SFO

SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

G74

Staying ahead of the curve

Responding to emerging trends in detecting fraud and corruption in New Zealand

Contents

Foreword 4

Executive summary 5

Understanding fraud, corruption and its costs 6

What is fraud costing us? 8

The evolving landscape: Key trends in fraud and corruption detection 10

Technological arms race:
Increased sophistication and
artificial intelligence 12

Collaboration and information sharing:
A critical imperative 14

Data and analytics:
Understanding the problem 15

The human element:
Psychological and behavioural insights 18

What's ahead? Three possible futures for New Zealand 20

The digital fortress: A global leader in
anti-fraud and corruption innovation
A best-case scenario 22

The shadow economy: Corruption creeps in
A middle-ground scenario 23

The captured state: A nation compromised
A worst-case scenario 24

Findings: Turning challenges into opportunities 25

Finding: Reducing the effort to report
fraud enhances detection 28

Finding: Impetus for change comes from
understanding the scale of the problem 30

Finding: The innovation race – technology
creates novel threats and opportunities
to counter them 31

Finding: Informants and whistleblowers
are crucial pieces in the detection toolkit 32

Finding: Detecting corruption requires
specialist expertise 33

Finding: Understanding human psychology
helps us detect fraud and corruption 34

Conclusion 36

End notes 38

Foreword

Tēnā koutou,

Welcome to the Serious Fraud Office's Long-term Insights Briefing, examining trends in fraud and corruption detection. The release of this briefing comes at an important time.

We are in the midst of a global fraud epidemic. Around the world, and in New Zealand, fraud is the most common and fastest growing crime type. Domestically it is affecting hundreds of thousands of people every year, driven by rapidly advancing technology, increased digitisation, financial strain and changes in our social fabric. While it's hard to get an exact measure on the extent of the problem, evidence suggests we are potentially losing billions of dollars every year to unscrupulous fraudsters.

New Zealand has a reputation as a country with low levels of corruption, but our global corruption perception ranking is slipping, risking our attractiveness as a safe place to invest. The impact isn't just on our economy - fraud and corruption can destroy individual lives, cause generational harm, divert funds from vulnerable communities and threaten our health and safety.

Against this fast-paced and rapidly evolving backdrop, it is critical we do all we can to continue effectively detecting fraud and corruption. This landscape presents challenges, but it also brings opportunities. Advances in technology create detection opportunities for law enforcement agencies across the globe, and our international partners are launching initiatives which are worth exploring in the New Zealand setting. We must keep a keen eye on new developments to ensure we are staying ahead of the curve.

Thank you to all those who contributed their time and effort to this work. It is vital that we work together with our partners in protecting New Zealand from the ever-present and growing threat of fraud and corruption.

Ngā mihi,

Karen Chang
Director and Chief Executive
Serious Fraud Office
Te Tari Hara Tāware

Executive summary

Fraud and corruption represent escalating global threats that undermine economic stability, erode public trust, and divert crucial resources. Over recent years, the volume and sophistication of these crimes have surged, driven by rapid technological advancements and increasingly complex methodologies. Interpol estimates that financial fraud accounts for 40-70% of all crime in many member countries, highlighting the pervasive nature of this criminal activity.

In New Zealand, fraud is now the most commonly experienced crime, resulting in hundreds of millions of dollars in losses for individuals and businesses annually, with public sector losses potentially reaching billions. Traditional methods of detection, investigation, and prosecution are increasingly challenged by the scale and complexity of modern fraud and corruption.

This briefing explores the evolving landscape of fraud and corruption detection, with key insights and best practices from international jurisdictions as well as the Serious Fraud Office's (SFO) own experience. It examines trends impacting fraud detection, including the technology (particularly artificial intelligence) being employed by both those committing fraud and those fighting it; the importance of increased collaboration between agencies as well as with private stakeholders; how data and analytics are driving an improved response; and the human factors which underpin offending.

These findings are used to develop three possible futures faced by New Zealand, from a digital fortress lauded as one of the most secure nations in the world through to a captured state which has become a hub for fraud and corruption.

While there are forces at play that, left unchecked, could push us towards a worst-case scenario, there are also strategic opportunities being explored by our international partners which can enhance detection capabilities. These include harnessing new technology, protecting and incentivising whistleblowers, reducing confusion around reporting, improving the data which drives detection, modernising legislation and recognising the importance of specialisation.

It is critical we continue to adapt - not only to ensure we are detecting fraud in the face of increasingly sophisticated tools employed by criminals, but also to harness the opportunities presented and ensure an intelligence-driven, proactive and predictive detection approach. Addressing this requires innovative thinking, investment in technology, enhanced specialist expertise and integrated approaches involving the public and private sector.

Understanding fraud, corruption and its costs

For this Briefing, we have used the definitions of fraud and corruption put forward by the New Zealand's Office of the Auditor General.[1]

Fraud: *an intentional act by one or more individuals involving the use of deception to obtain an unjust or illegal advantage.*

Fraud encompasses a wide range of financial crime. Some fraud is complex and confined to a specific entity, while other types of fraud, like scams, can impact a wide range of victims.

Corruption: *the abuse of entrusted power for private gain (such as soliciting or receiving gifts or other gratuities to perform an official duty or omit to perform an official duty). Corruption is a type of fraud, and it includes bribery.*

The sometimes indistinct line between the actions people consider corrupt, actions of unfair practice, and explicit criminal offending makes defining corruption a challenge. Broadly, corruption fits across three categories:[2]

- Grand corruption (complex offending, undertaken by high-level officials or senior leaders, involving large sums and potentially widespread harm. It may include the misappropriation of public or corporate funds).
- Petty corruption (less complicated, undertaken by single actors – often in the form of bribery, or petty theft).
- Electoral fraud, aimed at unfairly influencing election outcomes, which is distinct from the above in that it is primarily committed by political figures and political parties rather than public officials.

From a legislative perspective, New Zealand has no singular fraud or corruption offence. Fraudulent behaviour is charged under offences involving deception and dishonesty, such as 'obtaining by deception' under the Crimes Act 1961. Corruption offending, including bribery, is deceptive and dishonest by its nature, and fits within the behaviours associated with fraud. It is charged under the Crimes Act and the Secret Commissions Act 1910.

While corruption can be considered a form of fraud, in the context of financial crime that this briefing is concerned with, one can occur without the other. However, law enforcement and public sector prevention and detection responses increasingly target fraud and corruption collectively, on the basis that improved systems will reduce instances of either occurring. Experience tells us that in many instances they overlap – fraud may be committed to fund corruption activity, or corrupt practices are enabled by fraudulent activity.

What is fraud costing us?

While financial losses to fraud and corruption are widely believed to be in the hundreds of millions of dollars, there is no agreed measure and accurately assessing the scale of the problem presents challenges.

Fraud and corruption are inherently hidden crimes and widely considered to be under-reported. New Zealand often relies on estimates, although these estimates vary. The abstract cost, such as the damage to the trust and integrity placed in our institutions, is even more difficult to measure.

An estimate of losses:

- **$601 million to $12.97 billion** (estimated) taxpayer dollars lost to fraud and error (including corruption) each year in New Zealand[3]
- New Zealand consumers **lost $194.3 million to fraud** (including scams) 1 October 2022 to 30 September 2023[4]
- Companies globally are thought to lose 5% of their annual revenue due to fraud – or about **$5 trillion USD** every year[5]

Quite apart from financial losses, fraud can cause significant physical and mental health harm to individual victims and their communities.

On an individual level, people impacted by fraud report feelings of shame, anxiety, depression, relationship deterioration, and even a lack of trust in the financial and other institutions meant to protect against these crimes. Victims may be less willing to invest, start a business or take constructive financial risks.[6] These effects are often felt by entire families, extending lifetimes and even generations.

In times of economic difficulty these effects may be magnified. The exposure of major frauds during the 2008 Global Financial Crisis, for example, had an enduring negative impact on public trust in the finance sector.

Corruption independent of fraud is even more difficult to measure, and New Zealand lacks a concrete estimate on its scale. Measuring its cost in dollar terms fails to paint an accurate picture, as corrupt actions involving even a small amount of money can have severe and lasting consequences.

Private sector corruption can result in inflated prices and unfair competition. While companies might gain individual short-term benefits, the fallout from scandals can be wide-reaching. In the long run, higher levels of corporate integrity lead to stronger commercial performance.[7]

Corruption is a key enabler of transnational and serious organised crime, facilitating the introduction of crime groups into society and helping them influence decision-making processes.[8] A European study found two thirds of criminals use corruption on a regular basis, and more than 80% of criminal networks in Europe use legal business structures.

The harm caused by individual acts of bribery or corruption can have wide-reaching impacts. A corruptly awarded infrastructure, building or roading contract can have wide scale health and safety implications to whole communities, if it means a contract is awarded to a sub-qualified party. More broadly, corruption is corrosive to trust and confidence in public institutions. Even very low levels of bribery can drastically impact public corruption perceptions, and complacency can have steep consequences.

Transparency International's *Corruption Perceptions Index* (CPI) is one of the most utilised corruption measures. Through a range of assessments, countries are rated from 0 (most corrupt) to 100 (least corrupt). This is a measure of corruption *perception* and does not literally capture all corruption occurring in a nation.

New Zealand has seen a slow decline in its CPI rating. Although we remain one of the top-rated countries on the index, our position has slipped from first equal in 2019 to fourth in 2024, and we are not immune to corruption. For example, the SFO estimates around 30-40% of its current caseload involves allegations of corruption and it recently successfully prosecuted New Zealand's largest corruption case to date. In May 2025 former IT contractors and Australian citizens Mark Lester and Sean Bryan were sentenced to prison after admitting to their offending. While employed by Spark, New Zealand's largest telecommunications and digital services provider, Mr Lester ensured more than $20 million in contract work was awarded to Mr Bryan's company Victory IT. In exchange he received around $4.1 million in kickbacks.

CASE STUDY: Corruption threatens community wellbeing

The direct impact of corruption on the wellbeing of a community was demonstrated in an SFO case brought to trial in 2022. The local body corruption case included bribes being paid in exchange for being awarded council contracts, as well as the sharing of confidential information and advice around tenders. Two offenders were found guilty and sentenced to prison. A third pleaded guilty and was sentenced to home detention.

Contracts affected by the corrupt offending included upgrading the Kumara and Whataroa Water Treatment Plants which was awarded to Techno Economic Services (TES) NZ. The company's sole director was an Auckland cake decorator with no relevant background experience.

A contract to build a multi-million-dollar Wastewater Treatment Plant at Franz Josef was awarded to Techno Economic Services (TES India). This project did not go ahead and was subsequently subject to an enquiry by the Auditor-General.

CASE STUDY: Volkswagen Emission Scandal

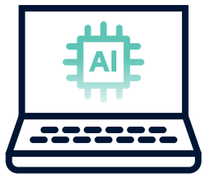
In 2015, the US Environmental Protection Agency found that some Volkswagen cars sold in America had a 'defeat device' – software that could detect when a car was being tested for carbon emissions and cheat the test, by changing the performance to improve the results.

This was an intentional long-term deception aimed at cheating pollution regulations to boost profit, potentially resulting in 1200 premature deaths. The company faced steep consequences. They were forced to refit many diesel vehicles and suffered a significant stock price drop. In 2018 former CEO Martin Winterkorn was indicted on fraud and conspiracy charges. As of 2020, the scandal had cost Volkswagen €30.1 billion in fines and settlements.

Beyond the immediate financial cost, the scandal drove concerns about greenwashing, which undermined corporate sustainability initiatives and ultimately reduced the premium consumers were willing to pay for 'green' products.

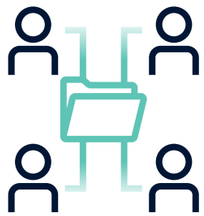
The evolving landscape: Key trends in fraud and corruption detection

Advancing technology, open borders, societal shifts and growing distrust are shaping a fraud landscape which is in constant motion, necessitating a dynamic and adaptive approach to detection. Key trends include:



Technological arms race:

Increased sophistication and artificial intelligence



Collaboration and information sharing:

A critical imperative

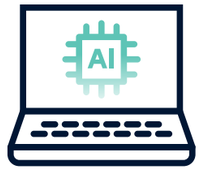
Data and analytics:

Understanding the problem

The human element:

Psychological and behavioural insights

Technological arms race: Increased sophistication and artificial intelligence



The increased digitisation of our everyday lives, particularly in the aftermath of the COVID-19 pandemic, contributed to a massive growth in fraud. Now we are grappling with an additional complication: the rise of artificial intelligence (AI).

Fraudsters are increasingly leveraging advanced technologies such as AI and large language models to create more sophisticated and widespread fraudulent schemes, including highly convincing phishing attacks and deepfake identities. These AI-driven scams are a significant driver of fraud growth in New Zealand and comparable nations.[9]

Advances in AI have made it easier for less sophisticated actors to create convincing attacks, increasing the potential harm. Further, sophisticated actors involved in complex financial crime are employing AI and machine learning not just to commit fraud and corruption but also to avoid detection, including by obscuring identities, transaction patterns, hiding illicit funds, and manipulating large financial datasets to mask irregularities. Beyond its direct impact as a tool for offending, it's possible AI may have broader implications – for example, new AI-driven systems in workplaces may introduce new vulnerabilities for exploitation.

The international counter fraud community has seen an influx of bad actors providing 'fraud as a service', where scammers empower other less technically skilled people to commit fraud, or enable fraud to be committed in increasingly sophisticated and professional ways. AI and the dark web have made this significantly easier, and encrypted communication applications like Telegram mean fraud as a service is often difficult for government agencies to detect.[10]

Technological advancements also present challenges for law enforcement agencies when investigating and prosecuting fraud cases. The volume of information that needs to be analysed in fraud cases has grown exponentially in the digital era. The United Kingdom (UK) is currently carrying out a review of fraud and disclosure in the context of technological changes. Part one of the review, Disclosure in the Digital Age,[11] looked at the proliferation of digital evidence investigators now face and what changes these necessitate in its disclosure regime.

Part two of the independent review was launched in April 2025, with a focus on the greatest challenges faced in bringing criminals committing fraud offences to justice. This includes ensuring that investigators have the skills, tools and powers needed to pursue leads, review case material and share relevant data, both privately and publicly; and evaluating if fraud offences and the Fraud Act 2006 can keep pace with modern offending.

The findings in part one of the review suggested that while technology is putting pressure on the disclosure regime, technological developments should also provide solutions.

> "... we should not be afraid to fight fire with fire. The same technology that supercharged the proliferation of digital material may well provide, at least in part, a panacea for the difficulties we presently find ourselves in."
>
> **Jonathan Fisher KC, March 2025, Disclosure in the Digital Age**

This theme is mirrored in other areas – for example, AI-powered detection tools are being developed to analyse vast datasets, identify subtle anomalies, and uncover hidden patterns indicative of fraud and corruption. Meta-analysis of 47 studies suggests that AI-powered fraud detection systems achieve detection rates of 87-94%, with a 40-60% reduction in false positives compared to traditional rule-based methods.[12] Financial institutions have reported an increase in detecting financial crimes since implementing AI for this purpose.

Law enforcement agencies, including the New Zealand SFO, are also increasingly harnessing AI to improve the efficiency and capability of their detection and investigation processes, such as to refine large amounts of evidence. Agencies like the SFO are investing in building the digital literacy and analytical skills of their personnel, ensuring they can effectively utilise these technologies.

Establishing frameworks for the safe and rapid testing of innovative solutions is crucial as there are pitfalls associated with the advances in technology that law enforcement must be alive to, as identified in the Disclosure in Digital Age report:[13]

> Improper use of technology may lead to the overlooking of relevant material and increase the chance for a miscarriage of justice. It is therefore important to look at this technology as an instrument to aid officers in discharging their duties. It must not diminish from their accountability over the process.

Technological advancement has also led to increased use of cryptocurrencies in fraud, complicating traditional financial tracking and detection. Expertise and tools for tracing and analysing cryptocurrency transactions are becoming essential, although these are often costly. Collaborative efforts to pool knowledge and resources in this area are being explored.

The SFO works with organisations like the International Association of Computer Investigative Specialists to provide training to other domestic and international law enforcement agencies. These initiatives provide a platform to both share expertise and learn from partners to support cross-government efforts to combat fraud and corruption.

Collaboration and information sharing: A critical imperative

Collaborative approaches are becoming increasingly critical as countries recognise the importance of intelligence sharing, including through public-private partnerships.

Traditional detection methods, sometimes restricted by traditional country borders, are less effective against more advanced techniques and necessitate increased coordination, collaboration and information sharing by law enforcement agencies. Detection efforts will rely more heavily on shared intelligence and coordinated analysis across different entities and jurisdictions.

Singapore, for example, has adopted a centralised approach by integrating various counter fraud investigation and response units under a single umbrella, the Anti-Scam Command, established in 2022. The Command prioritises public-private collaboration and has expanded its partnerships to include over 90 institutions, comprising mostly of banks and finance companies. They facilitate the swift freezing of accounts to allow the recovery of victim funds. As part of their collaboration efforts ASCom has worked with banks to co-locate their staff within ASCom premises, saying this enhances real-time coordination with police in investigative efforts, tracing the flow of funds, and freezing bank accounts.

In the first half of 2023, the Anti-Scam Command froze more than 9000 accounts based on reports referred to them, resulting in the recovery of over $50 million.[14]

Singapore's response is in part due to privacy and information sharing settings that are more permissible than those found in the New Zealand context, both between private institutions (such as banks and other financial institutions) and between private and public sector institutions. These systems and processes are still evolving – in 2023, Singapore's Parliament passed the Financial Services and Markets (Amendment) Act, which sought to further improve information sharing for the purposes of combating money laundering and the financing of terrorism. This Act has created the legal framework for financial institutions to share customer data and risk information through a secure digital platform.[15] Secure platforms for sharing financial and corruption-related intelligence enable faster detection and more coordinated action.

Singapore's centralised approach has learnings for jurisdictions like New Zealand, many of which have a decentralised model with multiple agencies responsible for detecting and investigating fraud and corruption in their mandated area.

Canada has adopted a single-point-of-entry reporting model, which simplifies the reporting process and improves intelligence gathering. The Canadian Anti-Fraud Centre (CAFC), originally established in 1993 to combat deceptive practices in telemarketing has evolved into a single point of entry to which individual and enterprise victims of fraud can report offending. In 2021, the CAFC recovered $3.35 million in victim funds by partnering with police and other relevant agencies.[16] The CAFC also undertakes comprehensive prevention activities which aim to reduce total victimhood.

The CAFC maintains intelligence on fraud and identity crime, and engages in disruption activities by assisting agencies to freeze assets. It has also been tasked with building a new National Cybercrime and Fraud Reporting System in partnership with other agencies.

In most cases of fraud and corruption, financial transactions through banks and other financial institutions are highly relevant to any investigation, meaning private sector entities often hold key data relevant to law enforcement's enquiries. While these institutions are compelled to provide information in response to the use of law enforcement powers or other legislative requirements, such as under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, gathering sufficient intelligence to meet emerging threats will nonetheless require ongoing public-private partnerships, both formal and informal.

Since banks are often the first place fraud victims report their losses, real-time collaboration between fraud investigators and law enforcement will be crucial. Centralised reporting hubs like the CAFC make it simpler for private businesses to interact with enforcement agencies and report offending, in turn providing a broader intelligence picture for assessing risks and threats. In New Zealand there are some existing public-private initiatives, like the Police-led Financial Crime Prevention Network, which sees law enforcement partner with major banks. However there remains scope for further partnerships, especially in the prevention and education space.

Data and analytics: Understanding the problem

A collaborative approach and improved reporting ensure agencies are armed with the comprehensive data and advanced analytical capabilities necessary to understand the evolving patterns of fraud.

Future strategies will likely integrate detection mechanisms more closely with preventative measures. By leveraging data to identify vulnerabilities and understand how fraud and corruption occur, organisations can implement more effective preventative controls, reducing the need for reactive detection efforts.

Moving beyond reactive detection, the focus will likely shift towards more proactive and predictive analytics. By identifying risk factors and potential areas of vulnerability, organisations (including law enforcement) can anticipate and prevent fraud and corruption before they occur. Critically, law enforcement will need to ensure that challenges associated with big data such as data quality, false positives, adaptability and scalability and ethical considerations are mitigated.

A growing trend involves integrating fraud detection with proactive prevention strategies, using insights from past cases to design more resilient systems. The UK's Public Sector Fraud Authority and Australia's Commonwealth

Fraud Prevention Centre exemplify this integrated approach, using data analytics and behavioural science to inform both detection and prevention efforts. The New Zealand SFO has also established a Counter Fraud Centre and in 2024 brought it together under a single manager in a Detection and Prevention Unit.

However, there will always be a need for a robust approach to investigating and prosecuting fraud and corruption to effectively deter criminal activity, and data is important to the better targeting of detection efforts.

As historically under-reported, hidden crimes, gathering accurate data can be a challenge. Agencies, industry, and the public often have different understandings of what fraud and corruption are. Fraud is more likely to happen in organisations where people are not aware of what it is, are unable to spot the signs of where it might be happening, or do not know what to do if they see something suspicious.

Similarly, while it's widely accepted that hundreds of millions of dollars are lost each year to fraud in New Zealand, there is no agreed measure of the cost. New Zealand often relies on estimates to assess the harm caused by fraud, although these estimates vary. This can be confusing for the public and make it difficult for policy makers to both assess the scale of the problem and evaluate the success of prevention measures.

In order to better understand the scale of the issue, countries including the UK and Australia have moved to introduce mandatory reporting of public sector fraud (including corruption) in their jurisdictions. This ensures the timely collection of crucial intelligence, enabling more targeted allocation of resources for detection, prevention, and enforcement. Examples of this include the UK's National Fraud Initiative, which mandates data matching across government bodies. This initiative has been successful in identifying a significant number of fraudulent claims and errors, leading to substantial recoveries of public funds.[17]

Australia requires mandatory reporting of fraud and corruption within the public sector at both a state and federal level, and has established AS 8001:2021, *Fraud and corruption control*, as a baseline to measure systems maturity. The Queensland Audit Office (QAO) requires government entities to report losses of greater than $500, or if the agency suspects it may be due to fraud. The QAO considers reported losses at the entity level (as part of its financial audit process) and on a collective public sector basis to understand emerging risks. It has developed a public sector fraud maturity tool which state agencies can use to assess and enhance fraud prevention and detection measures.

On a nation-wide level, an annual fraud census is run by the Australian Institute of Criminology on behalf of the Attorney-General's Commonwealth Fraud Prevention Centre. The Commonwealth Fraud Control Framework requires non-commercial public entities complete the fraud census, which is used to derive insights and inform policy making based on accurate information.

The human element: Psychological and behavioural insights

While technology, collaboration and data are critical to a dynamic fraud response, understanding the psychological and behavioural factors that contribute to both perpetrating and falling victim to fraud remains important for developing effective detection and prevention strategies.

Recognising the role of insiders, many countries are strengthening whistleblower protections and considering financial incentives. Studies indicate that whistleblower tips are the most effective method of detecting fraud, uncovering 43% of occupational frauds, more than three times the rate of internal audits.[18] For small nations, enabling whistleblowers to remain anonymous is essential, since many people who spot wrongdoing fail to come forward for fear of retaliation. Transparency International's Global Corruption Barometer found that in 2016, the most common reason that citizens did not report corruption was fear of consequences.[19]

The European Union in 2019 published a Whistleblowing Directive White Paper, which introduced minimum standards for whistleblower frameworks maintained by member states. This included a new system to protect and encourage reporting of breaches of EU law, more choices for whistleblower reporting channels, and safeguards against reprisals from employers. Denmark was the first EU country to implement the directive into national law. Denmark is regarded as a low corruption nation and scores similarly to New Zealand in many international indexes, however still faces challenges. Research indicates Danish public servants have become increasingly concerned about reporting wrongdoing in the workplace since 2008, citing career consequences as the main reason for remaining silent.[20]

New Zealand has made some changes in this area, replacing its Protected Disclosures Act 2000 with the Protected Disclosures (Protection of Whistleblowers) Act 2022 which introduced some strengthened protections. The Organisation for Economic Co-operation and Development recognised this as "among New Zealand's most important reforms in recent years and increases the potential to detect foreign bribery".[21] In May 2025, the NZ SFO launched a campaign targeting foreign bribery, including piloting a new online platform to support safe, anonymous reporting. The fully encrypted platform allows SFO investigators to communicate with whistleblowers. It mirrors tools already in use by other regulators and is configured to meet the highest possible settings for privacy and data security.

Some countries are going a step further and providing or considering the benefits of financial incentives for whistleblowers. This could significantly enhance detection, particularly in complex cases. The US Securities and Exchange Commission's Whistleblower Program has paid out billions of dollars in rewards to individuals who have provided high-quality information leading to successful enforcement actions. In fiscal year 2020 alone, whistleblower-initiated cases brought in over US$1.6 billion in False Claims Act settlements and judgments.[22] This has inspired similar frameworks in Canada, where whistleblowers have helped the Government collect millions of dollars in cases of international tax evasion and aggressive tax avoidance.[23]

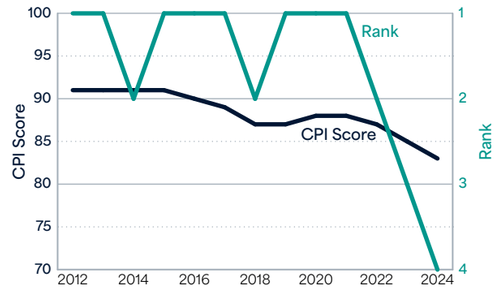
Incentivising whistleblowers to come forward is one of the key issues being considered in the UK's independent review. The UK SFO has been vocal in its support of such a measure, noting that supporting whistleblowers to come forward 'has the potential to speed up our cases, bring in more money for the taxpayer and deliver justice for victims more effectively.'[24] In his maiden speech, the UK SFO Chief Executive Nick Ephgrave endorsed paying whistleblowers, noting the $2.2 billion recovered by the US Department of Justice from whistleblower-driven civil settlements.[25]

In some cases companies are also being incentivised to self-report fraud and corruption by the availability of deferred prosecution agreements (DPAs). These involve companies reaching an agreement, where the prosecutor agrees to defer any prosecution in return for the company meeting certain requirements or conditions, such as the payment of penalties, improving compliance and cooperation. DPAs are used in the UK, for example in R v Entain[26] where the online sports betting giant accepted £615 million in penalties after it was investigated for failing to prevent bribery. In April 2025 the UK SFO issued new corporate guidance in relation to corporate criminal offending, which confirms that if a corporate self-reports promptly and cooperates fully, it will be invited to negotiate a DPA.[27] This removes previous uncertainty for corporates and their advisors as to the consequences of early self-reporting. The use of DPAs in New Zealand would need to be carefully considered with regard to existing prosecution practices, case law and their impact on the interests of justice.

Building public confidence through strong enforcement is also crucial to increase the likelihood of whistleblowers coming forward.

Nations around the globe are having to contend with growing mistrust and inequality, as well as perceptions that society is becoming more corrupt. This includes New Zealand, which has seen a slow decline in its Corruption Perceptions Index rating over recent years. This perception not only erodes confidence in institutions, but through apathy also disenfranchises citizens from taking steps to report corruption when it occurs.

New Zealand CPI Score since 2012



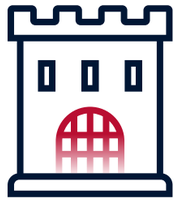
Growing economic pressures are also impacting fraud growth globally. Desperation is a powerful motivator and during recessionary periods, opportunistic lapses in process combined with financial strain can drive regular citizens to commit acts of fraud. The NZ SFO was established in 1990 in response to the 1987 share market collapse and ensuing economic recession, which exposed fraud on a scale not previously seen in New Zealand.

Understanding what drives people to commit fraud and corruption can help power detection and prevention initiatives. For example, evidence shows traits like high levels of extrinsic motivation and ambition, a sense of entitlement, compulsive lying and the desire to maintain a false image of success can all be associated with fraud. Prevention-focused organisations like the NZ SFO's Counter Fraud Centre draw on this knowledge to educate public sector agencies about common fraudster personas and red flags they can be alert to in their organisation, increasing detection capabilities.

What's ahead? Three possible futures for New Zealand

This briefing captures a snapshot of global trends shaping both how and why fraud is committed, and its detection. As financial crime and corruption evolve, small, developed nations like New Zealand face growing risks. For illustrative purposes we have explored three possible future scenarios, each considering different responses to the challenges of increasing fraud and corruption.

For the purposes of this briefing we have adopted a 25-year timeframe, allowing us to effectively consider systemic risks, emerging technologies, and structural shifts in how fraud and corruption may evolve. While some of the more profound risks - such as the erosion of public trust, institutional capture, or high-level corruption - often unfold over longer periods, there are also nearer-term red flags to be alert to, including politicised appointments, increased secrecy of information, concentrated lobbying and declining media freedom.



The digital fortress

A global leader in anti-fraud and corruption innovation

A best-case scenario

The shadow economy

Corruption creeps in

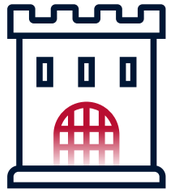
A middle-ground scenario

The captured state

A nation compromised

A worst-case scenario

The digital fortress: A global leader in anti-fraud and corruption innovation



A best-case scenario

By 2050, New Zealand has become one of the most digitally secure nations in the world.

After a series of high-profile financial scandals and cyberattacks targeting its banking and public sectors, the Government invests heavily in regulatory technology, AI-driven fraud and corruption detection and transparency measures.

A real-time national fraud monitoring system flags suspicious financial transactions across the public and private sectors before they escalate. A transparency drive mandates all businesses to use blockchain-verified accounting, preventing money laundering and financial manipulation. Biometric verification and AI-driven behavioural analysis make identity fraud nearly impossible with predictive analysis modelling.

Public trust in institutions soars as strict anti-corruption laws, whistleblower protections and incentives, and automated (and mandated) government audits creates engagement, lifts awareness and capability to identify red flags and prevent and disrupt criminals – while ensuring robust protection of citizens' rights. New Zealand reclaims the top position in international anti-corruption rankings and international organisations, such as the OECD, hold New Zealand up as a model for tackling fraud and corruption. As other nations struggle with fraud and corruption, New Zealand becomes a global hub for quality investment and transparent governance, attracting international businesses looking for a secure financial environment.

Key outcomes

- Very low levels of financial crime due to AI-powered detection
- Strong public trust in government and institutions
- New Zealand becomes the hardest place in the world for serious and organised crime to occur
- We enjoy a thriving economy as ethical businesses relocate to New Zealand

The shadow economy: Corruption creeps in

A middle-ground scenario

By 2050, New Zealand's clean reputation is under strain.

Global cybercriminals and organised transnational fraud networks target its financial sector, exploiting regulatory blind spots in cryptocurrency and digital assets. The hidden economy, made up of undeclared, untaxable transactions, grows. Loopholes in corporate ownership laws allow offshore shell companies to launder billions through the country.

At the same time, corporate lobbying and political donations become less transparent, leading to quiet but growing concerns about regulatory capture. Despite some use of AI-driven fraud detection systems, resource constraints and the inability of enforcement agencies to keep pace with the technology and methodologies being applied by criminals allows fraud and corruption to occur beneath the surface.

As a result, public trust in institutions declines, but successive governments resist major reforms, fearing economic repercussions. New Zealand remains one of the world's least corrupt nations but continues its slow slide in international rankings. Organisations like the OECD become increasingly critical of its commitment to tackling fraud and corruption.

Key outcomes

- Moderately effective fraud controls, but loopholes remain
- Public trust declines, but democratic institutions remain intact
- Serious and organised crime takes a stronger foothold across both public and private sectors
- New Zealand still has economic stability, though reputational risks deter some foreign investment

The captured state: A nation compromised

A worst-case scenario

By 2050, New Zealand's once-pristine reputation for transparency is in ruins.

Sophisticated organised crime networks, cybercriminals, and corrupt actors have infiltrated its financial, public service and political systems leading to distrust and polarisation. Cryptocurrency scams driven by deepfake endorsements, fraudulent shell companies, and high-level corporate corruption run unchecked, turning the country into an offshore haven for illicit money flows.

New Zealand falls prey to foreign interference, as authoritarian regimes exert influence through hidden donations, backdoor deals, and soft power strategies. Public institutions are weakened by regulatory capture, where lawmakers are indirectly controlled by corporate and foreign interests. Whistleblowers attempting to expose corruption face serious intimidation or legal threats.

The country becomes a hub for fraud and financial secrecy interwoven with corrupt practices, similar to past tax havens. International bodies like the Financial Action Task Force (FATF) place New Zealand on a "grey list," leading to sanctions and capital flight. New Zealand plummets down international anti-corruption rankings, and organisations such as the OECD use it as a warning example to other countries. Public protests erupt as faith in democracy collapses, but with institutions compromised, reversing course becomes nearly impossible.

Key outcomes

- Widespread corruption undermines government
- Economic decline as foreign investors pull out of the New Zealand market
- Serious and organised crime groups operate with near impunity
- New Zealand experiences rising civil unrest as public trust erodes

Findings: Turning challenges into opportunities

These three scenarios outline starkly different paths. They are not predictions but possible futures. While New Zealand's strong institutions give it the potential to become a global leader in anti-fraud and corruption measures, inaction or weak detection and enforcement could allow corruption to take root.

The SFO and other New Zealand agencies with a responsibility for tackling fraud and corruption have a keen eye on technological developments and an increasingly collaborative approach to information sharing and enforcement. However, the problem continues to grow and it is crucial we get ahead of the curve.

To steer toward the digital fortress scenario and prevent the risks of a captured state, New Zealand can learn from the initiatives adopted in other jurisdictions, some examples of which (not exhaustive) are highlighted below.

Canada

- Centralised, single point of entry for reporting fraud
- Whistleblower payment scheme

United States of America

- Whistleblower payments
- Government Accountability Office publishing estimates of federal government fraud losses
- FraudNet hotline for reports of fraud, waste, abuse, or mismanagement of federal funds

United Kingdom

- Increasing focus on data sharing and partnerships
- Exploring reimbursement for whistleblowers
- Reviewing legislation and processes to ensure they are fit for the modern age
- Established counter fraud profession
- Establishing single-entry reporting system
- Deferred prosecution agreements

Europe

- European Union's Whistleblowing Directive

Singapore

- Centralised Anti-Scam Command
- Increasing information sharing between public and private entities

Australia

- Mandatory reporting through annual fraud census
- Minimum requirements set around detecting and deterring offending
- Queensland requires reporting of public sector losses in excess of $500
- Established National Anti-Corruption Commission

New Zealand

- Strengthened whistleblowing anonymity including foreign bribery reporting campaign
- Trialling mandatory public sector reporting
- Exploring opportunities for AI-driven investigative tools and AI-integrated evidence management platforms

Finding: Reducing the effort to report fraud enhances detection

Despite being the most common offence type in New Zealand, fraud (including scams) is the least reported.[28]

Several barriers have been identified to reporting. Victims are often unsure where to report offending and tend to notify their banks instead of law enforcement. There is also scepticism around whether agencies can help them recover their losses.[29]

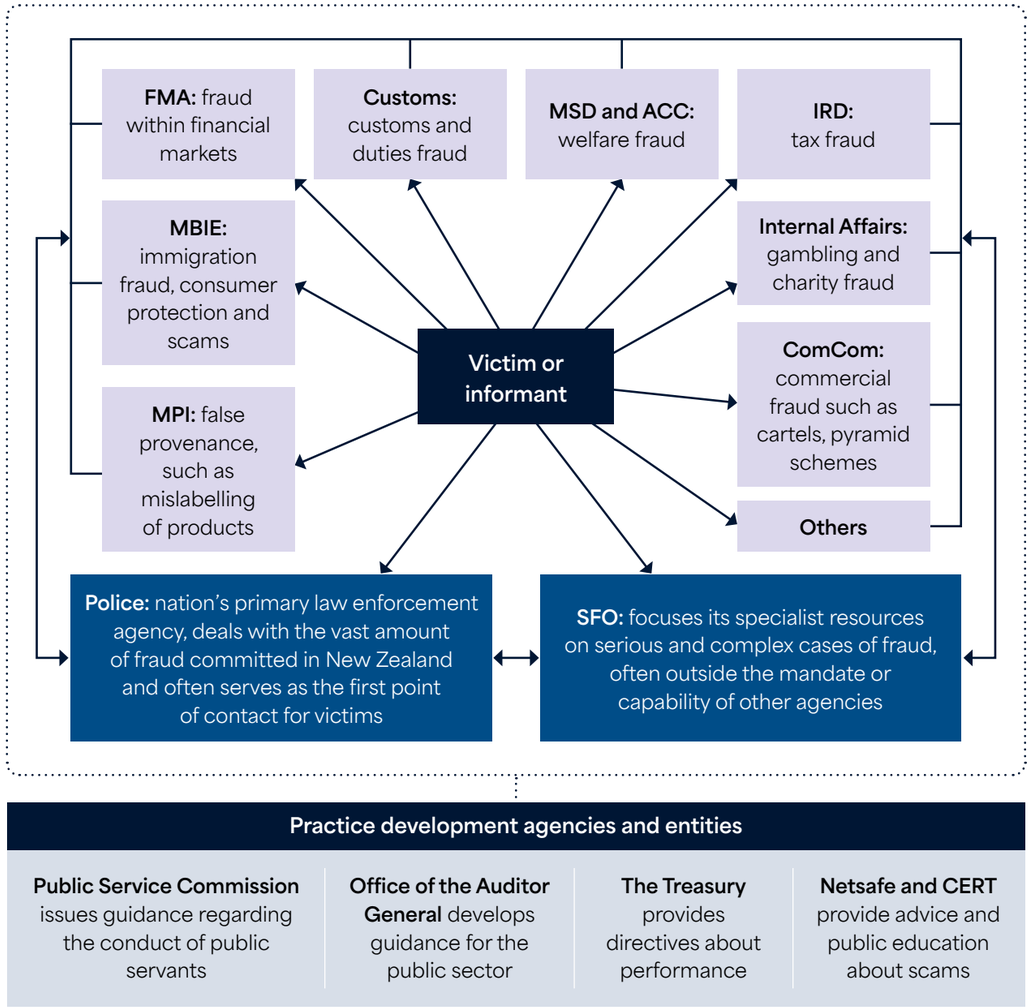
Like our international partners, New Zealand has a multi-agency counter fraud model with a range of agencies responding to fraud. Many agencies investigate offending within their mandated area (both fraud and non-fraud) while Police and the SFO respond to fraud across industries, with the specialist capabilities of the SFO focused on the more serious and complex end of offending.

This model allows agencies to leverage their specific expertise and resources to tackle the broad array of fraud occurring. For example, the Serious Fraud Office Act 1990 provides the SFO with wide-ranging investigative powers. It was considered important that these powers be confined to the investigation and prosecution of only the most serious and complex financial crime.

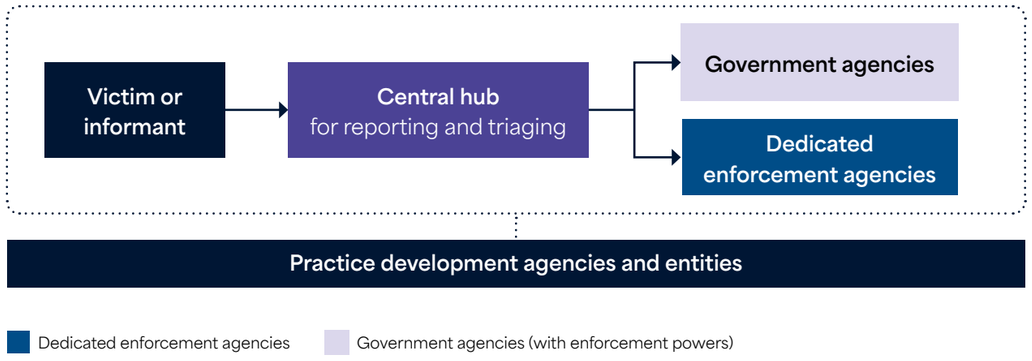
However, the multi-agency model can lead to confusion and duplication for both victims and investigators. To counter this, nations including Singapore and Canada have implemented or are exploring some form of no wrong door or single point of entry reporting, which offer streamlined access to services. No wrong door models typically refer to a system where victims receive assistance no matter which organisation they contact within the model; while single point of entry models establish a central hub for reporting and triaging reports of fraud and corruption. Using this model, a victim does not need to worry about which agency is most suitable to receive their complaint, nor do they have to make multiple complaints to various agencies.

There is a growing need to facilitate secure and efficient information sharing, both between government agencies within a jurisdiction, and across borders. This includes platforms enabling financial institutions to share customer data to combat money laundering and terrorism financing (as in Singapore) which can also aid in broader fraud detection. Working on improved information sharing systems and developing real-time intervention capacity could help empower future progress towards a single point of entry model. Streamlining the reporting process will also assist in gathering data to understand the scale of the problem and where best to focus detection efforts.

Multi-agency model (current)



Single point of entry model



Finding: Impetus for change comes from understanding the scale of the problem

As explored in this briefing, New Zealand lacks a clear picture of what is lost to fraud and corruption each year.

Data is drawn from reported losses, extrapolation from representative samples, and international modelling (extrapolation from a non-representative sample). All of these methods have their limitations, but underestimating the scale of the problem by using only reported losses is a poor option for fraud and corruption. Both are historically underreported crimes, and policy makers need to have a benchmark of how much fraud is occurring to both tailor their interventions and measure the effectiveness of detection and prevention activities.

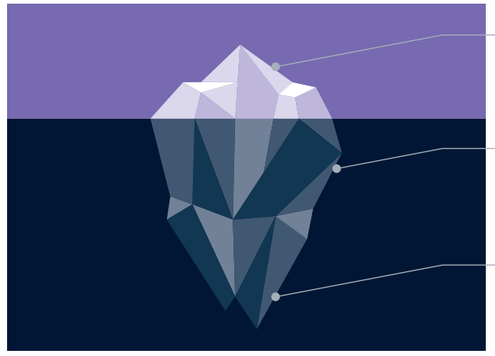
In the public sector alone, losses to fraud and error could be in the billions. In 2021, the United Kingdom Government Counter Fraud Function carried out a desktop review of the New Zealand system. The report concluded that New Zealand likely loses between $601 million to $12.97 billion per year in public funds due to fraud and error, including corruption.[30] Areas of government expenditure noted as being particularly vulnerable to fraud and corruption included the health, education and welfare sectors. Disaster relief and emergency management funds are also vulnerable due to the need for grants to be distributed rapidly.[31]

Currently the New Zealand public sector has no requirement to report on fraud losses. A lack of insight into the issue means agencies are unable to meaningfully intervene at a system level, understand where to focus detection and prevention activities or assess their effectiveness. Additionally, a fundamental shift is underway towards leveraging the power of data analytics to identify indicators of fraud and corruption. This involves employing sophisticated analytical techniques to uncover complex schemes and patterns that traditional methods might miss. The increasing availability of data and advancements in analytical tools is driving this trend.

The data used to inform detection and prevention activities could be improved through public sector fraud reporting models, which assess both the maturity of agency level counter fraud initiatives and measure the total amount of detected and suspected fraud loss.

The SFO in July 2025 launched a new pilot programme which aims to improve intelligence on the scale of corruption and fraud in the public sector, and uplift the sector's resilience against these risks. The pilot will use a representative selection of government agencies to undertake an assessment of their fraud and corruption control environment, including a measure to report the amount and volume of offending that agencies detect, prevent or recover funds from.

A New Zealand fraud and corruption control standard, modelled on the Australian Standard AS 8001:2021, *Fraud and corruption control,* could help organisations to easily demonstrate conformance with best practice and develop a clearer understanding of their fraud losses. AS 8001:2021 is used as a baseline to measure systems maturity. This Standard includes minimum requirements across a range of measures aimed at detecting and deterring offending. This standard, set in 2008, was updated in 2021 to include additional requirements around information systems security and updated guidance on whistleblower protections.



Detected fraud: There is currently no agreed figure for detected fraud in the New Zealand public sector.

Estimated fraud: Just below the surface, government estimates of losses are based on unique modelling in each agency.

Unknown fraud: Deep below the surface is the unknown – thought to be potentially billions of dollars.

Finding: The innovation race – technology creates novel threats and opportunities to counter them

The increasing use of digital platforms and cryptocurrencies in illicit activities necessitates the development of advanced digital forensics capabilities.

The ability to trace and analyse cryptocurrency transactions is becoming increasingly vital for detecting and prosecuting financial crime, including fraud and corruption.

AI is also supercharging existing fraud risks, making it easier for criminals to deceive the public en masse, and with increasing levels of sophistication. In response, the deployment of AI-powered tools for detection is becoming critical. These tools can analyse vast datasets, identify subtle anomalies, and detect patterns indicative of fraudulent or corrupt activities that might escape traditional methods.

While such technology can also boost detection capabilities and enhance investigative efficiency, they can be cost-prohibitive, particularly in a resource-constrained environment. Public-private partnerships could enable agencies to leverage the unique data and technological capabilities of the private sector alongside the investigative and enforcement powers of public agencies.

The proliferation of digital information available also creates challenges for law enforcement. Stakeholders will need to ensure their data and analysis functions are fit for purpose and have sufficient capacity to process larger volumes of relevant information.

Countries such as the UK are updating their legislation to ensure law enforcement can continue to operate effectively in the wake of massive technological change. As agencies increasingly look to harness technology for detection and investigation, this may also have implications as courts consider the use of such tools.

Finding: Informants and whistleblowers are crucial pieces in the detection toolkit

Since informants are a primary pathway to detecting fraud and corruption offending, many countries and international bodies have prioritised the strengthening of whistleblower legislation, particularly around protecting whistleblowers.

New Zealand has a small population with fewer employment opportunities, especially in niche fields. This means the ability of whistleblowers to remain anonymous is of increased importance, especially in foreign bribery cases where retaliation can be more difficult to prevent. Some changes have been made in recent years to strengthen protections, however there is scope to do more, such as exploring new technology and platforms to ensure truly anonymous reporting.

Our international scan highlighted that several partner nations also have incentivised whistleblowing through payment schemes, often with several bespoke programs run by different agencies. Such schemes are effective because:

- They bring in revenue – since whistleblowers are only compensated a portion of the funds recovered. This may be of specific interest in a fiscally constrained environment.
- They generate viable leads – in the US, informants are the primary source of corruption cases, meanwhile, in Canada, the Offshore Tax Informant Program has generated over 500 leads since 2020.[32]
- They compensate whistleblowers for risk – weak whistleblower protections are often identified as a major barrier to fraud and corruption reporting. The state has limited ways to protect whistleblowers from professional reprisals.

Finding: Detecting corruption requires specialist expertise

As explored in this briefing, the distinction between actions people consider corrupt, actions of unfair practice, and explicit criminal offending is often not well understood.

Corruption's existence in grey areas also makes it more difficult to detect. While fraud may be picked up through internal controls or tracing funds, corruption often exists in relationships between individuals and evidence may not always be readily accessible.

In New Zealand, corruption cases are primarily the remit of the SFO and Police. Corruption is a key focus for the SFO and makes up approximately 40% of its caseload.

Recognising the importance of specialist expertise and the necessary toolkits, including enabling legislation in detecting corruption, some international jurisdictions have, or are creating, standalone bodies with the remit to focus on corruption. Examples include Australia's National Anti-Corruption Commission, Singapore's Corrupt Practices Investigation Bureau and the UK's International Anti-Corruption Coordination Centre.

There have been calls from some advocates for a greater focus on addressing corruption in New Zealand, including through creating a new specialist agency. A May 2025 report from the Ministerial Advisory Group on Transnational, Serious and Organised Crime (TSOC MAG) suggested a central authority was necessary to manage system-wide corruption risks in New Zealand. The report recommended this either be an existing agency, such as the Public Service Commission, Police or SFO, or a new entity.[33] A 2024 report released by Transparency International (TINZ) called for the Government to appoint and appropriately fund an agency (suggesting it could be the SFO, Ministry of Justice or Public Service Commission) with responsibility for anti-corruption monitoring, coordination, research and strategic operations.[34]

Given the limited availability of specialist skills and resources required to investigate this type of offending, and New Zealand's relatively small operating environment, establishing a new agency may not be feasible. Empowering and mandating an existing agency with responsibility for addressing corruption could provide a better fit for the New Zealand setting.

> "Despite New Zealand's longstanding reputation for integrity, mounting evidence from multiple agencies consulted during this review indicates a growing concern: corruption and insider threats are increasing, and parts of the system are falling behind this evolving threat."
>
> TSOC MAG, *Corruption in New Zealand and the Pacific*

> "This is a wakeup call. Our low level of corruption in New Zealand is a key asset from which we all benefit. We are not protecting it against rising corruption within and outside New Zealand."
>
> **Debbie Gee, Deputy Chair of Transparency International New Zealand**

With corruption evidence often contained within communication between individuals, it is also key that legislation keeps pace with the digital era and the range of devices which may be involved in modern corruption offending. Advances in technology afford greater opportunities for concealment, with offenders able to reduce their chances of detection including through use of cryptocurrencies, encrypted communications and cloud data. The UK, for example, is currently conducting a review which is considering challenges faced by fraud investigators in the digital age.

> "... when the Criminal Procedure and Investigations Act 1996 (CPIA) was introduced, few would have predicted quite how swiftly and pervasively technology would enter almost every area of our lives. With this rise in technology also came the proliferation of digital material, stored in myriad formats and locations such as phones, laptops, smartwatches, and the cloud, to name just a few."
>
> **Jonathan Fisher KC**
> **Disclosure in the Digital Age**

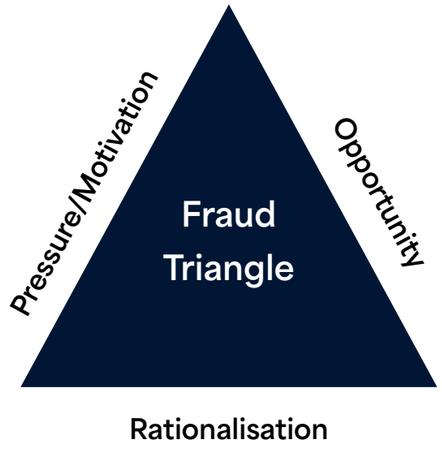
Finding: Understanding human psychology helps us detect fraud and corruption

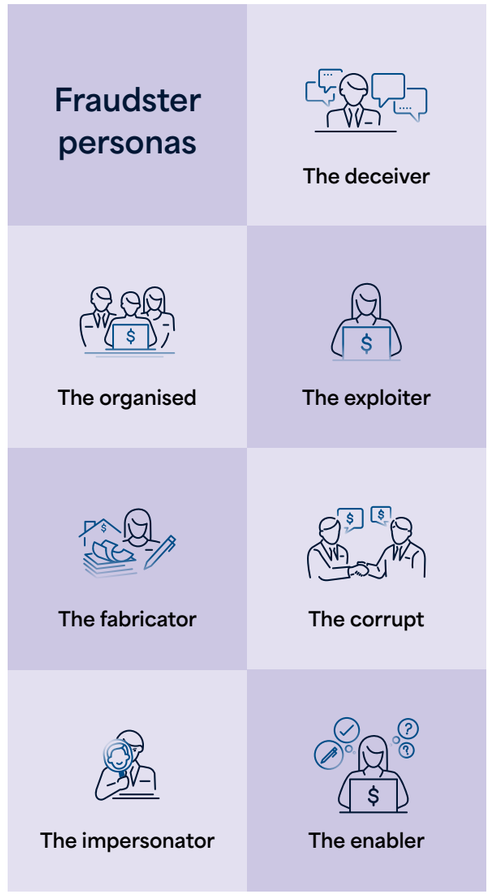
Technological advances have significantly impacted the prevalence and complexity of fraud, and those looking to commit fraud may seize on the opportunity they present. However there are other underlying drivers behind offending to consider, particularly in the corporate or public sector environment.

The fraud triangle is a popular tool used by practitioners to highlight person-level drivers for fraud. This tool highlights that two of the key drivers come down to psychological factors: pressure or motivation (impacted by personality traits like greed propensity) and rationalisation (the internalised justification for offending). These two factors cannot be directly controlled by organisations, whose fraud control systems primarily reduce the opportunity component of the triangle. Technological changes create opportunities for fraudsters but have a limited impact on the motivation or rationale.

Our understanding of the factors that motivate people to commit fraudulent acts is evolving. 'Love of money' or high extrinsic motivation makes individuals more likely to commit fraud offences. Recent research suggests that it is easier to identify these individuals during employment screening or internal company investigations than previously thought, because such individuals freely disclose their acquisitive nature, seeing it as a hallmark of success and employability.[35] While ambition can be a healthy motivator, this finding suggests that more focus on an individual's motivation is required in fraud-vulnerable activities. Further, despite academic debate over their practical value, corporate ethical frameworks appear to have a genuine dampening effect of fraud offending, even in areas of work (for example sales) that attracts a disproportionate number of extrinsically motivated employees.

As they keep abreast of emerging technological trends, domestic agencies should also prioritise utilising the latest psychological insights. The SFO's Counter Fraud Centre, which works with public sector agencies to improve their fraud detection and prevention capability, creates resources using insights gathered from its own operations as well as through its connections with international partners. These include helping agencies to identify eight common fraudster personas, or common archetypes for financial crime offenders. The personas outline the most common methods fraudsters use and can aide in awareness and prevention work.





Conclusion

New Zealand has long been viewed as a country with low levels of corruption and high levels of integrity, and this has a direct impact on our quality of life. However as we have explored in this briefing, our wellbeing is threatened by the explosion of fraud being experienced around the world. This landscape is dynamic and ever-changing, with sophisticated tools being employed in a technological arm race between good and bad actors.

Continuing to effectively detect fraud and corruption in the face of these evolving forces is key to protecting the wellbeing of our people. Detection disrupts harmful behaviour, prevents further damage and demonstrates to others that it will not be tolerated in our society.

During our consultation process, we received feedback from government agencies and several key stakeholders including the New Zealand Institute of Directors and Chartered Accountants Australia and New Zealand, alongside academics. This feedback highlighted the intersections between fraud, corruption and the hidden economy, as well as highlighting the role good governance plays in creating a speak-up culture. Thank you to all our agency and community partners who participated in both rounds of consultation.

Strategic opportunities are being explored or implemented by other countries which could further enhance our detection capabilities and may be worthy of further exploration.

- Fighting fire with fire by investing in new technology to detect and investigate fraud and corruption, while simultaneously upskilling those on the frontline and modernising our legislation to ensure its effectiveness.
- Improving reporting of fraud by streamlining the process for victims, ensuring the anonymity of whistleblowers and offering incentives for them to come forward.
- Enhancing focus on data and analytics, enabling a proactive and predictive approach to fraud detection.
- Improving data sharing and collaboration between private and public bodies, enabling fast and accurate detection of fraud and ensuring everyone is equipped with the tools necessary for a co-ordinated and dynamic approach.
- Equipping businesses and the public sector with the tools needed to recognise drivers of fraud, red flags within their organisations and how to strengthen their internal controls.

End notes

1 Office of the Auditor General (n.d) *The Basics* https://oag.parliament.nz/good-practice/fraud

2 Yazbek, Philippa / The Helen Clark Foundation (2023) *Shining a Light: Improving Transparency in New Zealand's political and governance systems* https://helenclark.foundation/publications-and-medias/shining-a-light/

3 UK Government Counter Fraud Function, (2021) *New Zealand Serious Fraud Office Counter Fraud Centre: Fraud Loss in the New Zealand Public Sector* https://www.sfo.govt.nz/assets/UKGCFF-NZ-Fraud-Evidence-Base-December-2021.pdf

4 Banking Ombudsman: Scammers sophisticated deception costing consumers $194 million dollars a year https://bankomb.org.nz/about-us/media-releases/2024-media-releases

5 Association of Certified Fraud Examiners (ACFE) (2024) *Occupational Fraud 2024: A Report to the Nations* https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

6 Johannes Hagen, Amedeus Malisa (2022) *Financial fraud and individual investment behavior*, Journal of Economic Behavior & Organization (Volume 203). See: https://www.sciencedirect.com/science/article/pii/S0167268122003390

7 United Nations Office on Drugs and Crime, (n.d) *Consequences of Private Sector Corruption*. See: https://www.unodc.org/e4j/ru/anti-corruption/module-5/key-issues/consequences-of-private-sector-corruption.html

8 European Commission: *Corruption in organised crime*. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/anti-corruption/corruption-organised-crime

9 Watson, M (2025) *AI-fuelled scams & phishing soar in New Zealand, says Gen*. See: https://securitybrief.co.nz/story/ai-fuelled-scams-phishing-soar-in-new-zealand-says-gen

10 Revolut (2025) *Scammers Shifting to 'Secure' Encrypted Apps WhatsApp & Telegram, Reports Revolut; Meta Still Biggest Overall Source of Scams*. See: https://www.revolut.com/en-NZ/news/scammers_shifting_to_secure_encrypted_apps_whatsapp_telegram_reports_revolut_meta_still_biggest_overall_source_of_scams/

11 Jonathan Fisher KC (March 2025) *Disclosure in the Digital Age*. See: https://www.gov.uk/government/publications/independent-review-of-disclosure-and-fraud-offences/disclosure-in-the-digital-age-independent-review-of-disclosure-and-fraud-offences-accessible

12 Olowu et al (2024) *AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity*. See: https://www.researchgate.net/publication/386276951_AI-driven_fraud_detection_in_banking_A_systematic_review_of_data_science_approaches_to_enhancing_cybersecurity

13 https://www.gov.uk/government/publications/independent-review-of-disclosure-and-fraud-offences/disclosure-in-the-digital-age-independent-review-of-disclosure-and-fraud-offences-accessible

14 Singapore Ministry of Digital Development and Information (January 2024) *Measures to protect Singaporeans against online scams*. See: https://www.mddi.gov.sg/media-centre/press-releases/measures-to-protect-singaporeans-against-online-scams/

15 Allen & Gledhill (2024) Financial services and markets amendment act 2023 establishing platform to facilitate sharing customer information among FIs to combat money laundering and terrorism financing in force. See: https://www.allenandgledhill.com/sg/publication/articles/27958/financial-services-and-markets-amendment-act-2023-establishing-platform-to-facilitate-sharing-customer-information-among-fis-to-combat-money-laundering-and-terrorism-financing-in-force

16 Canadian Anti-Fraud Centre (2022) *Canadian Anti-Fraud Centre Annual Report 2022*. See: https://publications.gc.ca/collections/collection_2024/grc-rcmp/PS61-46-2022-eng.pdf

17 UK Government. National Fraud Initiative case studies. See https://www.gov.uk/government/publications/national-fraud-initiative-case-studies

18 ACFE Occupational Fraud 2024: A report to the nations. See https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

19 ConsumerProtection (2024), *Kiwis lose $194 million to scams*. See: https://www.consumerprotection.govt.nz/news-and-media/kiwis-lose-184-million-to-scams

20 Transparency International (2018) *Denmark: Overview of corruption and anti corruption*. See: https://knowledgehub.transparency.org/assets/uploads/helpdesk/Country-profile-Denmark-2018_PR.pdf

21 OECD (2024). https://www.oecd.org/en/about/news/press-releases/2024/12/new-zealand-must-strengthen-foreign-bribery-detection-and-its-corporate-liability-framework-for-foreign-bribery-says-the-oecd-working-group-on-bribery.html

22 National Whistleblower Centre (n.d) *Why whistleblowing works*. See: https://www.whistleblowers.org/why-whistleblowing-works/#:~:text=In%20Fiscal%20Year%202020%20alone%2C%20whistleblower%2Dinitiated%20cases,$840%20million%20being%20awarded%20to%-20whistleblowers%20who

23 https://www.whistleblowers.org/canada-whistleblower-reward-laws/

24 UK Serious Fraud Office (2025). https://www.linkedin.com/posts/uksfo_independent-review-of-disclosure-and-fraud-activity-7320455559437053952-WkWd?utm_source=share&utm_medium=member_ios&rcm=ACoAAAmcciUBRqUVvMHPtBG6XN_v2hZF35sUSpg

25 Serious Fraud Office and Nick Ephgrave QPM, *Director Ephgrave's speech* at RUSI 13 February 2024. See: https://www.gov.uk/government/speeches/director-ephgraves-speech-at-rusi-13-february-2024#:~:text=In%20summary%2C%20under%20my%20leadership,we%20gather%20at%20the%20outset

26 https://www.cps.gov.uk/sites/default/files/documents/publications/R%20v%20Entain%20DPA%20summary%20of%20judgment.pdf

27 UK Serious Fraud Office (2025). *SFO External Guidance on Corporate Co-Operation and Enforcement in relation to Corporate Criminal Offending*. See https://www.gov.uk/government/publications/sfo-corporate-guidance/sfo-corporate-guidance

28 Ministry of Justice (2024), *New Zealand Crime and Victims Survey Published*.
See: https://www.justice.govt.nz/about/news-and-media/news/new-zealand-crime-and-victims-survey-published-june-2024/#:~:text=%E2%80%9CLast%20year%20we%20reported%20a,common%20offence%20in%20New%20Zealand.%E2%80%9D

29 Serious Fraud Office (2023) - *NCFCS Victims Survey response: Citizens Advice Bureau*

30 UK Government Counter Fraud Function (2021). *Fraud Loss in the New Zealand Public Sector.*
See https://www.sfo.govt.nz/assets/UKGCFF-NZ-Fraud-Evidence-Base-December-2021.pdf

31 SFO Counter Fraud Centre (May 2023) *Preventing Fraud in Times of Crisis*
https://www.sfo.govt.nz/assets/Uploads/Counter-Fraud-Centre-Portal-Docs/CFC-Resources/Fraud-Prevention-in-Times-of-Crisis-/Preventing-Fraud-in-Times-of-Crises.pdf

32 Artello & Albanse (2020), *Rising to the Surface - Detecting Public Corruption*, Criminology, Criminal Justice, Law & Society

33 Ministerial Advisory Group on Transnational, Serious and Organised Crime (May 2025). *Corruption in New Zealand and the Pacific.* See https://www.customs.govt.nz/media/fdziwfmf/tsoc-mag-25-03-final-corruption-and-the-pacific.pdf

34 Dr Simon Chapple (2024). *An assessment of the effectiveness of anti-corruption institutions in New Zealand in deterring, detecting and exposing corruption*. See https://www.transparency.org.nz/blog/the-effectiveness-of-anti-corruption-institutions-in-new-zealand

35 Li-Ping, et al (2016), *Monetary Intelligence and Behavioural Economics: The Enron Effect - Love of Money, Corporate Ethical Values, Corruption Perceptions Index (CPI), and Dishonesty Across 31 Geopolitical Entities*, Journal of Business Ethics

Serious Fraud Office
Te Tari Hara Tāware

PO Box 7124
Victoria Street West
Auckland 1141
New Zealand

www.sfo.govt.nz

October 2025
ISBN 978-0-473-75059-6 (online)

SFO
SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Te Kāwanatanga o Aotearoa
New Zealand Government