide them with expertise and tools.

Because they operate internationally, these groups have a wide view across scam prevention measures around the world, and can move to exploit vulnerabilities wherever they become apparent. This is not unlike the approach used by groups distributing illicit drugs, but can take place much faster, moving at the speed of information instead of shipping lanes.

Because no system can ever be truly immune to scams, the most vulnerable systems may simply be those whose defence regime is the least developed relative to others. As many countries move to harden their systems against scam, and to develop approaches that are capable of reacting to emerging scam methodologies more rapidly, transnational fraudsters will be looking toward those whose response is weaker than others.

If we do not ensure our approach is in line with international best practice, New Zealand could find itself in the position of being targeted.

> If you don't do it, and lots of other countries are, New Zealand will be the weak link, and the criminals will work that out. [They will realise] New Zealanders are a softer touch to get, because the banks don't stop these payments. And these forces are obviously very clever, and they work these things out. They will target New Zealand more.
> *Prof. Mark Button, University of Portsmouth*

Conversely, building a reputation for being a leader in scam prevention is likely to act as something of a shield.

It must be noted that although many other countries – primarily those whose resources are the most limited – are not working on novel scam prevention measures, this fact will not necessarily mean they are targeted more than New Zealand. As a relatively wealthy country, New Zealand will always be considered a high value target, so it is not a question of how our scam response compares with all countries, but rather how it compares among other wealthy nations specifically.

New Zealand must take steps to ensure that its response is at least as good as those in comparable nations, to ensure that we do not fall behind. It must also do so in ways that are highly visible: a centralised response that is well-branded and publicised not only builds buy-in among the public, but also sends a clear message to transnational criminal operators. A divided approach grounded in an enhanced version of business-as-usual scam policing may risk sending the opposite message.