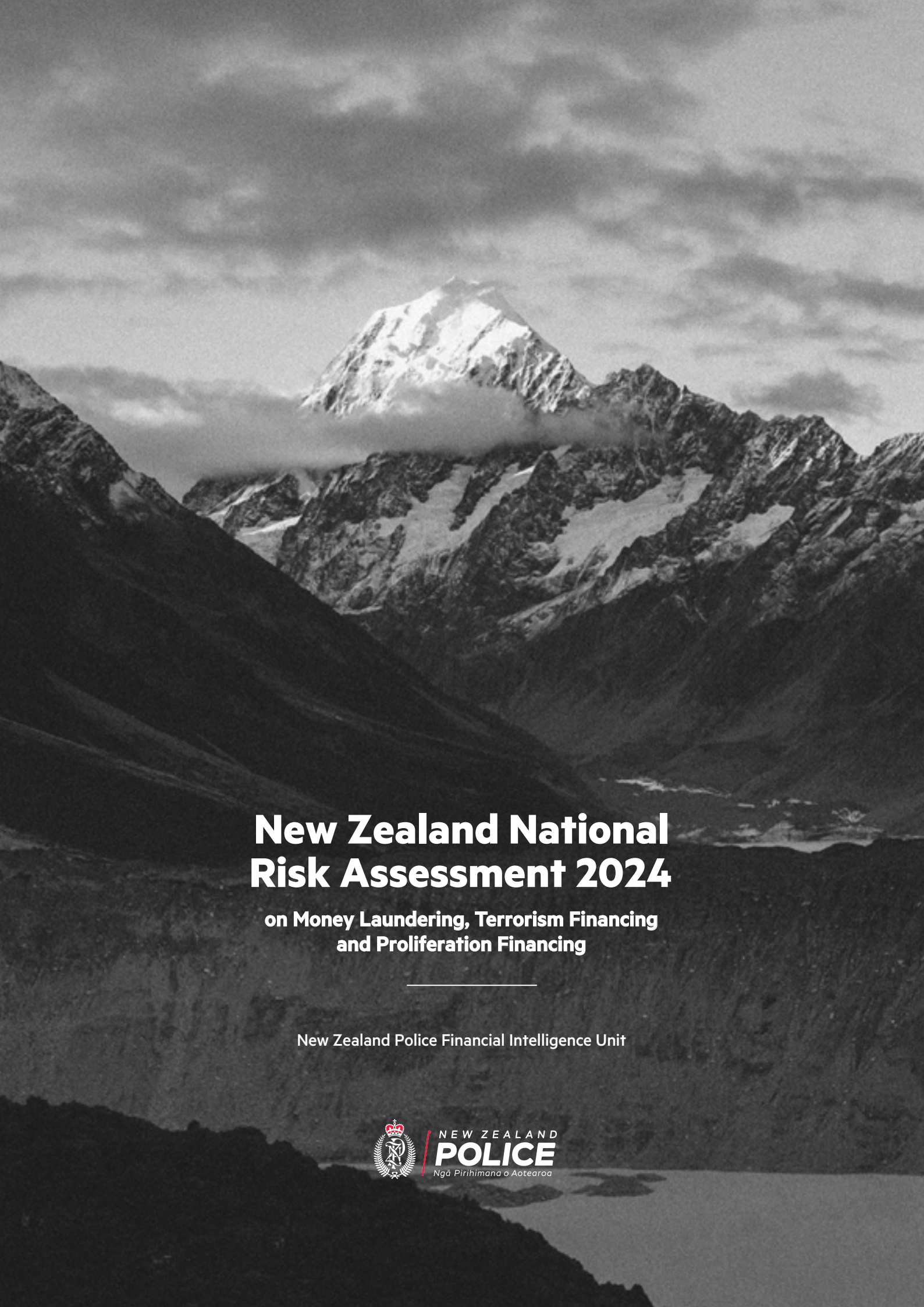


New Zealand National Risk Assessment 2024

on Money Laundering, Terrorism Financing and Proliferation Financing

New Zealand Police Financial Intelligence Unit

NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

Foreword

Through an effective AML/CFT system we can improve the well-being of New Zealanders. This occurs firstly by maintaining integrity of our financial system, and secondly by ensuring our financial system is hostile to crime. This NRA builds on the 2019 NRA and informs all stakeholders across the AML/CFT community of the contemporary risk. Understanding risk is critical to the effectiveness and resilience of our AML/CFT system, allowing us to respond directly to risk and to maximise the benefits of improved safety and security to our financial system and our communities.

This NRA updates and describes the significant criminal behaviours generating illicit income that threatens New Zealand's financial system. It also assesses and identifies the vulnerabilities within our financial system that criminals are taking advantage of when they launder proceeds of crime. There are some key changes to risk from both a crime threat perspective and within the various parts of New Zealand's financial system.

This NRA identifies that fraud-related crime, drug crime and transnational money laundering currently expose New Zealand's AML/CFT system to the highest threat. The occurrence of fraud is accelerating, with both 'defrauding' and the subsequent 'laundering' occurring within the financial system. For this reason, the banking sector remains highly vulnerable to money laundering along with any sector that offers services and products enabling movement of proceeds out or into New Zealand. These sectors include the Money or Value Transfer Service (MVTS), sectors offering remittance service – or more commonly referred to as 'money remitters' – and virtual assets service providers (VASPs).

Transnational money laundering occurs when foreign generated proceeds of crime are transferred into New Zealand's economy, or when a New Zealand formed legal structure is misused for money laundering purposes. The designated non-financial business and profession (DNFBP) sectors, including the trust and company service provider (TCSP) sector, are vulnerable to risk associated with the laundering of foreign generated illicit wealth. Criminals are innovative in how they attempt hide and conceal illicit wealth. These sectors, and all other reporting sectors must remain alert to the threat from foreign criminals who may look to misuse our country and damage our international reputation in their efforts to launder proceeds of crime.

With respect to drug crime, our country has a significant problem. Methamphetamine, in particular, is a significant driver of harm. Many within our AML/CFT community will be aware of the damage this drug can cause within families. Money is the vulnerability for this type of criminal behaviour in that much of our methamphetamine is imported, which requires payment being made offshore. If we harden the environment and prevent payment through a highly vigilant and responsive AML/CFT system, we help make New Zealand a harder place for criminals to do business. As an AML/CFT community we therefore all have an opportunity to directly contribute to the safety of our families, friends and communities; in addition, we can improve economic wellbeing.

This NRA also includes our first assessment of proliferation financing (PF) risk. Proliferation financing activities refers to the raising and moving of funds to finance the development of weapons of mass destruction. The international community has agreed to combat the proliferation of these dangerous weapons by aggressively countering the ability to finance their development. This is a global collective responsibility. It is recognised that no financial system in the world is immune to being misused for avoiding sanctions and disguising funds ultimately used to finance these weapons.

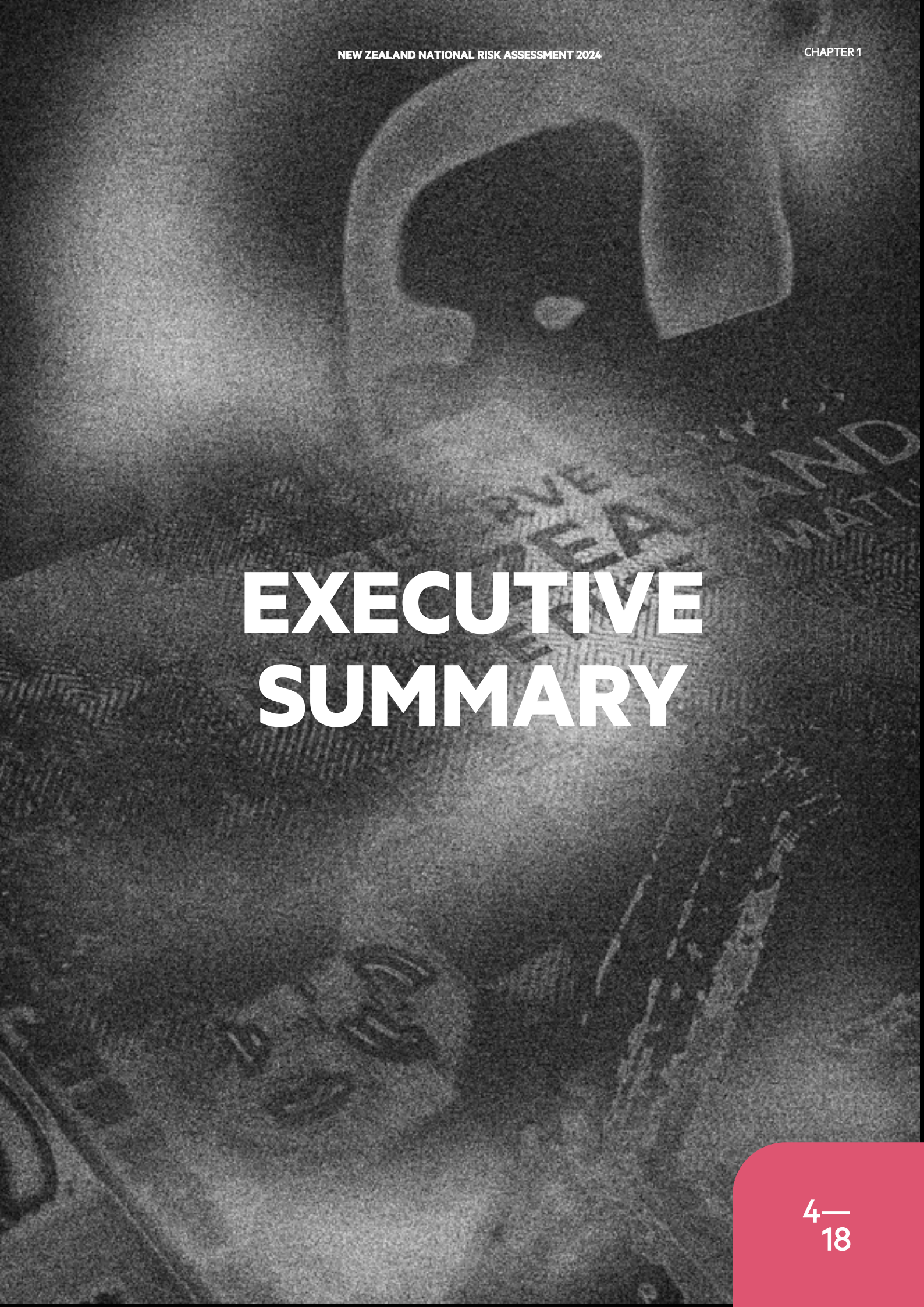
Although this NRA identifies that New Zealand is not considered 'high-risk' with regards to PF, it also acknowledges that our economy is well-integrated and connected to the global financial system so as a country we must remain vigilant to PF. We must ensure our financial system is not misused to fund the development and manufacture of weapons that threaten global safety and security.

Finally, this NRA relies on a range of sources – in particular, information from reporting entities across New Zealand. The successes we have had in detecting, preventing and responding to criminal behaviour are often directly a result of the intelligence we receive from the reporting community. For this reason, on behalf of your families, friends and all New Zealanders, I take this opportunity to thank you for the important contributions you make and continue to make to improve the safety and security of our communities.

Dave Lynch
Director Financial Crime Group

CONTENTS

Click a tab to skip to chapter →



EXECUTIVE SUMMARY

This 2024 NRA consists of two broad assessments: the assessment of threat, and a sectoral vulnerability assessment. It discusses how these assessments influence money laundering risk, terrorism financing risk and proliferation financing risk in New Zealand.

1. THREAT ASSESSMENT

An appreciation of current crime types, within the AML/CFT landscape domestically and globally, that pose a ML/TF/PF threat to New Zealand. This assessment has been undertaken through profiling criminal behaviours and considers the effectiveness of anti-money laundering / financing of terrorism enforcement measures in addressing AML/CFT risk related to those criminal behaviours.

2. SECTORAL VULNERABILITY ASSESSMENT

Each sector has been profiled to assess vulnerabilities of the products and services offered by reporting entities (in the financial and non-financial sectors) to ML/TF/PF. This assessment considers these sectors' inherent characteristics, and how these sectors can be exploited by criminals to undertake criminal activities. These assessments also review reporting from the sectors and consider how this reporting features in money laundering investigations.

Key Findings of the NRA

This NRA's findings provide critical understanding of current risk. They provide the critical foundation for informing reporting entities (REs) on contemporary risk, and the development of sectoral risk assessments. This NRA also informs the effectiveness of measures implemented as a result of the 2019 NRA.

Risk understanding should provide input into the design and development of national and institutional AML/CFT policies; deployment of supervisory measures and resources; and the co-ordination and deployment of enforcement response measures.

HIGH-RISK CRIME

- Fraud, inclusive of frauds against the government and cyber-enabled fraud
- Dealing in drugs
- Transnational money laundering: the movement of illicit wealth across our borders

OTHER NOTABLE CRIMES

- Tax-related offending – related to non-compliance with New Zealand's tax system
- Property crime: including vehicle theft, burglary, and retail crime

HIGH-RISK SECTORS

- Banks
- MVTS (sectors offering remittance services)*
- VASPs (Virtual Asset Service Providers)

SECTORS ABUSED FOR HIGH-RISK CRIMES – facilitating transfer or placement of proceeds of crime.

- Real estate sector
- High value dealers
- Casinos
- Law firms and accounting practices
- NBDT (Non-Bank Deposit Takers) to a lesser extent

* Money Value Transfer Services (MVTS), often referred to as the remittance sector, provide services of money or value transfer.

Threat risk assessment: key highlights

The threat risk assessment has profiled: likely significant predicate money laundering crimes, potential terrorism financing, and proliferation financing activities that threaten our AML/CFT system.

Money Laundering (ML)

Predicate crimes are those that are a component of another criminal activity. In money laundering, predicate crimes are the criminal activities from which illicit income is derived and which a person then 'deals with' for the purpose of laundering. Crime profiles were developed using quantitative and qualitative data on inherent risk and the effectiveness of our current control measures to determine current and projected risk.

All crimes generating income present risk; however, a key focus of a national risk assessment is to inform on current risk. From this, response, policies, and strategies can be developed to make the greatest difference in preventing money laundering, terrorism financing and proliferation financing. Hence, there is a focus on current high-threat criminal behaviours in this NRA. Risk ratings emerge into three categories: most risk, lesser risk, and low-risk. 'Most risk' emerges from high-volume and high-value crimes that therefore have high threat to our system, while 'low-risk' relates to crimes with low frequency and low value.

Fraud (which includes different types of fraud), illicit drug supply, and the laundering of proceeds from crimes that have occurred in foreign jurisdictions (foreign-generated illicit wealth) are the most prevalent and highest-value crime threats currently. The highest-volume crimes are fraud and drug-related offending. There is currently an elevated risk of fraud, compared to the 2019 NRA, due to technology exposing New Zealanders to higher volumes of scams and frauds.

Lower ML risk is observed in a range of other crime types, including: proceeds generated because of non-compliance with New Zealand's tax system, and property-related crime. Although the occurrence of these crime types might be significant, the value and severity associated with the laundering of the proceeds of these crime types is less than fraud, drug-related offending and transnational money laundering.

Terrorism Financing (TF)

The challenges with detecting TF in New Zealand's context are: detecting low-volume, low-value transactions; that these transactions are often ambiguous, funded through family or legitimate activities; and the overall environment of low terror threat in our country. Despite the current low threat, in the last five years New Zealand has had two terrorist attacks – both by self-funded lone actors. The world has become increasingly connected, allowing individuals in New Zealand to engage online with offshore groups and become radicalised through the exchange of ideas on extremist forums.

The ease of transferring funds offshore – through banking, remittance, and cryptocurrencies – allows sympathisers and supporters in New Zealand to effortlessly finance, and donate to, offshore groups with extreme views. Banking, MVTS and the VASP sector were identified as sectors most likely to be misused to finance terrorism offshore. These sectors will remain attractive to individuals intending to support offshore terrorist groups as they provide fast and easily accessible methods of international funds transfer.

Given the prevalence of transnational fraud and drug crime, it must be considered that foreign-based criminal activities and the remittance of related criminal proceeds could indirectly benefit foreign terrorist organisations. The existence of a strong and resilient AML system responding to domestic crime in New Zealand could also support the global efforts to counter terrorism.

The threat outlook for New Zealand will likely largely remain the same, with lone actors continuing to be the main concern. International events will continue to impact New Zealand with individuals supporting various causes offshore – including groups with extreme views. Vigilance and awareness are critical given the consequences of terrorist acts.

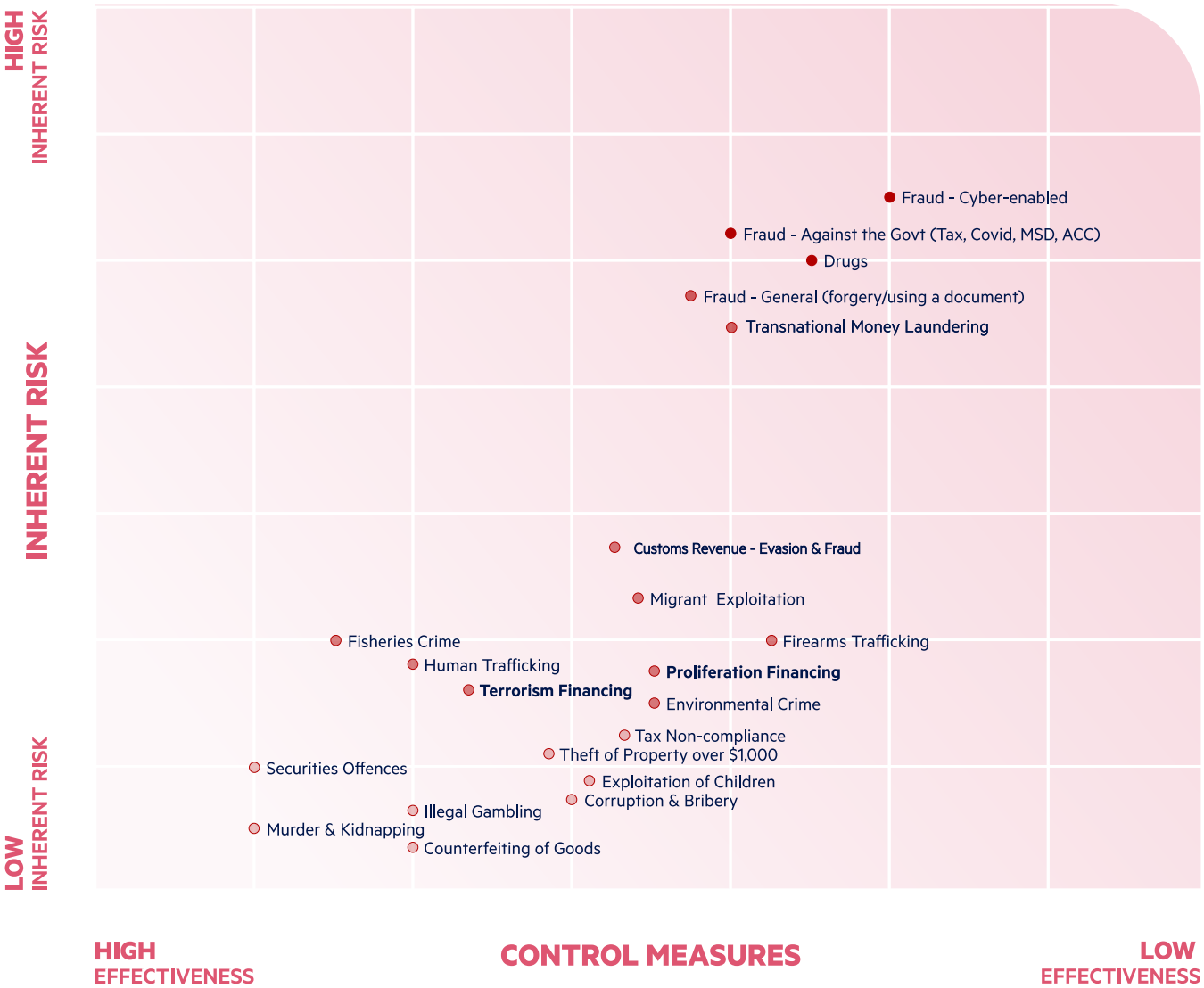
Proliferation Financing(PF)

PF risk largely emanates from the Democratic People's Republic of Korea (North Korea or the DPRK) and Iran. Criminals from these countries are known to conduct a range of crimes, including complex cyber-enabled frauds, to derive income – this NRA recognises the increasing prevalence of this type of offending targeting New Zealand.

The assessment of PF risk also includes an assessment of potential breaches, non-implementation, and the evasion of targeted financial sanctions[1] within the New Zealand system. Cyber attacks, and the misuse of corporate structures and legal arrangements, are the most significant vulnerabilities to proliferation financing. New Zealand's risk also lies in the transfers to intermediary jurisdictions that are sympathetic to North Korea and Iran.

The banking, remittance and VASP sectors are vulnerable to proliferation financiers as they provide methods for transferring funds internationally. Despite these being the three sectors with the highest vulnerabilities, the PF risk assessment concludes their PF risk as likely low. However, it identifies that improved understanding of risk across all reporting entities is a requirement.

Graph 1: *Inherent Risk – Control Measures.*



1. The term 'targeted financial sanctions' means both asset freezing and prohibitions to prevent funds or other assets from being made available directly or indirectly for the benefit of designated persons or entities.

High-risk crimes/crime threats

FRAUD

The New Zealand Government experiences the highest rate of fraud in New Zealand. This includes tax-related fraud, Covid-19 fraud, and welfare-related fraud.

Recent crime surveys suggest one in ten New Zealanders have been the victim of a fraud or scam.

All New Zealanders and New Zealand businesses who purchase insurance are impacted by insurance fraud.

'Low-value/high-volume' fraud facilitated by offshore criminals evades the prescribed transaction reporting framework. It is challenging to detect and identify these transactions as they can move between domestic banks – before they are transferred offshore.

DRUGS

New Zealand has a high demand for illicit drugs.

New Zealanders are willing to pay some of the highest prices in the world for illicit drugs; therefore, our market remains highly attractive to transnational organised crime groups, and the associated domestic criminal enterprise.

Organised crime and gangs operate extensively across New Zealand to distribute drugs across our communities.

The networks that control drug supply include importers, those who also manufacture, wholesale distributers and retail dealers.

This crime type is cash-intensive. Ultimately, some revenue is remitted offshore to pay for the importations that are distributed throughout every community across New Zealand.

FOREIGN PREDICATE CRIME

Offshore-generated proceeds have been introduced to the New Zealand economy. These involve low-volume but very high-value laundering.

It is recognised that cross-border movement of criminal proceeds affords those proceeds some degree of protection and criminals are taking advantage of the challenges that countries experience when working cross-border to investigate illicit wealth.

New Zealand should be recognised as a country where AML/CFT systems will detect, investigate and confiscate foreign-generated illicit wealth when it enters our economy.

Other notable behaviours/crimes

PROPERTY CRIME

Property-related crime (vehicle theft, burglary, ram raids) is widespread and common. Although high-volume in contrast to fraud and drug-related crime, the value of funds generated that could be subject to laundering is lower.

TAX NON-COMPLIANCE

Non-compliance with New Zealand's tax regime is discrete from tax-related fraud.

Submitting a return that misrepresents income or contains untruthful information for financial advantage is a fraud.

Criminals do not declare illicit income for tax purposes – this is a non-compliance issue and not a fraud.

Establishing whether income is unreported legitimate income or proceeds of criminal behaviour is challenging. An effective AML/CFT system will detect illicit income; some may be undeclared and untaxed legitimate income. All possible illicit income should be reported for the most appropriate response.

Key Threat Drivers:

Drivers of ML/TF and PF include the use of cash, mule banking facilities, and facilitators who enable movement of money domestically and internationally. Using nominees to obscure source, purpose, and beneficial ownership of illicit wealth is a practice by organised crime to launder illicit wealth. Technology is another key enabler for criminal enterprise – enabling both predicate crime and the related laundering of proceeds.

GAMBLING

Although not high-value, criminals involved in both drug and fraud offending actively participate in gambling domestically and via online gambling sites.

GANGS AND ORGANISED CRIME

Organised crime and syndication of criminal enterprise, in the domestic and international environments, enables criminal enterprise. This generates illicit wealth threatening the financial system.

DOMESTIC DEMAND FOR ILLICIT DRUGS

Demand drives supply which drives transnational remittance of both profit and payment for supply.

CASH

Cash affords anonymity. Cash is a critical feature within the criminal economy. Cash is introduced into the financial system and 'used', or converted into high-value property. The ability to move cash between the illicit economy and the legitimate economy is both an enabler and driver of both predicate crime and money laundering.

BUSINESSES OFFERING SERVICES AND PRODUCTS OUTSIDE OF THE REGULATED SECTORS

As improved compliance and regulation occurs, opportunities for underground sectors will emerge. An effective system will identify persons and businesses providing unregulated financial services.

CHANGING ECONOMIC CONDITIONS AND THE PROSPECT OF FINANCIAL HARDSHIP

These may encourage risky financial behaviours. Scam investment schemes offering high short-term returns may be more attractive to those currently suffering financial pressure or hardship. Participation in criminal behaviour or permitting criminals to use third party bank accounts (exploitation of mule accounts) to enable money laundering could be influenced by current economic conditions.

TECHNOLOGY – the use of technology to reach people and businesses who then become victims of fraud:

This was accelerated due to the Covid-19 pandemic. Increasing use and availability of technology increases exposure to foreign criminals. Technology enables communication between criminals, and the transfer of funds (domestically and internationally) – which drives the expansion of fraud-related criminal enterprise.

WIRE TRANSFERS – that enable the movement of funds offshore:

When crime is rewarding and foreign criminals receive benefit, expansion of enterprise is fueled. This environment drives increased risk.

Sectoral vulnerabilities in New Zealand

The NRA assessed 35 sectors, including banks, money remitters, virtual asset service providers, the DNFBP sectors (law firms and conveyancers, accounting firms, real estate agents and trust and company service providers, known as professional gatekeepers), issuers of securities, currency exchange service providers, and derivative issuers.

The sectors most vulnerable to exploitation by threat actors in New Zealand were assessed to be banking, money or value transfer service (MVTS) providers, and VASPs.

Trust and company service providers (TCSPs), lawyers, real estate agents, high-value dealers, accountants, NBDTs and casinos were all identified as being misused by criminals to launder proceeds of crime.

Each sector's inherent risk is mitigated by: control measures assessed through the quality SAR reporting, the levels of AML/CFT compliance, and the levels of client monitoring.

It is aggravated by threat characteristics such as: offender capability, confiscation value associated with the sector, and use of the sector by criminals for money laundering activity. Table 1 illustrates inherent risk, the impact of control measures and overall risk across sectors considered most vulnerable in New Zealand.

Sector size

The banking sector is highly vulnerable because of high exposure to proceeds generated through the high-threat crime types. Almost all fraud (where victims' funds are transferred to offenders) occurs within the banking system. This sector is colossal in contrast to the other recognised higher-risk sectors and is complex due to its broad range of products and services.

Domestically, cash is a characteristic of drug crime. Typically, this cash is laundered when it enters the banking system, either directly or via the Designated Non-Financial Businesses and Professions (DNFBP) or Non-bank Deposit Takers (NBDT) sectors. Wire transfers typically enable cross-border transfer of proceeds associated with fraud and drug dealing, and the inwards movement of illicit wealth to the New Zealand financial system. Also impacting on risk is the interconnectedness of the banking sector; all other sectors operate within or have high reliance on it.

Table 1: *Shows the inherent risk, strength of control measures applied and overall ranking of the risk of these sectors.*

Inherent risk: *vulnerability that ML/TF/PF could occur within the sector.*
Strength of control measures: *how well controls across the AML/CFT system mitigate vulnerabilities. The darker the shade, the stronger the control measures to mitigate sector vulnerabilities.*
Overall risk: *ranks the risk of these sectors, given the current threat environment.*

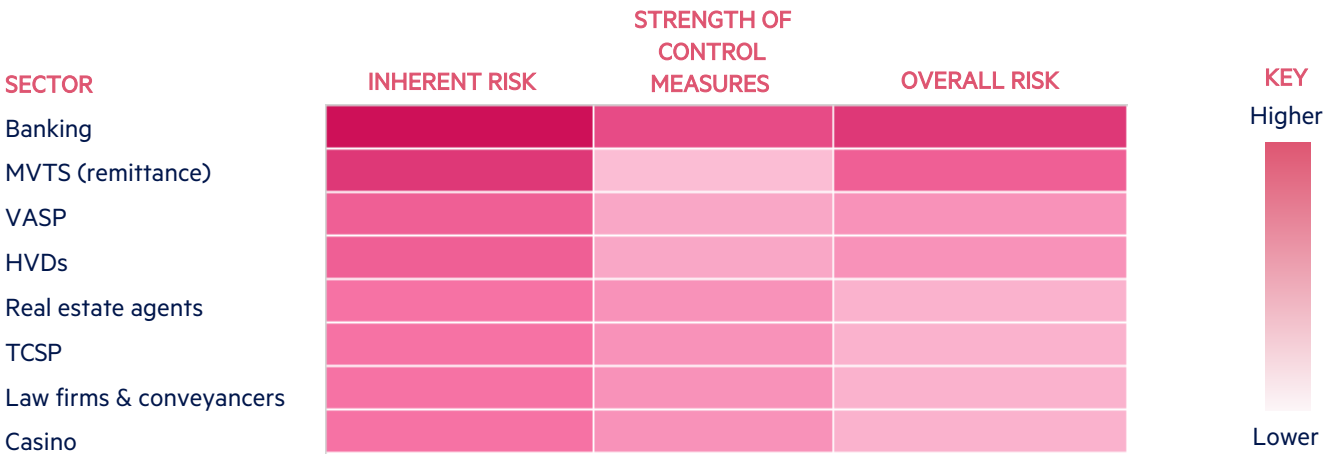
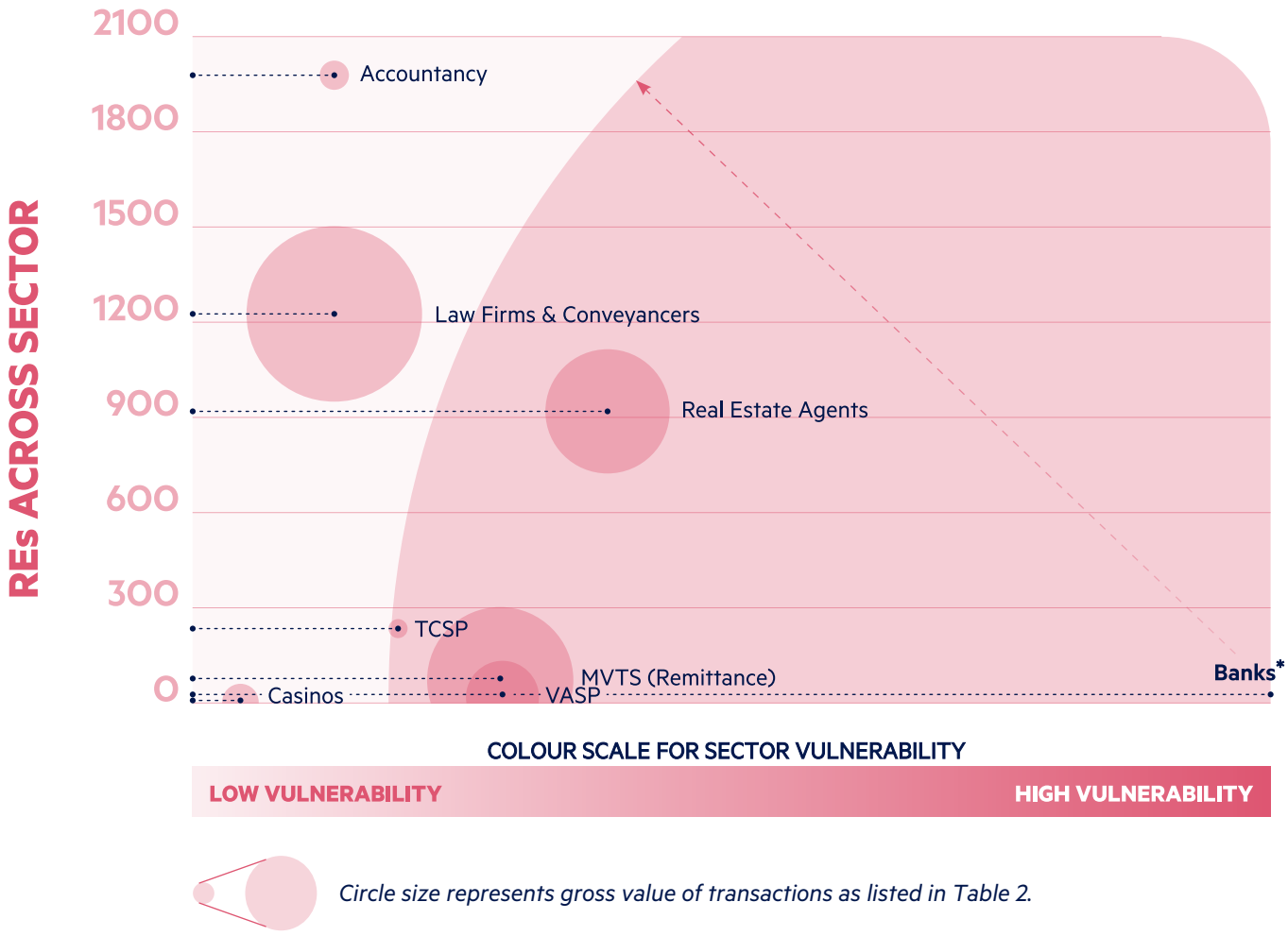


Table 2: *Describes sector size based on self-reported transaction value per sector for 2022-2023. For example, for every million transacted through the banking sector, the casino sector transacted $19.54. This provides context of the size of the reporting sectors when contrasted with each other.*

SECTOR	REs ACROSS SECTOR	SUM OF GROSS VALUE OF TRANSACTIONS	SECTOR SUPERVISOR	MONEY MOVEMENT PER $1M
Banking	27	$58,957,954,065,908.80	RBNZ	$1,000,000.00
MVTS (remittance)	92	$28,662,780,140.76	DIA	$486.16
VASP	23	$4,889,567,932.31	DIA	$82.93
Real estate agents	923	$17,564,000,000.00	DIA	$297.91
TCSP sector	246	$398,500,000.00	DIA	$6.76
Law firms & conveyancers	1267	$38,246,000,000.00	DIA	$648.70
Casino	3	$1,151,937,397.22	DIA	$19.54

Graph 2: *Size of the banking sector in contrast to the other sectors.*



Circle size represents gross value of transactions as listed in Table 2.

**The sum of gross value of transactions for Banks is approximately 150 times larger than represented in this graphic, or approximately 1500 times larger than Law Firms & Conveyancers.*

Sectors abused for ML across the high-risk crimes

MVTS is a sector routinely identified in drug investigations. Criminals seek to transfer funds offshore using this sector. Some high-profile examples of remittance sector misuse have occurred in recent years, identifying that this sector has been the payment corridor to fund importation of drugs into New Zealand.

The VASP sector is vulnerable to exploitation – for transferring fraud/scam proceeds – due to the speed that payment can be made to any jurisdiction. Similarly, it can be exploited for cross-border payments for the transhipment of drug imports to New Zealand. Peer-to-peer transfers (operating inside and outside of the regulated sector) and individuals selling virtual assets are high-risk activities.

Real estate continues to feature prominently in asset seizure data, with lawyers or conveyancers necessary for conveyancing property transactions. Real estate and law firm sectors are both vulnerable to exploitation by individuals looking to launder criminal proceeds through New Zealand property. Analysis of SAR data submitted by lawyers highlights that individuals in New Zealand are attempting to purchase real estate without disclosing their source of funds and occasionally, they are unwilling to comply with the sector's AML/CFT obligations. This demonstrates the attractiveness of real estate.

High-value items such as vehicles, motorcycles, jewellery, gold, and gems comprise the largest number of assets confiscated in New Zealand. Dealers in these items are vulnerable to exploitation as they deal with valuable items, many easily portable. As of May 2023, dealers in these items are prohibited from accepting cash greater than $10,000 for these goods. It is too early to assess the impact of this legislation change; however, there have been no prosecutions for non-compliance with the $10,000 threshold.

Some DNFPBs, including law firms, accounting firms and TCSPs, provide specialist services, including trust and company formation, which can be abused to launder proceeds of crime. Investigations in New Zealand have identified instances involving the misuse of companies and trusts to launder criminal proceeds.

Casinos continue to be vulnerable in New Zealand, although this risk appears to have shifted to online gambling. Investigations in New Zealand have identified proceeds of drug and fraud offending being laundered through offshore online gambling platforms.

A review from the sectors identified as being misused by criminals highlighted the top ten reasons for reporting a SAR (see p.14-16).

> **Frauds and scams are a leading concern across each sector (highlighted in red), alongside suspicious source of funds or cash deposits (highlighted in blue-grey).**

This aligns with the threat assessment, which identified frauds and scams as leading threats in New Zealand and recognises cash-generating crime, which includes drug crime.

Top 10 reasons for SAR reporting

Table 3: *Top 10 reasons for SAR reporting.*

Frauds and Scams Suspicious source of funds or cash deposits

BANKING 2020	BANKING 2021	BANKING 2022	BANKING 2023
Large Cash Transactions / Deposits	Suspicious Cash Deposit(s)	Fraud / Scam	Fraud / Scam
Unknown Customer Due Diligence / Source of Wealth information	Suspected Tax Evasion	Large Cash Deposit(s)	Cash Deposits
Money Laundering	Child Exploitation	Cash Withdrawals	Movement Of Funds
Large / High Volume International Transactions	Fraud / Scam Victim	High Value Domestic Transfer(s)	Third Party Deposits
Large / High Volume Transactions	Rapid Movement of Funds	Extremist Spending Concerns	Unknown Source of Funds /Source of Wealth
Tax Evasion	National Security Concerns	Cash Deposits Rapidly Followed by Account Transfers	Funds From High-Risk Jurisdiction(s)
Rapid Movement of Funds	High-Value / Excessive Withdrawals	Cash Deposits And / Or Account Transfers Sent To High-Risk Sector (Remitter)	Scam / Fraud Victim
Scam	Suspected Fraudster	High Value Wire Transfer(s)	Cash Withdrawals
Fraudulent Activity	High Value International Funds Transfer(s) Received	Funds Received from High-Risk Country (China)	Funds to High-Risk Jurisdiction
Child Exploitation Material	Cryptocurrency Purchase / Trading	Child Exploitation	Child Exploitation

Continued next page

Table 3 (continued): *Top 10 reasons for SAR reporting.*

Frauds and Scams Suspicious source of funds or cash deposits

MVTS	VASPs	LAW FIRMS & CONVEYANCERS	REAL ESTATE
Receipt Of Criminal Proceeds / Fraudulently Obtained Funds	Scam / Fraud Victim	Failure To Provide Customer Due Diligence / Source of Wealth information	Refusal to Complete Customer / Enhanced Due Diligence / Supply Source of Wealth information
Scam Victim	Identity Fraud	Adverse Media / Criminal Links	Purchased & Sold Within Short Timeframe
Individuals Sending Funds Offshore Appear to Share ID Information	Transactions To Darknet Market	Property Purchase with Unexplained Offshore Source of Funds	Use Of Trust
One Individual Sending Funds to Multiple Persons Offshore	Possible Fraudster	Unexplained Source of Funds	Foreign Source of Funds for Property Purchase
Suspected Money Mule	Suspected Money Mule	Unexplained Payment / Overpayment	Possible Scam / Fraud
Child Exploitation	Refusal to Complete Customer / Enhanced Due Diligence / Supply Source of Wealth information	Scam / Fraud Victim	Adverse Media
Individuals Sending Funds to High-Risk Jurisdictions	Child Exploitation	Inconsistent Information	Unexplained Source of Funds / Cash Payment
Refused To Respond to Enhanced Customer Due Diligence Request	Funds To Iranian Exchange	Suspicious Loan	Property Sold Below Value
Reactive Reporting to Police	Funds To Russian Exchange	Refund to Third Party	Unusual / Evasive Behaviour
False Identification Used	Sharing Wallet with Another User	Unexplained Cash	Gang Links

Continued next page

Table 3 (continued): *Top 10 reasons for SAR reporting.*

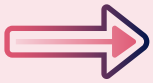
Frauds and Scams Suspicious source of funds or cash deposits

HVDs	ACCOUNTING FIRMS	CASINOS
Cash Purchase / Structured Payment	Suspected Tax Offending	Funds Obtained via Fraud withdrawn at Casino - With No / Minimal Gambling Activity
Possible Fraudster	Suspicious Source of Funds	Cash Withdrawn via Eftpos and Not Used for Gaming Activity
Unusual Sale / Purchase Pattern	Large Volumes of Cash Deposits	Attempts to Obscure Origin of Funds / Refinement
Reactive Reporting in Response to Police Interest	Refusal to Provide Information / Complete Customer Due Diligence	Suspicious Source of Funds Based on Cash Appearance / State / Behaviour of Customer
Gang Links	Reluctant / Hesitant to Provide Identification	Reactive Reporting in Response to Police Interest
Multiple Credit Cards Used For One Purchase	Possible Fraud / Scam Victim	Fails To Complete Customer Due Diligence / Provide ID
Payments Made Before Expected	Gang / Criminal Links	Gang Links
Nonsensical Reasons for Vehicle Purchase	Nonsensical Transactions	Adverse Media
Offshore Source of Funds for Vehicle Purchase	Understating Income	Suspected Tax Evasion
Failed Lending Application	Use of Shell Companies	Cash Exchange Between Two Parties

Key changes from last NRA

INCREASING RISK

- Increasing volumes and values of fraud crime – including where the government is targeted, cyber-enabled fraud and more general fraud.
- VASPs – virtual assets feature in both fraud and drug investigations.



UNCHANGED RISK

- Banking remains the dominant vulnerability sector, still high-risk as per the 2019 NRA.
- Drug-related crime remains high-risk and cash-intensive.
- MVTS remains high-risk. Note that money laundering investigations targeting the remittance sector, in response to the 2019 NRA, have resulted in a number of successful prosecution outcomes.
- Real estate, law firms, accountancy firms and high-value dealers all feature in investigations and therefore the level of risk remains unchanged.
- TF risk is unchanged and currently low.

REDUCED RISK

- Money laundering risk associated with non-compliance with New Zealand's tax system has declined. However, tax fraud (for example, GST-related fraud) is captured in the high-threat crime of fraud.
- TCSPs are recognised as having lowered risk, based on identified misuse associated with money laundering. However, this sector remains vulnerable as criminals use legal structures to conceal beneficial ownership of illicit wealth.
- Casinos with physical premises are recognised as having decreasing risk, likely due to enforcement action and improved compliance.

Outlook beyond 2024

Threats

The high-threat crimes described in this NRA are likely to drive risk for the next two to three years. Technology advancement, including the use of artificial intelligence, will likely increase the exposure to scams and frauds across New Zealand. Demand for illicit drugs across New Zealand will likely remain high, meaning New Zealand remains a marketplace of choice for foreign transnational organised crime groups – the proceeds of which will in part need to be remitted offshore.

The use of recent changes to the Criminal Proceeds (Recovery) Act may make New Zealand less attractive as a destination for foreign-generated illicit wealth and therefore reduce the threat of transnational money laundering.

Vulnerabilities

Banking is likely to remain the highest-risk sector. The introduction of 'confirmation of payee' – where the bank checks the name and account details of the person or business their customer intends to pay, to confirm a match of details before payment – may harden the banking system and prevent some scams and frauds.

Technology advancement, the increasing efficiency of payment processes, and strengthening compliance and supervision of the most vulnerable sectors could displace risk into sectors currently considered lower risk. For this reason, complacency within the recognised low-risk sectors should be avoided.

New Zealand's highest-value prevention activity (the 'anti-' in AML) occurs by the people who work within the reporting sectors. Our greatest opportunities exist when our AML/ CFT community looks beyond AML/CFT as a pure compliance obligation. Complacency is an enabler and a vulnerability.

With the increasing prevalence of fraud, many reporting entities and their customers are becoming victims of sophisticated crime. All sectors should adopt a 'mindset' of vigilance and actively look to identify, prevent, detect and disrupt criminal enterprise at all levels.

CRIMINAL THREATS TO NEW ZEALAND'S AML/CFT/ CPF SYSTEM

All crime that derives illicit income exposes New Zealand's AML/CFT/CPF system to threat. Crime that generates high volumes and value of illicit income presents an elevated threat. High-threat crime can include emerging crime – this likely presents increasing threat unless policy, process and practice pivots in response to that threat. Finally, high-threat crime can occur offshore if the proceeds of that offending enter New Zealand's financial system.

KEY HIGH-THREAT CRIMES IDENTIFIED IN THIS NRA ARE

- Illicit drug crime
- Fraud offending
- Transnational money laundering

Drug crime

Drug demand in New Zealand is driven by addiction and recreational use. Meeting demand in New Zealand is highly profitable for international crime groups, domestic organised crime and individual participants in the domestic drug supply marketplace. In New Zealand, methamphetamine and cocaine are sold for some of the highest prices in the world which incentivises entry and participation in this market. Demand for methamphetamine, MDMA and cannabis is high and will likely remain high. Demand for cocaine is increasing.

Gangs and organised crime groups are active in the 'business' of selling and distributing illicit drugs across New Zealand. Through international connections, drugs such as methamphetamine, MDMA and cocaine are purchased from the international marketplace and imported into New Zealand.

> **Like any imported good, payment is a requirement so financial services or sectors that enable payments offshore have higher vulnerability to money laundering associated with drug-related crime.**

Between 2018-2023, the FIU disseminated 1,211 reports to investigators relating to drug crime. This captured intelligence received through 5,115 suspicious activity reports (SARs), 18,732 prescribed transaction reports (PTRs) and 55 border cash reports (BCRs).

The illicit drug domestic market in New Zealand operates within a cash-dominated marketplace. A small online marketplace operates using cryptocurrency. Money laundering threat largely emerges through transnational cross-border payment activity and at a domestic wholesale and retail level through the introduction of cash into the financial system or the exchange of cash for property.

Methamphetamine

Methamphetamine seized at our border is indicative of the demand. In 2022, a total of 1,959 kilograms of methamphetamine was seized domestically and offshore (en route to New Zealand). 2022 also saw record single seizures at the border, including 613 kilograms from Malaysia, and 510 kilograms of grease containing methamphetamine paste from Iran.[2] These seizures used sophisticated trafficking methodologies.

Production of illicit drugs is increasing in Southeast Asia and the Americas. Increased supply has resulted in large seizures globally, including in New Zealand. The largest methamphetamine seizure in New Zealand occurred in March 2023, when 747 kilograms was seized in South Auckland.

Methamphetamine remains the most detected drug in wastewater testing. It is detected at all testing sites across New Zealand.

In 2022, Malaysia emerged as the top source country of methamphetamine to New Zealand. This likely reflects that Malaysia is used as a transit country through which methamphetamine is exported to New Zealand. Myanmar[3] is a significant source country for methamphetamine in Southeast Asia; it is probable that methamphetamine seized in New

[2] See Chapter 6: Proliferation Financing Risk Assessment, pages 90-95.
[3] Refer to pages 29, 78, 83 and 84, regarding Myanmar.

Zealand from Malaysia originates from Myanmar. The other two leading transit countries (source countries) are Canada and the United States, both likely to transit methamphetamine manufactured in Mexico.

$400,000 worth of jewellery was seized from a methamphetamine dealer. The dealer had obtained insurance on these items. Some of the jewellery items were purchased in Australia. An associate also purchased $450,000 of gold with cash.

16 kilograms of methamphetamine was imported from South America. Cash was provided to an individual selling cryptocurrency to drug dealers; he would take a 10%-20% commission on the sales. Some cryptocurrency purchased by drug dealers would be transferred to South America to fund the purchase of methamphetamine, for import into New Zealand. The cryptocurrency seller would (via remitters) transfer the proceeds of selling cryptocurrency to bank accounts in China. The investigation identified that cash to the value of $17.5M was transferred to China. Using the funds from the bank accounts in China, he would purchase cryptocurrency that he would then sell in New Zealand.

CASE STUDY

Operation Weirton

In February 2022, Police and Customs seized New Zealand's largest single seizure of methamphetamine (613kgs) at Auckland Airport. The methamphetamine was routed through Malaysia and was in one-kilogram bricks wrapped in tea packets, a known concealment method of methamphetamine originating in Myanmar.

This operation resulted in six people facing charges for the supply of methamphetamine and money laundering offences. Some of these people have links to the Comanchero Motorcycle Club. The disruption of this shipment prevented an estimated 30,650,000 common doses of methamphetamine entering New Zealand and likely prevented over $642 million in social harm.

Significant volumes of transactions occur between New Zealand and Malaysia. Data captured by the FIU through both prescribed and SAR reporting identifies that between 2018 – 2023, $7B was transferred to Malaysia. A much greater sum was transferred from New Zealand to Canada ($20B) and the United States ($267B) during this same period. It is possible that within this volume of transactions, drug-related payments are being made.

Between 2018-2023, 2,598 persons were charged with importing, manufacturing or supplying methamphetamine. An additional 2,989 persons were charged in relation to being in possession of methamphetamine with the intention to supply to others. 59 persons were charged with money laundering, where the predicate offence related to methamphetamine crime.

Police focus on methamphetamine remains high and in alignment with risk. Between 2018-2023, property to the value of $147M was restrained in association with methamphetamine crime. During this same period, $40M was forfeited. In addition to cash and bank accounts, property restrained or forfeited included 454 vehicles, 190 motorcycles, 107 residential properties, 11 lifestyle blocks, 91 items of jewellery, and 32 boats. Through these restraint proceedings, money laundering involving nominees, trusts, family members and other third parties was identified on 39 occasions.

> **The type of property restrained identifies the sectors which are exposed to methamphetamine-related crime threat.**

Domestic laundering of drug proceeds through intermediatory contractors is an emerging ML typology. This is occurring in the construction and horticulture sectors. What is observed is that a contractor employs subcontractors to provide a service. The subcontractors are paid with illicit cash by the primary contractor. The primary contractor then supplies an invoice to a customer, who pays the primary contractor via a legitimate transaction. This process in effect allows the primary contractor to swap illicit funds (cash) for legitimate funds (funds received from a legitimate customer). Amounts laundered through this method are likely to be significant.

Cocaine

Cocaine consumption is rising in New Zealand. The profiles of persons involved in the importation and distribution of cocaine are largely consistent with those involved in methamphetamine.

This includes those involved in gangs and organised crime. Several investigations have identified foreign nationals working in New Zealand – operating as a syndicate to import cocaine from criminal contacts in their home country for distribution here. from the South American community, who are living in New Zealand, have been importing and distributing cocaine.

Operation Mist (2021) was a significant police investigation into the importation of cocaine into this country from South America.

Drug "catchers" – originally from Colombia – who were employed as farm workers in rural Canterbury, received packages containing cocaine at various addresses in the South Island. Former dairy farm workers, who had returned to South America, were involved in sending cocaine to New Zealand. This investigation has linked the source of supply to Colombia.

Pricing remains relatively steady at $400-$500 per gram, with price slightly lower when sold via online marketplaces. The New Zealand cocaine market continues to offer one of the highest profit margins in the world.

Wastewater testing shows increasing consumption of cocaine across New Zealand. This likely demonstrates that international crime groups are increasing their efforts to supply this drug and grow demand for it nationwide.

Between 2018 and 2023, property to the value of $8M has been restrained in relation to cocaine-related crime. In addition to cash and funds held in bank accounts, this included 24 vehicles, 3 motorcycles, 3 residential properties, 1 item of jewellery, and 1 boat. Although this is a modest value in contrast to asset forfeitures from methamphetamine related crime, the types of property are broadly consistent.

Major source countries for cocaine include Ecuador, Colombia and Mexico. Funds flowing from New Zealand to Ecuador during 2018-2023 totalled $168M, to Colombia $131M, and to Mexico $350M.[4] It is probable that drug-related payments exist within these payment flows.

Laundering money using cryptocurrency is occurring. During a South Island police investigation, criminals were purchasing and then transferring Bitcoin to move funds to associates in New Zealand and Colombia.

CASE STUDY

Operation Depot

In November 2022, Police and Customs seized at least 190kgs of cocaine in Tāmaki Makaurau with an estimated "street" value of $38M. The cocaine was concealed inside the pipes of a commercial boiler imported from Ecuador. This concealment method indicates the sophistication and investment by organised crime groups (OCGs) to conceal drugs for distribution into the New Zealand market.

Seven people were arrested in relation to Operation Depot for participating in an OCG and importing and supplying cocaine.

Operation Depot prevented an estimated 1,900,000 common doses of cocaine being distributed throughout New Zealand. A seizure of this quantity also likely prevented over $70 million in social harm.

MDMA[5] – Ecstasy

There is some domestic organised crime involvement in the distribution of MDMA in New Zealand. However, relative to other illicit drugs, there was a greater proportion of non-organised crime actors participating in the market.

MDMA continues to be widely distributed through both online platforms and in person. Social media platforms continue to be used to facilitate sales within New Zealand. Dark web marketplaces are also used to distribute MDMA domestically and enable international purchases.

The price of MDMA remained stable at $200-300 per gram. Almost 100 kilograms more MDMA was imported in larger consignment sizes (over one kilogram) in 2022 compared to 2021.

[4] This excludes Fisher and Paykel Healthcare Limited sending funds to their own account in Mexico.

[5] 3,4-Methylenedio methamphetamine.

The importation of increased quantities in kilogram amounts indicates demand for distribution, and possibly indicates increased domestic organised involvement.

It is likely MDMA suppliers in Europe continue to shift and use different supply routes to circumvent law enforcement activity.

Europe continues to be the main source and export region for MDMA imported into New Zealand. In 2022, 90% of all MDMA seizures by Customs originated from Europe. The majority of MDMA produced in Europe is likely produced in the Netherlands as well as surrounding countries. In 2022, new export countries emerged with Portugal, Italy and Greece joining France and the United Kingdom as the top five MDMA export countries to New Zealand.

Cannabis

The 2021/2022 Health Survey[6] found cannabis to be New Zealand's most used illegal drug, with an estimated 178,000 people using cannabis weekly. The supply of cannabis emerges from small-scale cultivators to large commercial operations involving organised crime groups. Recently, Vietnamese nationals holding New Zealand visas and those with expired visas have been involved in very large-scale commercial cannabis cultivation enterprises, operating largely in the upper North Island. $112M in assets have been restrained in the last five years with $13.5M forfeited. These include cash, 100 residential properties, 11 lifestyle properties, 91 vehicles, 70 motorcycles, and 14 boats.

Other drugs

Ketamine, LSD[7], opioids, Fantasy-type substances, GBL[8], and synthetic cannabis are consumed in New Zealand. A number of these drugs are sourced from China, India, Vietnam, Japan, the Netherlands, and Singapore. Between 2018-2023, just over $9.5M had been restrained in relation to these drugs and $1.2M forfeited. Property comprised cash, residential property, vehicles, jewellery and precious metals.

Examples of use of proceeds generated through drug crime, by sector

BANKING

- Criminals depositing cash into third party accounts.
- Criminals placing and layering criminal proceeds through products and services provided by banks.
- A customer identified as receiving large volumes of cash into her account which was then transferred to a law firm to facilitate a property purchase.
- Criminals taking control of bank accounts in the names of associates and family members then depositing cash.
- Servicing mortgage debt through cash deposits.
- Transferring funds internationally.
- Vietnamese cannabis cultivators depositing cash and then remitting funds to Vietnam.

MVTS

- Transferring drug-dealing profit offshore to third parties; this includes the transfer of funds to finance the importation of illicit drugs into New Zealand.
- Complicit money remitters depositing cash directly into the bank accounts of their customers.
- Complicit money remitters who use companies with nominee directors, third party bank accounts, and cash depositors to distance themselves from the remittance sector.
- Members of a cocaine syndicate remitted funds to Brazil, Canada, Chile, Colombia, Ecuador, Iran, USA and Mexico, using four separate money remitters. Remittances were undertaken at foreign exchange outlets using cash, or online using credit cards. Senders then made cash payments against the credit cards used.

VASPs

- Criminals using the banking sector to transfer funds to VASPs to purchase cryptocurrency. The cryptocurrency purchased was then transferred to offshore third parties.
- Individuals involved in the supply of methamphetamine purchasing cryptocurrency for the purpose of investment.
- Individuals involved in the supply of methamphetamine purchasing cryptocurrency from crypto ATMs.
- Individuals involved in the supply of methamphetamine purchasing cryptocurrency from businesses who also provide money remittance services.
- An MDMA importer using proceeds from his drug-dealing activities to purchase cryptocurrency.

[6] Ministry of Health 2012/2022 New Zealand Health Survey.
[7] Lysergic acid diethylamide – a Class A controlled drug.
[8] Gamma-Butyrolactone – a Class B controlled drug.

HIGH VALUE GOODS

- Criminals used the proceeds of illicit drug crime to purchase vehicles, motorcycles, boats and jewellery.
- In an Auckland investigation, a criminal used the proceeds of methamphetamine and cocaine sales to purchase four items of artwork valued in total at $100,000.

REAL ESTATE

- Purchases of real estate, or the servicing of mortgages with proceeds of crime, is occurring across New Zealand.
- A criminal sold a property to a shell company at an inflated price to launder $5 million cash. The vendor orchestrated the sale to a company for which a known third party was a nominee director. The vendor maintained effective control over the property.

OTHER

- Purchasers of drugs using Paysafecard for payment, which is redeemed on online gambling platforms. Prezzy cards have also been accepted as payment for illicit drugs.

Estimation of the value of proceeds generated through drug crime

Wastewater analysis provides an estimation of the amount of illicit drugs consumed across New Zealand weekly. Using domestic sale price, and the cost of purchasing illicit drugs in the international market, profitability can be estimated.

Retail domestic price is not consistently stable. Price is determined by several factors, e.g., volume purchased, quality of the drug supplied, market conditions (availability/scarcity) and the relationship between the buyer and seller. Hence, the amount of 'profit' generated from the sale of illicit drugs that is subject to actual laundering is difficult to establish with accuracy. It can be conservatively estimated as:

Methamphetamine: between $300M-$500M annually
Cocaine: between $25M-$35M annually
MDMA: between $10M-$15M annually
Cannabis: between $100M-$200M annually

This value reflects net profit. It excludes the cost of purchasing illicit drugs which are then on-sold. Actual purchase price varies subject to where the drugs are purchased. Purchase in the international marketplace would mean that additional funds were laundered for the purpose of settling payment.

> **In summary, profit from drug crime is conservatively estimated to be in the range of $500M - $600M annually.[9]**

Fraud

The volumes and value of fraud is increasing in New Zealand and in many parts of the world. Criminals have embraced technology and are reaching across borders to target victims in countries other than their own. Fraud is currently one of the most reported crimes to Police.

Domestic offenders target victims with a range of fraud types – these victims include individuals, businesses, insurance companies, banks, and the government. The vulnerability of offenders who commit fraud is that unlike drug crime and its reliance on cash, the proceeds associated with fraud are all transferred within the AML/CFT regulated financial system. The NZ AML/CFT system should consider implementing programs to improve understanding of the harm caused from fraud as part of a wider response to combat fraud.

> The Ministry of Justice's New Zealand Crime and Victims Survey showed that fraud is now the most common type of offence overall and it is on the increase. There were 510,000 offences between November 2021 and November 2022, compared with 288,000 offences between 2020 and 2021. "The State of Scams in New Zealand 2023" report identified that of 1000 people surveyed, 17% lost money to scams with an average loss of $3,165. Although caution must be taken with the sample size, if applied across the population this would amount to a financial loss of $2.5B or 0.5% of New Zealand's GDP.

CYBER-ENABLED FRAUD

> Between 2018-2023, the FIU disseminated 604 reports to investigators, related to frauds. These reports related to intelligence received through 5,984 SARs, 42,337 PTRs and 172 BCRs.

Cyber-enabled fraud presents a range of challenges. Scams (including phishing, smishing, identity theft, business email compromise, fraud facilitated through social media platforms, online marketplace fraud, romance scams, investments scams) are increasing. Although fraud offenders can operate from anywhere in the world, some countries have emerged as global hotspots for fraud and scams targeting New Zealanders. These countries include Nigeria, China, India, Romania, Eastern Europe more generally, and Russia. Some

[9] The value estimated in the 2019 NRA was $553M.

of these offenders could be terrorist organisations raising funds for terror operations[10] or state actors raising funds for proliferation.[11]

Victimisation is occurring right across New Zealand. Fraud criminals are opportunists and target victims of all demographics. Levels of victimisation have increased across all ages. In Tāmaki Makaurau, it has been identified that individuals aged 26 to 45 reported significantly higher levels of all fraud to Police, compared to other age groups. The proportion of individuals reporting fraud crime aged 18 to 25 is declining, while the proportion of reports from the 26 to 45 age group is increasing.

Older victims are observed to suffer a higher value of loss than younger victims. 'Money mules' often enable offending when responding to adverts for casual work – e.g., through Facebook, TikTok or Snapchat. The casual work involves the use of their bank account to consolidate fraud proceeds (for a fee) before transferring funds offshore. Some victims are also unwitting participants of money laundering where their bank accounts are used to consolidate funds from unconnected victims before being transferred offshore.

Between 2018-2023, Police charged 11,625 individuals with 29,285 fraud-related charges.

Fraud against the Government

Frauds against the Accident Compensation Corporation (ACC) and the Ministry of Social Development (MSD) include persons receiving benefits they are not entitled to, the making of false representations to obtain benefit, and the submission of false documents.

In relation to ACC, some vendors have inflated invoicing or have billed for false or phantom persons. The MSD, Serious Fraud Office (SFO) and Police have also been responding to Covid-19 wage subsidy frauds where individuals have taken advantage of high-trust government-initiated models, creating false identities and companies to obtain financial benefit. These offences used identities from immigrants in New Zealand who did not know their identities were being misused.

With disaster relief, there have been instances where companies have colluded to take advantage of local government tender processes – submitting documents from which they are awarded contracts for disaster relief and recovery work.

Between 2018-2023, the FIU disseminated 113 reports to investigators, relating to intelligence associated with potential frauds against the government. These reports referenced 2,416 SARs, 1,336 PTRs and 1 BCR (excluding tax).

Between 1 July 2018 – 30 March 2023, MSD prosecuted 315 benefit fraud cases.

In relation to wage subsidy claims as of March 2024, there has been:

- 25,014 repayments of taxpayers' funds, totalling $824.4 million.
- 15,687 pre-payment and post-payment checks on wage subsidy applications (as of 31 December 2023).
- 7,461 allegations of wage subsidy misuse resolved (as of 31 December 2023).
- 46 people have been prosecuted for wage subsidy misuse, in relation to more than $3 million in subsidy payments.
- 45 businesses have civil recovery action underway against them to recover payments.
- 11 cases of significant and complex alleged wage subsidy fraud referred to the SFO.

An Auckland accountant made 12 fraudulent applications on behalf of several companies, in an attempt to defraud the Covid-19 Wage Subsidy Scheme of more than $68,000. In another matter, a man was sentenced to 20.5 months in prison for defrauding taxpayers to the tune of almost $200,000 in Covid-19 wage subsidies. Other wage subsidy frauds include persons in foreign jurisdictions successfully applying for wage subsidy grants; and persons applying for wage subsidies for their children, and companies that have not operated for two years. Often proceeds of these frauds were remitted offshore or consumed at online gambling sites.

[10] See Chapter 5: Terrorism Financing, page 85.
[11] See Chapter 6: Proliferation Financing risk assessment, page 90.

A Waikato plumber provided services to Kāinga Ora (Housing New Zealand). The plumber submitted inflated invoicing for services provided ($520,000 overpaid). The police investigation also identified tax-related crime (involving $2,250,000). Undeclared cash was deposited into a family member's account and remitted to a law firm's account (via a money remitter) to purchase real estate. The plumber made payment to Inland Revenue (IR) and was also subject to a forfeiture order issued under the Criminal Proceeds Recovery Act valued at $2.2M.

Tax fraud relates to behaviour where a taxpayer intentionally falsifies information on their tax returns or other documents to obtain financial gain such as a refund or a reduction in 'tax to pay'. This typically occurs with fraudulent GST claims, manipulation of income records, identity fraud (compromised IR identities where the true owner has had their account accessed and used by a 3rd party as a consequence of their wider personal details being obtained) and employer frauds where fictitious employees are created to obtain refunds on PAYE paid.

Working for Families (WfF) fraud occurs when taxpayers register fictitious children, claim for children that are not in their actual care, claim WfF whilst overseas or do not declare relationships.

A current trend observed by Inland Revenue (IR) typically involves foreign nationals. The foreign national opens a bank account in the name of a false passport, then registers with IR using legitimate details. They incorporate companies and register for GST. They then claim false refunds which are credited to the account created under the identity of the fictitious passport. Having receipted funds through the fraud, the offender may leave New Zealand before the crime is detected and action can be taken.

Another trend is occurring where criminals harvest personal information and identities from online systems, gaining access to a group of people's IR accounts. Once inside the IR computer system, criminals then claim false refunds, advance fake donation rebate claims, and manipulate returns – directing refunds to mule bank accounts for laundering and moving the fraud proceeds.

Between 2018-2023, IR completed 306 prosecution cases involving tax fraud or evasion, with a combined value of $91M. Evidencing the laundering of evaded tax (legitimate earnings not declared) is challenging given the income not declared has a legitimate source. Benefit from tax crime that can be laundered occurs when financial benefit is derived from the filing of untruthful (deceptive) information to IR, as opposed to failure to file a return. A 2018 study by IR and Victoria University has identified that self-employed individuals under-reported approximately 20% of their gross income – representing foregone revenue of approximately $850M per year.

The 2024 IR annual report identifies that the IR system screened 9.7 million returns. $230 million in incorrect or fraudulent refunds and tax deductions were stopped and payment prevented, reflecting the improved effectiveness of IR's internal controls and system.

It is challenging for reporting entities to identify a specific type of crime with their reporting. High volumes of cash depositing by a "self-employed plumber" could be tax evasion, assuming the reporting entities suspects the plumber will file a false or deceptive return of the cash and/or that it could be the proceeds of drug dealing. Unexplained cash depositing cannot be assumed to relate to tax crime. For this reason, non-compliance with New Zealand's tax compliance framework is recognised as a notable crime in this NRA.[12] Suspected tax evasion activity may in fact be an indicator of a high-threat crime such as dealing in illicit drugs.

If a tax fraud specifically is suspected by a reporting entity, it would be useful to expand on the grounds for that suspicion, to ensure reporting is directed to the right agency.

Sectors considered high-risk in terms of committing tax fraud include the hospitality sector – in particular, takeaway and restaurant operations. These types of businesses present higher risk since cash is often the preferred method of payment for their products and services.[13]

[12] Refer to Executive Summary, page 9.
[13] Refer to Chapter 4: Risk Associated with Legal Persons and Legal Arrangements, page 67.

Customs revenue evasion and fraud

Between 2018-2023, 99 charges were laid in relation to offences under the Customs and Excise Act. Most of these charges related to tobacco smuggling and the failure to make accurate declarations (or making deliberately misleading declarations) when bringing products into New Zealand. Smuggling of cigarettes on a large scale is undertaken by transnational organised crime groups. Customs have seen payments linking the sale of black-market tobacco back to China and other South East Asian countries.

Between 2018-2023, the FIU disseminated 147 reports to New Zealand Customs relating to intelligence, associated with Customs and Excise Act compliance. These referenced 8,248 SARs, 11,403 PTRs and 23 BCRs.

Other frauds

Frauds against banks, including mortgage frauds, are occurring. Frauds are widespread through scams created in Facebook or Trade Me where persons using fictitious identities list items of property for sale that do not exist. The Financial Markets Authority (FMA) has also seen an increase in social media contact scams, romance/investment hybrid scams and imposter websites. Frauds are also undertaken by employees of businesses, who manipulate company records and documents to derive illicit benefit. Indicators include employees who received multiple and regular payments from their employers in addition to regular payment of wages or salary. The insurance sector also identify that they are also subject to high-value frauds.

The SFO charged a lawyer with mortgage fraud from which a bank advanced $1.35M. He was sentenced to nine months home detention in August 2024.

A New Zealand scammer was convicted in April 2024 over her involvement in a $17M cryptocurrency pyramid scam. The criminal promoted the global cryptocurrency-based scheme to Māori and Pasifika communities in New Zealand. 83% of participants lost their money. Globally, there were 150,000 participants in the scheme.

The insurance industry indicates that staged motor vehicle accidents co-ordinated by organised groups was one of the fastest emerging fraud trends in 2022.

FRAUD PROCEEDS RESTRAINED AND FORFEITED

Between 2018-2023, property to the value of $127.2M was restrained – involving 345 assets. During this timeframe, 113 assets were forfeited with a combined value of $31M.

Property restrained and forfeited included 88 residential properties, 7 commercial properties, 60 vehicles, 26 motorcycles and 3 boats. There were also a small number of securities and items of jewellery restrained or forfeited. Sectors associated with this property include law firms and conveyancers, real estate and high value dealers.

Estimation of the value of proceeds generated through fraud

It is challenging to accurately value of the proceeds generated through fraud; there are a range of estimates provided by different industries and agencies. The 2019 NRA estimated $500M was available to launder derived from fraud. Scams and fraud accounted for almost $15.7 million (86% of overall direct financial loss) in 2023. Of that loss:

- 4.6M went to investment scams
- 3.1M went to scams involving unauthorised money transfer
- 2.5M went to scams involving a new job or business opportunity offers
- 2.3M went to cryptocurrency scams
- 1.7M went to dating or romance scams
- 1M went to scams when buying, selling or donating goods online
- 0.5M was lost to other types of scams.

One recent figure from the banking sector indicated New Zealand banking customers lost $183.5 million to scams from October 2021 to September 2022, a 40% increase from the previous period and a total of $381.8 million for the two-year period from 1 October 2021 – 30 September 2023.

The Department of Internal Affairs estimates that identity theft costs the New Zealand economy more than $200 million per year.

The Insurance Fraud Bureau (IFB) New Zealand estimates that insurance fraud cost policyholders and insurers in New Zealand about $880 million in 2023.

Accurate data from across all government agencies is not available; however (while difficult to accurately assess), estimates from IR suggest:

- IR revenue risk on GST frauds is estimated to be $300M annually.
- IR revenue risk on income-related frauds is estimated to be$5M annually.
- IR revenue risk on identity-related frauds is estimated to be$50M annually.
- IR revenue risk on employer frauds is estimated to be less than $1M.
- IR revenue risk on Working for Families frauds is estimated to be $5M annually.

An accurate assessment of the value of proceeds laundered, where fraud is the predicate offence, is difficult as consolidated data has not been validated. It is possible that double capture of the same data has occurred by more than one agency.

However, it is likely that the value associated with fraud has significantly increased to $700M-$1B annually. This value is likely to continue to rise.

Transnational money laundering

New Zealand's transnational organised crime (TNOC) strategy[14] has a vision that 'We want New Zealand to be the hardest place in the world for organised criminal groups and networks to do business'. The TNOC strategy has a prevention focus which is why New Zealand's AML/CFT (anti- or prevention system) has an important role in strengthening our resilience to transnational organised crime. Money laundering enables organised crime, both domestically and internationally.

Transnational money laundering involves the movement of proceeds of crime from one country into another. Criminals recognise that moving these proceeds across borders almost guarantees that confiscation will not occur. This is due to challenges associated with the incompatibility of legal frameworks, geopolitical sensitivities, language difficulties, and the trust that exists between countries.

New Zealand has experienced transnational money laundering and the volumes involved have been significant. Our largest forfeitures all relate to foreign-generated illicit wealth derived from fraud and corruption. In these instances, we have seen deliberate placement of illicit wealth into New Zealand; this demonstrates that our economy and vulnerabilities are attractive to foreign criminals.

Where is this foreign-generated illicit wealth coming from?

The following cases involve more than $257M identified in New Zealand or under the control of a New Zealand legal person. The property described as follows is the subject of restraint (pending forfeiture) or has been forfeited. Countries from the Americas, Asia, and Europe were involved.

- It is alleged[15] that an individual is the beneficial owner of limited partnerships and trusts formed in New Zealand. These were used to receive $10M derived from corruption and fraud offences that occurred the United States. The funds were sent to New Zealand banks via Hong Kong, through the banking system. The intention was that the funds would be invested in New Zealand. These funds are restrained pending forfeiture.
- An individual was involved in the 'OneCoin' scam, a cryptocurrency Ponzi scheme. This scam is believed to have raised $6.5B through victims being scammed into investing in fraudulent cryptocurrency. Funds were sent to New Zealand from Europe via the United Arab Emirates (UAE). Funds were used to purchase vehicles and property in New Zealand. The vehicles and property with a collective value of $2.5M were purchased in the name of a nominee.
- A Russian national operated a cryptocurrency exchange in the United States. The exchange operated in the absence of any form of AML/CFT controls. The individual fled to Greece from where he was extradited to France then convicted of fraud and money laundering. From France, he was extradited to the United States where he has been convicted for a range of offences including money laundering. He awaits sentencing.

The individual held funds to the value of $140M NZD in a Russian bank; most of these funds were held in the name of a nominee legal person established in the Seychelles. However, the Russian account was controlled by a New Zealand established legal person. Police restrained the funds of the New Zealand legal person, on the basis that they were in possession of proceeds of crime. The High Court of New Zealand directed that the legal person repatriate the funds to New Zealand. The funds were returned to New Zealand and are pending forfeiture.

[14] Transnational Organised Crime in New Zealand – Our Strategy 2020-2025

[15] This matter is still before the High Court of New Zealand.

- An individual from Canada committed a series of frauds in China and directed the proceeds to New Zealand bank accounts; their intended purpose was for investment in hotels. Some of these funds came into New Zealand via an Auckland money remitter. Some of the funds were transferred from New Zealand bank accounts to Canada. However, $70M NZD was identified, restrained and subsequently forfeited.
- Two New Zealand citizens were the architects of an illegal website operating in the United States. The website sold illegal copyrighted materials. Proceeds from this offending were sent to New Zealand via PayPal. Funds were then deposited into bank accounts and used to purchase cryptocurrency. The confiscated cryptocurrency when sold was valued at $22M.
- An individual transferred $17M NZD to an accountant/lawyer for the purpose of investment. The beneficial owner is the spouse of a convicted lawyer, convicted in relation to money laundering and corruption. The convictions occurred in the United States and related to offending in a South American country. The funds are restrained pending further orders of the High Court.
- A nominee of a corrupt Indonesian official purchased a property in Queenstown. The official was convicted of offences in Indonesia. The property was forfeited in October 2023 – the value of the property exceeds $4M.
- An individual committed frauds in Malaysia and transferred the proceeds of those crimes to New Zealand. The individual was convicted in Malaysia and$1.8M was forfeited in New Zealand.

These examples demonstrate the volumes of cross-border transfers of illicit wealth occurring. New Zealand's financial system is highly interconnected with economies around the world; significant transfers occur every day. Over the last five years, $16.9B was transferred into New Zealand from the UAE.[16] $180.3B was transferred from Hong Kong[17] to New Zealand. As described with these examples within this international funds flow, are proceeds from crime that have occurred in various parts of the world.

Countries of concern

Proceeds of crime can emerge from any country; however, the following countries have publicly been identified as having weak AML/CFT systems at this point in time:

BLACKLIST

- The Democratic People's Republic of Korea (DPRK), due to proliferation financing risk.[18]
- Iran, for failure to address strategic deficiencies in its AML/CFT system.[19]
- Myanmar, for failure to address strategic deficiencies in its AML/CFT system.[20]

CHECK COUNTRY RISK

These lists are reviewed three times a year, and are subject to change.

Current lists are available at:
www.fatf-gafi.org/en/countries/black-and-grey-lists

Country risk should not be determined on the FATF lists alone.

A country's Corruption Perceptions Index is another useful resource to determine country risk – refer to www.transparency.org

[16] The United Arab Emirates was identified as a country with weak AML/CFT controls and was placed on Financial Action Task Force (FATF) 'grey list' in 2022. In response, the United Arab Emirates made significant change and was removed from the list in 2024.

[17] Refer to US Transfers, page 17.

[18] Refer to Chapter 6: Proliferation Financing, pages 90-95.

[19] Refer to Chapter 6 Proliferation Financing, pages 90-95.

[20] Refer to Myanmar, pages 29, 78, 83 and 84.

[21] Refer to Chapter 5: Terrorism Financing, page 79.

[22] Refer to Chapter 2, page 24.

[23] Refer to Chapter 5: Terrorism Financing, page 72.

[24] Refer to Chapter 2, page 23.

Foreign request for intelligence from New Zealand

Countries requesting information and intelligence from New Zealand most frequently include Australia, the United States, the United Kingdom, Singapore, the Cook Islands and Fiji.

The most common reasons for requesting information related to money laundering, fraud, drug dealing, foreign corruption and tax evasion.

Investor Visa Programmes (Immigration)

During the six years between 2018 and 2024-25[25], 143 Investor Visa applications were received. During this same timeframe, 58 were declined. Applications are processed by immigration officers but usually submitted by licensed immigration advisors or law firms.

Although data on the reason for why each visa application was declined is not available for this NRA, general reasons for declining include character grounds, and where the applicant cannot demonstrate ownership of their nominated funds or that the funds to support their application has been earned legally.

Investor 1 visas require an investment of $10M.

Chinese nationals accounted for the most Investor 1 visas issued over the past 10 years, investing a total of $1.94B.

They also accounted for the most Investor 2 visas ($3M) issued, with a total investment of $3.8B.

Other leading nationalities included the United States, Great Britain, Hong Kong, Germany, Singapore, Japan, South Africa, Malaysia and France.

This data demonstrates the attractiveness of New Zealand to live, work and invest.

Between 2018-2023, the FIU disseminated 314 reports to foreign FIUs. These referenced 1,101 SARs, 129,245 PTRs and 12 BCRs. An additional 52 dissemination reports were provided to agencies domestically which referenced relevancy to the 'Overseas Investment Act' – these reports referenced 836 SARs and 8,969 PTRs.

Examples of the sectors identified through transnational money laundering investigations

Persons involved in transnational money laundering used:

Banking: To transfer funds to or from New Zealand through the regulated banking system.

Accounting practices / Trust or Company Service Providers (TCSPs):[26] To establish companies and trusts. They establish these to obfuscate beneficial ownership of funds and assets, including for companies, by using nominee directors and shareholders.

Law Firms: As they need conveyancing lawyers for property purchases.

Real Estate: To integrate criminal proceeds into New Zealand property.

VASPs: To remit funds through cryptocurrency wallets.

Estimation of the value of proceeds generated from foreign illicit activities

The amount of foreign-generated wealth that moves in and out of New Zealand is unknown. Recent experience is that the values identified and seized have been significant as foreign criminals have been attracted to New Zealand. This demonstrates that transnational money laundering is a reality for New Zealand. Our risk is not limited to gang members and other criminals in our cities but also includes highly innovative international criminals, who conduct very serious crimes around the globe and then seek to use our country to provide safe harbour.

Other notable crime

TAX NON-COMPLIANCE[27]

Although not a high-threat crime, non-compliance with the New Zealand tax framework can derive financial gain through operating outside of the tax system.

Importantly, financial benefit from this type of crime is often indiscernible from the recognised high-threat crimes such as fraud or drug crime which is why it is notable.

Like drug crime, tax non-compliance can be observed through the apparent unexplained accrual of wealth or cash-intensive financial behaviours.

[25] To 2 April 2024.

[26] See Chapter 4: Risk Associated with Legal Persons and Legal Arrangements, and TCSP vulnerabilities, page 69.

[27] Refer to page 26, this chapter – tax non-compliance is discrete from tax-related fraud. Criminals involved in fraud, drugs or other income-generating crime do not habitually declare that income for tax purposes. An AML/CFT system that has high vigilance for tax non-compliance enables the identification of undetected predicate crime.

PROPERTY CRIME

Robbery, burglary, theft of vehicles and other property occur in high volume across New Zealand and is therefore a notable type of crime. Although some of these crimes are high-value, the majority derive limited proceeds when contrasted with fraud and drug crime. Often the proceeds of such crimes are self-consumed, transacted with third parties in payment for drugs, or sold for cash. Criminals depositing foreign cash (the proceeds of theft or burglaries) or undertaking suspicious financial activities, inconsistent with the normal patterns of behaviour, may be indicators of involvement in property crime. Laundering associated with property crime and drug crime is likely to be consistent and undiscernible.

Lower-threat crime

CORRUPTION AND BRIBERY

New Zealand is regarded as having one of the lowest levels of corruption in the world. The Serious Fraud Office (SFO) is the lead law enforcement agency for investigating and responding to corruption and bribery. A small number of persons are investigated and convicted for corruption and bribery offences in New Zealand. The SFO has not pursued prosecution of money laundering against those offenders. The volumes and value of this offending is low in contrast with the three high threat criminal behaviours described in this NRA.

HUMAN TRAFFICKING

Human trafficking has been identified in New Zealand; however, at very low levels. In March 2020 a person was convicted for trafficking ten people, and related slavery charges. He was sentenced to 11 years imprisonment and ordered to pay $183,000 in reparations to his victims. The low occurrence of this type of criminal behaviour presents low threat to New Zealand's AML/CFT system.

MIGRANT EXPLOITATION

This type of crime is being exposed with increasing frequency. The main industries involved include horticulture/viticulture, construction, retail, hospitality, cleaning, dairy farming, security. Migrants often pay significant amounts of money to offshore agents to secure visas and employment, with these agents colluding with New Zealand-approved employers to sponsor migrants into New Zealand. In context, the threat to New Zealand's AML/CFT system from this type of offending is low.

FISHERIES CRIME

No threat to the New Zealand AML/CFT system occurs when illegal fishing occurs involving foreign vessels who remove fish from New Zealand waters and sell or process that illegal catch in foreign jurisdictions. This is because the proceeds of such offending do not enter New Zealand's financial system.

Domestic fisheries crime involving the domestic black-market sale of illegally harvested fish presents a threat to the New Zealand financial system. The Ministry of Primary Industries identify that some domestic fisheries offending is organised and involves gangs who sell illegally caught fish for cash. Although the value of such offending could be in the millions, such offending is considered low-threat when contrasted with drugs and fraud.

ILLEGAL GAMBLING

Illegal gambling is not a widespread criminal behaviour in New Zealand. However, in May 2024 a prosecution was initiated in relation to an illegal lottery that involved $11M. Supporting this prosecution, Police initiated proceeds of crime proceedings and three residential properties; bank account contents; vehicles; motorcycles; and a boat were restrained. Although this example is high-value, most occurrences of this crime type are of modest value.

FIREARMS TRAFFICKING

There is demand for illicit firearms across New Zealand. Illicit firearms are routinely seized by police in drug and organised crime investigations and Police have dedicated resources to investigate the illegal sale and supply of firearms. The value of proceeds generated annually from trading in illicit firearms is not precisely known. In contrast to drug and fraud crime, which generate hundreds of millions annually, the value associated with firearms trafficking is likely to be moderate. This is a crime type which will be monitored.

ENVIRONMENTAL CRIME

Environmental crime associated with dumping or waste, illegal mining, and the trade in wildlife are significant issues regionally and globally. Within New Zealand, there is limited information regarding environmental offences from which profit is derived. In the absence of such information, it is considered that these types of crime present low threat to New Zealand's AML/CFT system.

SECURITIES CRIME

Securities offending (insider trading etc.) involve very low frequency offences in New Zealand. Money laundering related to these types of crimes is therefore limited, meaning this type of crime presents a limited threat to New Zealand's AML/CFT system.

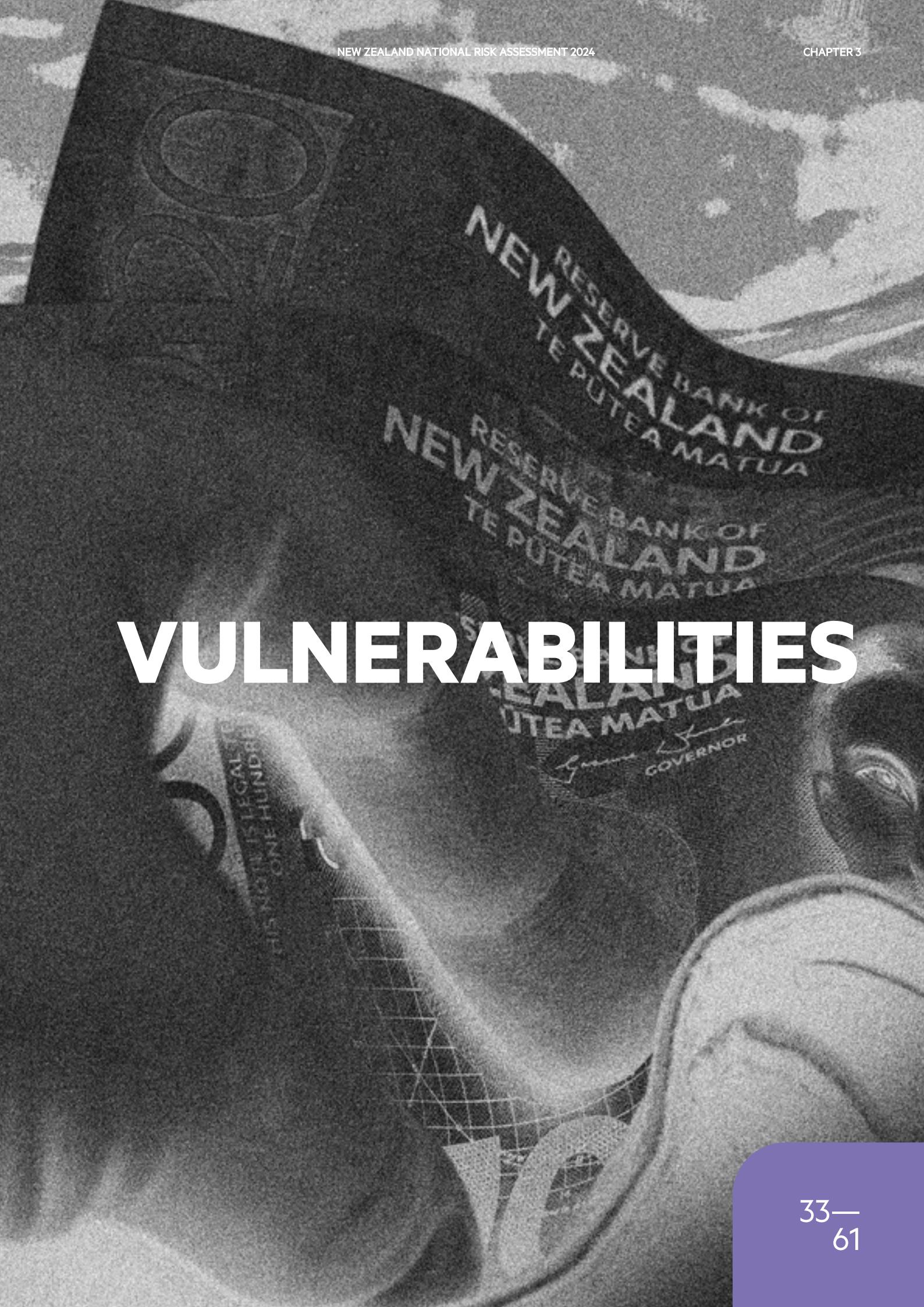
CHILD EXPLOITATION

Child exploitation for commercial reward occurs in low frequency in New Zealand. This type of crime is often international in nature with New Zealanders purchasing child exploitation materials from offshore providers. Leading

countries which host servers that contain online sexual abuse and images include the Netherlands, the United States, Slovakia, Russia, Chinese Taipei, Hong Kong, Bulgaria, Thailand, France, and Malaysia. Payments are often low value, and the proceeds of the offending is receipted in foreign countries. The proceeds of the offence are 'live proceeds' when they move from the New Zealand purchaser's account for remittance to the provider in a foreign location. The transfer of these proceeds across the New Zealand border is an ML offence. This type of crime is deplorable, but the value and volumes associated with this type of crime is low when contrasted with fraud and drug crime.

KIDNAPPING / MURDER / OTHER VIOLENCE

There have been occasional crimes of violence that were financially motivated. The value associated with this limited number of crimes is negligible. ML threat associated with these types of crimes is considered low.



VULNERABILITIES

Sectoral vulnerabilities summary

All sectors have vulnerabilities. Some have recognised vulnerabilities as they feature in high-threat criminal activities identified through intelligence and investigations. Vulnerability is greatest when the sector offers services of depositing, withdrawing and transfer (domestically and internationally) of funds that could be criminal proceeds.

35 sectors have been profiled in this NRA. Highest-risk sectors are most accessible and/or provide these services in the largest value and volume, making detection of money laundering more challenging. Others are vulnerable because an absence of information prevents comprehensive risk understanding. Recognising knowledge gaps is a valuable output for an NRA.

The three sectors considered most vulnerable and most used by criminals are banking, MVTS, and VASP. This NRA acknowledges the higher risk of these sectors, but reinforces every sector needs to be vigilant and proactive when customers and their transactions are considered suspicious.

Excluding proceeds of crime from the financial sector is a shared responsibility of banks and DNFBPs, also known as gatekeepers (accounting practices, law firms, real estate agents, trust and company service providers), MVTS, VASPs, HVDs, and to a lesser extent, the lower-risk sectors.

Data related to confiscation from drug crime (for January 2018 - December 2023) identifies that real estate, cash and vehicles feature in the three most common types of property confiscated.

In relation to fraud and money laundering (mostly foreign-generated illicit wealth or transnational ML), confiscations of funds recovered from bank accounts and real estate dominate. When property is recovered from these sectors, it confirms criminals are using these sectors to place criminal proceeds.

Virtual assets valued at $33.8M have been restrained and $29M have been confiscated.

Tables 4 and 5: *Confiscation data (Jan 2018 to Dec 2023).*

DRUG TYPE	CASH	BANK ACCOUNTS	REAL ESTATE VALUE	VEHICLES VALUE	JEWELLERY, PRECIOUS METALS AND GEMSTONES VALUE	SHARES/ INVESTMENT/ BONDS VALUE
Cannabis	$5,596,744.08	$2,643,567.44	$97,426,500.00	$4,273,167.92	$921,330.10	$705,357.30
Cocaine	$256,382.89	$1,078,301.07	$4,845,000.00	$2,195,900.00	$6,599.00	$0.00
MDMA/Ecstasy	$479,798.93	$50,238.01	$1,525,000.00	$299,180.00	$0.00	$0.00
Meth	$33,814,844.95	$5,272,233.10	$78,817,880.00	$21,428,330.98	$3,278,575.75	$906,799.00
Other Drugs	$1,806,411.34	$30,928.25	$6,365,000.00	$418,032.48	$531,797.20	$0.00
GRAND TOTAL	$41,954,182.19	$9,075,267.87	$188,979,380.00	$28,614,611.38	$4,738,302.05	$1,612,156.30

OFFENCE TYPE	CASH	BANK ACCOUNTS	REAL ESTATE VALUE	VEHICLES VALUE	JEWELLERY, PRECIOUS METALS AND GEMSTONES VALUE	SHARES/ INVESTMENT/ BONDS VALUE
Deception/ Fraud	$7,160,688.58	$2,185,902.52	$49,079,208.11	$3,560,375.00	$24,000.00	$0.00
Money laundering	$2,965,760.44	$176,643,445.64	$48,226,000.00	$3,787,270.00	$400,339.00	$0.00
Tax crime	$1,357,780.96	$1,950,579.27	$12,679,000.00	$760,000.00	$0.00	$81,613.81
GRAND TOTAL	$11,484,229.98	$180,779,927.43	$109,984,208.11	$8,107,645.00	$424,339.00	$81,613.81

Banking

Banks are ubiquitous in New Zealand towns and cities. There are 27 registered banks nationally: 18 incorporated in New Zealand, and 9 operating as branches of overseas-incorporated banks. There are over 2100 ATMs operating in New Zealand, and over 670 bank branches; however, bank branches are on the decline. Banking includes Non-Bank Deposit Takers (NBDTs), like credit unions, that provide more limited but similar services and products to banks.

The banking sector remains most vulnerable. Through profiling crime threats, banking was identified as the sector most exploited for money laundering.

This is due to the sector's size and complexity, which create an environment where money laundering can occur: banking products are easily accessible; bank accounts are the primary gateway for other sectors to gain access to the financial system; and transactions occur at volume. The banking sector is primarily vulnerable to the placement and layering stages of money laundering, e.g., cash deposits into bank accounts, domestic and international wire transfers, and currency/denomination exchange[28]. Added to this, customers demand transaction speed, given transaction speed is critical to commerce and efficient business. Speed means transaction transfer and layering can efficiently be undertaken at high velocity.

Retail transactional bank accounts, credit cards and international wire transfers are the highest-risk, or most vulnerable, products related to ML/TF. The ability to operate these products and services via self-service internet banking, without the need for physical contact or bank assistance, makes these products particularly susceptible to misuse for money laundering. Similarly Smart ATMs allow placement of illicit cash into the financial sector without the need to interact with a bank employee within a branch. The decline in branch numbers, and the increase nationally of smart ATMs increases this vulnerability.

Fraud is high threat. Most fraud occurs within, and is facilitated by, the banking system; most have elements of both customer and criminal behaviour; and it is recognised that it is difficult to detect and prevent fraud. It is also recognised that other types of crime enterprise, like any business, rely on an efficient banking system reinforcing the vulnerability of this sector.

Banks offer numerous products that could be misused to launder illicit proceeds. Of recent concern is customers establishing banking facilities that are then used by other parties to receive and transfer funds. These 'mule accounts' are often identified as accounts legitimately opened by temporary visa holders, who then depart New Zealand with the account operation continued by a criminal.

This strategy is a way for criminals to conceal their identities and the source of their illegal funds, and to evade the customer due diligence (CDD) measures that would otherwise raise red flags. The use of money mules also allows criminals to create layers of distance between them and their victims, making it more difficult for law enforcement to quickly reconstruct the movement of funds to a criminal to enable recovery.

According to the 2023 RBNZ Registered Banks Annual Report, non-resident individual customers accounted for 7.95% of the customer population, and non-resident entity customers accounted for 5.85%.

Other mule accounts are established by customers who then provide their account to a criminal or offer its use to a criminal for a fee. This is a high-risk practice and often the customer is deceived into this activity as part of a scam or fraud. Understanding account behaviour to identify changes in how an account operates is critical to the identification of mule accounts. The banking sector dominates submission of suspicious activity reports (SARs).

[28] This can involve the 'refining' the exchange of small denomination notes for larger denomination notes to reduce both weight and volume.

SAR Review

**Although 27 Banks are registered, 7 are part of Designated Business Group, and would not be expected to report a SAR.*

The maximum number of reporting banks is 20.

Table 6: *SAR Review: Banking.*

TIME PERIOD	No. SARs REPORTED	No. OF ENTITIES REPORTING SARs*
01 January 2020 to 31 December 2020	9,933 SARs	19
01 January 2021 to 31 December 2021	11,584 SARs	18
01 January 2022 to 31 December 2022	11,077 SARs	16
01 January 2023 to 31 December 2023	12,233 SARs	20

2023

The most common reason for reporting in 2023 was suspected 'scam/fraud proceeds' received into a bank account. The second most common type of report related to cash deposits. Cash is the enabler within the illicit drug and stolen property marketplace; it also enables tax evasion.

Other types of reporting related to:

- the rapid movement of funds
- third party deposits
- reports referencing that the source of funds used in the transaction was unknown

Less frequent reporting included:

- the receipt or sending of funds from high-risk jurisdictions
- individuals who were suspected of being fraud or scam victims
- large volumes of cash withdrawals, and low-value payments suspected of being related to funding the access to child exploitation material
- cryptocurrency purchase/trading
- national security concerns

The wide range of reporting indicates broad awareness of types of reporting that should occur. This is positive.

2023 SAR reporting reflects that the AML/CFT system is already responding to the emerging threats around frauds and scams. It is acknowledged that reporting all frauds will likely significantly increase reporting volumes; however, this reporting would deepen understanding about how the AML/CFT system can become more resilient to this type of crime.

Bank customers could be victimised by the same scam or offenders; however, without centralised reporting that detects this activity, identification of all offending is less likely. Such reporting also needs to be consolidated and quickly analysed. Improved understanding is critical for development of countermeasures to prevent occurrence and victimisation, and ultimately reduce the need for reporting this type of criminal activity.

2022

Analysis of all banking sector reporting in 2022 again reflects that reports of scams and frauds dominated. The second most common reason for reporting again related to large cash deposits.

This was followed by: cash withdrawals, high-value domestic transfers, national security concerns, cash deposits followed by immediate transfers to other accounts, cash deposits rapidly transferred to remitters, high-value wire transfers, funds received from China (given China's currency control measures), and funding access to child exploitation.

There is strong consistency between 2022 and 2023 regarding frauds, scams and cash.

2021

Analysis of reporting in 2021 identified the most common reporting related to suspicious cash deposit(s). This was followed by suspected tax evasion. Other reporting related to payments for access to child exploitation material, scam/fraud victims, rapid movement of funds, national security concerns, high-value/excessive withdrawals, suspected fraudsters (including individuals who had received Covid-19 payments that had been spent on online gambling), high-value international funds transfer/s or IFT(s) received, and cryptocurrency purchase or trading.

2020

The most common reason for reporting in 2020 was large cash deposits, followed by unknown source of wealth. Other reporting related to money laundering concerns, large or high-volume international or domestic transactions, tax evasion, rapid movement of funds, scams and fraudulent activity, and payments to access child exploitation material.

The banking sector has boosted prevention initiatives in response to the increasing prevalence of scams and frauds. These include guidance delivered through online banking services, regarding scams and frauds as well as educational media campaigns.

Changing customer behaviour is central to reducing money laundering associated with frauds and scams.

Key vulnerabilities within the banking system include

LACK OF INFORMATION SHARING

New Zealand currently lacks the provisions to allow registered banks to easily share information about their customers and transactions between one another. As a result, reported intelligence forms in silos, preventing effective analysis. This inhibits sharing insights and potential prevention initiatives (the "anti-" in "AML") across the sector. The Financial Crime Prevention Network (FCPN) is a Public Private Partnership (PPP) initiative created to develop shared information and its members currently include the New Zealand Police, New Zealand Customs, Inland Revenue, Immigration NZ, ANZ, ASB, BNZ, Kiwibank, TSB and Westpac.

DE-RISKING/DE-BANKING

A reluctance by larger retail banks to provide banking services for high-risk industries and sectors may influence the development of unregulated underground sectors. Since behaviours of other sectors (and customers) influence the risk of the banking sector, simple de-risking can have the unintended consequence of displacement of high-risk activities into another bank or NBDT.

> A system that displaces risk is less effective than a system that identifies and responds appropriately to suspicious or criminal behaviours.

SMART ATMS

As New Zealand's bank branches and traditional ATM networks continue to decrease in numbers/availability and are superseded by more reliance on self-service products such as Smart ATMs. There is risk of any vulnerabilities identified by bad actors being exploited to place illicit cash into the financial system before detection and preventative controls are in place.

PTR

Prescribed Transaction Reporting requirements were incorporated into the AML/CFT regime in 2017. The Reserve Bank of New Zealand (RBNZ) continues to identify where entities have not challenged their system design when building their PTR solutions. In some cases, not all transaction types are correctly identified as reportable.

The PTR framework needs to be effective given:

- the recognised threat of transnational money laundering
- the occurrence of foreign criminals targeting New Zealand through scams and frauds
- that domestic supply of illicit drugs is reliant on those drugs being purchased from the international drug market (requiring offshore payment).
- The value of such data as a collective source for analysis and detection of financial crime by the Financial Intelligence Unit.

A vulnerability is that the PTR threshold, set at $1000 for international electronic transfers and $10,000 for cash, excludes reporting of high volume-low value transactions that may be used by criminal networks to evade detection.

The PTR framework also should not operate the default mechanism which absolves regulated financial market participants of any further obligation to detect, deter and report suspicious financial activity.

> Since the last NRA, two banks were formally warned for PTR non-compliance. Proceedings were also filed for various non-compliance under the AML/CFT Act.

COMPLACENCY WITH SYSTEM DESIGN – A lack of ongoing testing/review of the systems used to detect ML/TF activity:

While systems may have been set up correctly, in compliance with international standards, these standards do not afford the protection that customers increasingly expect. The banking sector is challenged by the innovation of criminals and banking customers requiring further education on fraud prevention.

Another challenge is that the increasing threat of fraud suggests the design and operating effectiveness of the current AML/CFT system is not performing as circumstances now require. The FIU may therefore not be capturing all desired activity, from which policy and practice could be developed to make the banking environment more hostile to fraud, scams and other criminals.

Threats[29]

Investigations identified instances where banking services had been exploited with the aim of laundering proceeds of almost every crime type profiled for this NRA. For example:

- Cash proceeds of drug offending deposited into personal and/or business accounts operated by drug offenders as well as into accounts operated by their associates or third parties on their behalf or which they indirectly control. Illicit funds were occasionally layered through bank accounts held by offenders, associates, or third parties. These illicit funds were then wired offshore through banking facilities, or through on-line remittance services.
- Electronic proceeds of fraud offenses transferred domestically into mule accounts, internationally through the banking sector or through businesses providing on-line remittance services.
- Tax offenders deal with a mixture of cash and electronic funds. In some circumstances investigations identified cash was either simply spent or deposited for layering purposes into personal accounts. Electronic funds were spent or layered through accounts. Some tax offenders received cash from suppressed sales into their bank accounts deposited by their employees.
- Criminals involved in transnational money laundering transferred funds to New Zealand using banking facilities to make electronic transfers into lawyers' trust accounts to fund property purchases.

[29] See threat profile in Chapter 2 for more detailed information.

Money or Value Transfer Service (MVTS)

MVTS is identified as a key high-risk service. The sector consists of a few large multi-national businesses with agents across New Zealand. There are several other large multi-national businesses offering services to NZ customers online, with no physical presence in NZ.[30] However most of the sector are small to medium sized businesses typically servicing the remittance corridor, some of whom also offer currency exchange services.

Remittance is the transfer of money or value between individuals or companies in different locations. Money remitters are financial service providers who send and receive funds internationally for customers. There are 92 non-bank entities providing remittance services.

External to the regulated sector is an unknown number of unregistered remitters. These remitters are not registered on the Financial Service Providers Register and are not engaged with the AML/CFT obligations required. Determining the size of this portion of the sector is difficult; however, it is likely to be sizeable. This includes the use of bank accounts for which the purpose of the account was not declared to the bank. These money remitters are very high-risk and when identified, should be prosecuted for operating while unregistered on the Financial Service Providers Register.

As a sector, MVTS is exposed to transnational threats from organised crime groups operating domestically and internationally. These include international money laundering networks, persons involved with importation and distribution of illicit drugs, and persons who commit or move fraud proceeds. Much of this crime requires offshore transfer and/or transfer into New Zealand of criminal proceeds.

Many money remitters operating in New Zealand use informal money or value transfer systems, where international transfers are not transacted between countries through a formal banking messaging system (such as SWIFT). Rather, the money remitter (not a bank) controls and has overall visibility of the different parties to the transfer. Payments to the beneficiary in the destination country may be made by domestic payment (from a bank account held or controlled within that country). That account may be operated by the money remitter, by their agent in the destination country, or in some circumstances by an unrelated customer. Transferring funds internationally using an informal transfer system can occur at lower cost than remittance service through a bank, which is attractive to customers.

There are numerous methods and types of informal money or value transfer systems. They are common and not inherently unlawful. In different geographical regions, different names may be used such as ‘hawala’ in the Middle East, ‘hundi’ in India and ‘fei-chien’ in China. Sometimes the term ‘hawala’ is used more broadly to denote all methods of informal money or value transfer service.

The situation often arises when a money remitter does not have funds immediately available in New Zealand or the other country to make payment to a beneficiary. When this type of situation occurs, it is common to engage another (typically larger) money remitter to source the funds. This can include wholesale transactions, making or receiving payments to and from each other’s customers, as well as short term credit arrangements which are then settled through subsequent arrangements.

Use of informal money or value transfer systems has increased in demand in New Zealand and many parts of the world. Remitters who provide this service are often globally connected, and as a result, transactions can be simultaneously swapped across a series of countries.

For example, a customer located in China wants to remit funds to Australia; a customer in Australia wants to remit funds to New Zealand; and a customer in New Zealand wants to remit funds to China. In this scenario, respective customer needs are all paired in a way that allows for payments in each country to occur domestically via arrangement between remitters, without any funds crossing the borders through the formal banking systems of the three countries.

[30] Refer to payment providers, page 56.

A method that challenges PTR reporting frameworks (related to international transfer reporting requirements), and which operates at reduced cost because of the absences of the need to exchange currency, is the service of swapped remittance.

Swapped remittance

One type of informal money or value transfer service involves 'swap transactions' between unrelated customers of the same money remitter. In some circumstances two or more money remitters may work together to deliver the 'swap'.

For example, when a customer in New Zealand wants to send $5,000 to Australia and a customer in Australia wants to send $5,000 to New Zealand. The remitter facilitates exchange of funds between the two New Zealand parties and the same occurs in Australia. This results in the New Zealand customer making a domestic payment directly to the intended beneficiary of the Australian customer's inbound transaction to New Zealand. Funds do not cross the border through the formal banking system and the transfer can often be provided with much lower rate of foreign exchange.

These types of services make reconstruction of international funds transfer challenging, which in turn makes these services attractive to criminals when they are moving funds across borders.

The New Zealand - China corridor

China is New Zealand's largest trading partner with annual trade in 2023 valued at $17.2 B. The exchange of goods, services, money and people between New Zealand and China is substantial.

China operates strict currency control measures which prohibit its citizens from removing from China more than $80,000 NZD ($50,000 USD) for personal purposes per year without authority. All transfers must also be made through financial institutions approved to provide foreign exchange services. This policy is designed to prevent capital flight.

Informal money or value transfer systems are known in China as 'underground banking'. This includes 'swapped' transactions. These channels are used extensively to bypass Chinese currency controls, for example to transfer wealth to purchase property in New Zealand.

In New Zealand, there have been cases of money remitters offering services to facilitate money laundering: through offering anonymity to customers, no or lack of reporting, and a willingness to conduct business in large volumes of cash without complying with AML/CFT requirements.

SAR Review

Table 7: *SAR Review: MVTS.*

TIME PERIOD	No. SARs REPORTED	No. OF ENTITIES REPORTING SARs
01 January 2018 to 31 December 2023	35,068 SARs	35 Remittance Service Providers

Given the size of the MVTS sector compared to the banking sector, it reports a much higher percentage of its transactional activity as suspicious. Nearly 80% of this sector's reporting is from one large international remittance provider. This reflects that the large provider has robust internal controls to trigger reporting.

1206 SARs were sampled for 2023; analysis showed the largest proportion of reporting related to suspicion that a customer's account had received criminal proceeds or fraudulently obtained funds. The second most common reason was concern that the customer was a scam victim.

Other reasons included: multiple senders in New Zealand who appeared to share identification information, that the customer was suspected of being a money mule, suspicion of child exploitation, the sending of funds to high-risk jurisdictions, refusal to provide documents in relation to enhanced customer due diligence, and the use of false identification.

Compliance with AML requirements across larger multi national money remitters is recognised as relatively high, whereas smaller single corridor money remitters have demonstrated a lack of resources and/or knowledge in compliance with AML/CFT obligations. Given the risks associated with the MVTS sector money remitters require sound understanding of their risk and compliance requirements. This sector requires robust, ongoing and effective supervision.

In recognising this sector has elevated vulnerabilities, the AML/CFT system could respond with a strategy of de-risking this sector. However, this would adversely impact on a sector that has large volumes of legitimate transactional activity, including providing important financial support from migrant diaspora back to their home countries. De-risking could further isolate this financial activity outside of the central financial system, or encourage it to operate through nominee or mule accounts to disguise the operation of a remittance service. De-risking is only justified in response to specific customer risk activities as opposed to sectoral risk.

The DIA has issued 25 formal warnings to money remitters since 2014 and taken four civil proceedings against money remitters since 2017 for AML/CFT non-compliance.

It has undertaken two criminal prosecutions for AML/CFT non-compliance against money remitters. These prosecutions were taken due to serious AML/CFT non-compliance.

Threats

MVTS featured in half of the crime threats profiled for this NRA. Investigations across New Zealand have identified the use of witting and unwitting money remitters to launder and move crime proceeds.

- Drug offenders deal mostly in cash. Large volumes of cash were accepted by New Zealand based remitters who remitted the funds either through the banking system, or through informal money or value transfer systems (including swapped transactions). Some money remitters also provide cryptocurrency in exchange for illicit cash.
- Tax investigations identified offshore remittances by employees or associates of business owners engaged in tax offending, as well as the use of informal or money or value transfer systems, and remittances conducted in bulk on behalf of others.
- Individuals involved in transnational money laundering transferred funds to New Zealand using money remitters.

On 13 July 2020, Police commenced a money laundering investigation into a remitter's activities. This investigation was informed by the 2019 NRA.

The remitter was operating a money remitting and currency foreign exchange business in Auckland.

The business relied on informal systems to transfer funds between two countries. Transfers occurred outside of formal banking arrangements.

The remitter accepted deliveries of large amounts of cash. Funds were then electronically transferred into an overseas account controlled by the customer, or for the purchase of cryptocurrency.

This investigation and prosecution related to the laundered proceeds of illicit drug sales. $27.4m was laundered across 160 transactions between 3 July 2017 and 31 January 2020. The remitter was sentenced to seven years and six months in prison for money laundering.

Virtual Asset Service Providers (VASPs)

Virtual Asset Service Providers (VASPs) deal in virtual assets (VAs) – digital representations of value – that can be digitally traded or transferred and can be used for payment or investment. In New Zealand, there are 25 active registered VASP entities.

Virtual assets, including cryptocurrencies, are vulnerable to being misused by criminals to launder money, finance criminal activity, fund terrorism and fund the proliferation of weapons. Conducting transactions using virtual assets can allow anonymity, can have global reach that makes cross-border payments easier, and can transfer value at high speed.

VASPs provide services like banks (holding value) and remittance (transferring value overseas), but they are outside the existing banking system. VASPs can be exploited to enable cross-border payments (peer-to-peer transfers) for the transshipment of drug imports to New Zealand, and for the remittance of fraud proceeds out of New Zealand.

Criminal proceeds can be laundered via VASPs during on-ramping (the purchase of VAs),[31] the transfer of value between services/products/wallets,[32] or off-ramping (the sale of VAs). In New Zealand, the VASP sector provides products and services for the transfer of value as well as on/off-ramping. A single major global VASP operating in New Zealand facilitates peer-to-peer sales through providing a service with a matching engine to pair buyers and sellers on its platform. Cash and cryptocurrency are both recognised as high-risk in context of ML/TF.

Like money remitters, VASPs must be registered on the Financial Services Providers Register. However, there are a number of unregistered traders who trade peer-to-peer in cryptocurrency to the extent they are providing a financial service. These persons buy, sell and exchange virtual assets for customers; determining the number of these unregistered VASPs is difficult. Identifying unregistered VASPs is important given the risk recognised within this sector.

New Zealand has cryptocurrency ATMs[33] where users can deposit cash to purchase cryptocurrency or sell cryptocurrency for cash. These ATMs are particularly vulnerable to money laundering due to the lack of AML/CFT controls during on-ramping. ID verification is through biometric face scanning during use and presenting a government ID to the camera. Source of wealth checks are not undertaken.

Individuals deposit cash into the kiosk (ATM) which calculates the cryptocurrency amount based on the displayed exchange rate. Purchased cryptocurrency can be deposited into any wallet. As of June 2024, there were 157 cryptocurrency ATMs across New Zealand. These ATMs impose steep fees on transactions; Olliv is the sole cryptocurrency ATM provider in New Zealand and charges 15.99% per transaction. Better understanding of the volume and value of activity through these ATMs is urgently required.

SAR Review

Table 8: SAR Review: VASPS.

TIME PERIOD	No. SARs REPORTED	No. OF ENTITIES REPORTING SARs
01 January 2018 to 31 December 2023	891 SARs	5 VASPs

Only five of the 25 registered VASPs have submitted a SAR. 68% of the reported SARs were sampled – the most common reason for reporting was concern a client was a scam/fraud victim convinced to use cryptocurrency to invest in a fraudulent scheme or involved in the likes of a romance scam. The second most common reason was that the person was attempting to use magazine photos, a fraudulent driver licence, other false identification, or other altered documentation during onboarding. This was followed by individuals transacting with wallets relating to purchasing drugs or child exploitation material on the dark net.

[31] In New Zealand, on-ramping can be through payments (via debit card, bank transfer, or wire transfer) to a cryptocurrency exchange.
[32] A wallet is a software application which stores the information or digital credentials necessary to conduct transactions with cryptocurrency.
[33] The ATMs do not store cryptocurrency but connect to a Crypto Application Service server over the internet for exchange purposes.

Other reasons for reporting included: clients suspected to be money mules; transfers to the "fraud shop" (a website where stolen credit card information can be purchased); persons refusing to complete KYC/CDD or provide source of wealth documentation; cryptocurrency sent to Iranian or Russian exchanges; and in circumstances where it was suspected that a customer was sharing their wallet with another user.

Compliance with AML Requirements

The VASP sector is evolving and can change rapidly. The primary supervisor, DIA, has ongoing engagement with key stakeholders within the sector. Key players can emerge locally and create significant disruption to the market, and large global entities can enter the market (officially or simply by offering their services online without geographical restriction). Supervision of the sector has identified that enhanced customer due diligence and account monitoring are areas that could be improved.

Automated technology used within the VASP sector is the primary tool for mitigating risk. Changes to transactions or reporting processes can therefore often be implemented rapidly and universally without re-training staff or educating customers. This along with new processes and channels being created can cause unintended risks. This is compounded by the fact that virtual products are distinct from traditional financial services and transaction models, and there is often uncertainty about which regulations and obligations apply.

The DIA has taken an enforcement action against a VASP for non-compliance with AML/CFT policies, processes, and controls (inadequate or absent vetting, training, and review of risk understanding). Onboarding of customers occurred remotely, without sighting ID documents; the VASP did not comply with Identity Verification Code of Practice; and did not undertake adequate or effective CDD, account monitoring, ECDD, or obtain source of funds when required. The entity agreed to cease operations and no longer operates in NZ.

Threats

Investigations in New Zealand have identified misuse of VASPs to launder and move proceeds of crimes including drug, fraud and other offending:

- Drug offenders used cryptocurrency ATMs to launder cash from drug sales. They also used money remitters to purchase cryptocurrency with illicit cash and transferred this value to wallets held in other jurisdictions.
- Fraud offenders convinced New Zealanders to purchase cryptocurrency for investment in fraudulent schemes. Romance scam victims purchased cryptocurrency to send to mule wallets, or to the scammer's wallets in other jurisdictions. Victims in New Zealand also wired large volumes of funds offshore, believing they were investing in cryptocurrency.
- Virtual assets can be purchased offshore and placed into wallets owned by persons in New Zealand, in payment for criminal goods and services.

Between September 2015 and 2022, an individual was identified who was brokering the purchase and sale of Bitcoin via a cryptocurrency platform. He was transacting through his own bank accounts, those held by family members and other associates, or directly between the trading parties. He generated a commission from such activities.

In excess of $7m was deposited into bank accounts and subsequently traded. He purchased Bitcoin via a cryptocurrency platform, and transferred Bitcoin to the wallets of criminal organisations and third parties. He was not a registered financial service provider, nor was he compliant with AML/CFT requirements. It was evidenced that he laundered large sums of cash from various criminal organisations, using registered money remitters to deposit cash and transfer funds electronically into bank accounts in China held by himself and his associates.

From the commission he earned from this activity, he purchased real estate, motor vehicles and a boat via his family and associates' bank accounts, and likely through his personal Chinese bank accounts. He was successfully prosecuted for money laundering, obtaining by deception and providing an unregistered financial service. Property to the value of $3.5M is currently pending a confiscation proceeding.

G and H were involved in importing and distributing illicit drugs. Restrained from these persons was a range of different types of cryptocurrencies (the majority was Bitcoin). In January 2024, the cryptocurrency had a value of approximately $1M. Also restrained were four vehicles and two Harley Davidson motorcycles, all purchased with cash or via bank accounts that had received cash.

H purchased cryptocurrency from his New Zealand bank accounts from two global companies. G purchased the illicit drugs that were imported using cryptocurrency – the investigation identified he was the largest vendor, selling illicit drugs over the dark net within New Zealand. He received payment in cryptocurrency.

The criminal charges and confiscation proceedings are still before the courts.

Sectors being misused by criminals

Designated Non-Financial Businesses and Professions (DNFBPs)

The legal, accountancy and real estate sectors are known as designated non-financial businesses and professions (DNFBPs) or more commonly as "gatekeepers". This term refers to their role in providing services and products that can facilitate entry of illicit funds into the legitimate financial system.

Gatekeepers can provide access to specialist services, knowledge, and techniques, as well as an impression of respectability and normality. Although the DNFBP sector has AML/CFT compliance responsibilities, its transactions should not be assumed to have been subject to robust AML/CFT compliance checks.

New Zealand's AML/CFT system will be strongest when every sector independently applies a robust review of transactions and activities – this is particularly important for the DNFBP sectors.

Law firms and conveyancers

There are 1267 active reporting entities within the sector. Their sizes vary from single person firms to large law firms (>100 employees).

In addition, there are approximately 25 registered conveyancing practitioners or firms that solely provide conveyancing services. Conveyancing practitioners are regulated by the New Zealand Society of Conveyancers and only provide conveyancing services.

Lawyers who operate trust accounts are subject to oversight by the New Zealand Law society. This has the aim of ensuring proper conduct in respect of clients' money. This protects risk to the Lawyers' Fidelity Fund rather than AML/CFT compliance.

It is likely there are more law firms that are reporting entities but not known to the supervisor (the DIA). This is because there is no requirement to advise or register with DIA as a reporting entity if a law firm provides activities captured under the AML/CFT Act.

These activities include conveyancing; managing client funds, accounts, securities, or other assets; trust and company formation services including providing a registered office, business correspondence, or administrative address for a company, partnership, or any other legal person or legal arrangement; acting as, or arranging for, someone to act as a nominee director/nominee shareholder/nominee general partner, or trustee; and engaging in or giving instructions on behalf of a customer for specified services.

SAR Review

Table 9: SAR Review: Law firms and conveyancers.

TIME PERIOD	No. SARs REPORTED	No. OF ENTITIES REPORTING SARs
01 January 2018 to 31 December 2023	614 SARs	240 law firms

Only 20% of reporting entities from this sector have reported a SAR. Of the 614 SARs reported, 44% related to a property transaction – the most common concern was the client not providing CDD or KYC information, or source of wealth information related to the purchase of property. After property transaction related SARs, the next common reasons were unexplained source of funds from offshore, and then clients with adverse media or criminal links.

Other types of reporting related to:

- overpayment to the lawyer's trust account
- suspicion that clients were subject to a scam that required sending funds offshore
- circumstances where the client was expecting funds from offshore for a property purchase.

Less frequent reporting included:

- clients providing inconsistent information
- suspicious loan agreements
- refunds to third parties
- and when unexplained cash was used to purchase property.

The level of reporting and content of suspicious reports from this sector indicates law firms are cognisant of suspicious activity indicators, and recognise risk associated with property purchase. Reporting indicates that the requirement to produce source of wealth documentation appears to be dissuading some criminals from exploiting this sector to launder criminal proceeds.

Conveyancing services are a recognised area of risk across most proceeds of crime investigations. Conveyancing entities have visibility over property transactions that often move through a lawyer's trust account. Lawyers are therefore critical gatekeepers in preventing illicit wealth from entering the real estate sector; improved reporting could emerge from this sector.

Since 2019, six formal warnings have been issued to law firms non-compliant with their AML/CFT obligations.

Threats

Investigations in NZ have identified misuse of products and services offered by lawyers to launder and move the proceeds of crimes:[34]

- Drug offenders deposited illicit cash into a lawyer's trust account for purchasing real estate and vehicles.
- The lawyer established trusts that became the registered owners of property purchased with criminal proceeds. The bank accounts linked to these trusts were also used to launder proceeds of drug offending. The lawyer was the trustee, thereby distancing the criminal from the property and bank account. The lawyers coached drug offenders on the amounts of cash deposits that would trigger PTR reporting (the lawyer was prosecuted for money laundering).
- A fraud offender engaged a law firm to establish a trust then used the trust to conceal beneficial ownership of property purchased from the proceeds of a fraud. The fraud victim was the New Zealand Government.
- Individuals involved in tax offending used legal arrangements (power of attorney) to conduct purchases on behalf of others. Law firms were involved in the purchase of multiple properties.
- Individuals involved in international money laundering engaged lawyers for property purchases in New Zealand involving personal lending contracts and fraudulent loans.
- A lawyer's trust account was the recipient of funds disguised as loans from offshore third parties (that were in fact proceeds of crime). The loans were then used to fund property developments.
- Cash was deposited via ATMs in Asia then transferred to a New Zealand solicitor's trust account for payment to a barrister. The barrister was representing a client facing criminal proceeds recovery proceedings.
- Cash deposited into the trust accounts of instructing solicitors (to pay criminal barristers for criminal defence services associated with high-threat predicate crimes) has obvious risk. In the presence of criminal disclosure (which informs of the allegation of criminal behaviour), the barrister is likely well-informed of the risk associated with receiving funds directly or indirectly to make payment for the legal services they provide. s243 (3) of the Crimes Act 1961, provides for the offence of money laundering in that everyone (which would include an instructing solicitor and/or barrister) who obtains or has in his or her possession any property (being property of an offence committed by another person), knowing or believing that all or part of the property is the proceeds of an offence, or being reckless to whether the property is the proceeds of an offence, is liable to a term of imprisonment not exceeding 5 years.

Instructing solicitors and barristers have higher vulnerability for receiving criminal proceeds, when paid by clients (directly or indirectly) to fund criminal litigation and the litigation is associated with income-generating crime such as those described as high-threat crime in this NRA.

CASE STUDY

A lawyer was instructed to incorporate a company in NZ; set up a foreign trust in NZ; become a professional trustee of the trust; and become director of the company. The beneficiary of the trust was the wife of an individual prosecuted in a foreign jurisdiction for corruption. Funds to the value of $17 million were transferred to New Zealand.

These funds have been restrained by the High Court on the basis that the funds are believed to be part proceeds of corruption, and have therefore been laundered into New Zealand. This matter remains before the High Court and demonstrates that criminals in other parts of the world will seek to invest illicit wealth into the New Zealand's economy.

[34] Note: Risk Associated with Legal Persons and Legal Arrangements, and TCSP sectoral vulnerabilities, are described in Chapter 4. Refer to that chapter, noting accounting practices can provide TCSP services.

Real estate agents

There are 923 active reporting entities in the real estate sector. The sector is broad; some agents are sole operators, while others are employed by large businesses or franchises. Real estate agents are important gatekeepers as they have direct involvement in the sale and purchase of real estate. Real estate is proven to be a sought after asset type by criminals.

In the real estate sector, CDD obligations generally extend only to the vendor (the seller) not the purchaser. However, reporting obligations apply in relation to either party. 44% of SARs reported by lawyers relate to property transactions where individuals want to purchase real estate without providing source of wealth documentation, reflecting that the legal sector is also a critical gatekeeper for the purchaser.

Real estate as a property type can be used for money laundering, primarily during layering and integration of the proceeds of crime. This includes renovating with illicit cash; repaying mortgage debt with illicit cash; manipulating purchase price between a complicit vendor and purchaser; and using legal structures to conceal beneficial ownership. Nominee ownership may also occur to navigate foreign buyer rules.

Although CDD obligations generally only involve establishing the identity and monitoring transactions of the seller, and some of the described activities may be outside of the purview of real estate professionals, suspicious activity reporting obligations still apply in relation to both the vendors and purchasers of real estate. Making New Zealand a safer country is a responsibility of everyone.

SAR Review

Table 10: *SAR Review: Real estate.*

TIME PERIOD	No. SARs REPORTED	No. OF ENTITIES REPORTING SARs
01 January 2018 to 31 December 2023	555 SARs	107 real estate agencies

Slightly more than 10% of the sector has reported a SAR. 25% were sampled and reviewed. The most common reason for reporting was the vendor's avoidance to complete CDD/EDD. The second most common reason was concern that the property was purchased and sold within a short timeframe.

Other types of reporting related to:

- a client's use of a trust
- the use of offshore source of funds for the initial property purchase
- reported clients being possibly victimised by scams or frauds.

Less frequent reporting included:

- adverse media in relation to the client
- property sold below value
- unusual/evasive behaviour
- the vendor having gang links.

Between January 2018 and December 2023, real estate was the third most commonly restrained asset in New Zealand (after cash and vehicles). During this time, Police restrained 339 residential properties; the total restrained properties (when including commercial property, farms/orchards, and lifestyle blocks) was 418.

Real Estate Institute data identifies that 63,361 residential properties were sold in 2023. This was a slight increase on 2022. In contrast to these sale volumes, sector reporting averages 100 SARs per year. This indicates an opportunity to improve the number and quality of SAR from this sector.

Non-compliance has been identified in more complex AML/CFT obligations such as the exact timing of when verification must be completed. In these instances, entities were requested to remediate issues. Between January 2018 and December 2023, there were five enforcement actions undertaken in the real estate sector related to deficiencies in AML programmes. Five formal warnings were given: three public and two non-publicised. Remediation is ongoing for several entities.

Threats

Insights from investigations in New Zealand have identified real estate purchases across almost half the threats profiled for this NRA:

- Drug offenders integrated their criminal proceeds into property. They also renovated properties by using illicitly obtained cash. Drug offenders also used criminal proceeds to service mortgages. Drug offenders placed properties into the names of relatives and associates when purchasing property, presumably to conceal and disguise their beneficial ownership.
- Fraud offenders integrated proceeds of frauds committed against the Government to purchase properties. In one such matter, the conveyancing lawyer received a formal warning for non-compliance with the AML/CFT Act.
- Tax offenders integrated proceeds of their offending into property in New Zealand; property had been bought and sold – with multiple purchases on the same day.
- Individuals involved in international money laundering integrated the proceeds of global frauds into real estate that included land and residential property. To facilitate such purchases, funds were transferred from offshore bank accounts into trust accounts of lawyers in New Zealand.

Accountants

In New Zealand, there are 1976 active registered entities in the accountancy sector, varying in size and activities. The sector comprises a wide spectrum of practitioners, from large multinational accounting firms to individual bookkeepers.

The accountancy sector has several industry bodies which vary in size and in scope of the services they provide. It is not a requirement for accountants to be registered with an industry body, which makes it difficult to identify all potential reporting entities.

Like lawyers, accountants provide specialist services that can be misused by criminals to facilitate entry of illicit funds into the financial system. Moreover, they provide access to services and techniques to which money launderers would not normally have access, such as setting up trusts and companies. Accountants also provide an impression of respectability and legitimacy for a criminal using their services.

Other than conveyancing, accountants can provide the same 'captured activities'[35] that require AML/CFT obligations. These include managing client funds, accounts, securities, or other assets; trust and company formation services; acting as, or arranging for, someone to act as a nominee director / nominee shareholder / nominee general partner, or trustee; providing a registered or correspondence address; engaging in or giving instructions on behalf of a customer for specified services.

Accountants are not required to advise their supervisor (the DIA) if they engage in activity capturing them as a reporting entity under the Act (captured activity). Like law firms, it is likely that there are accountants that are reporting entities but not known to the DIA. These accountants would not have direct access to relevant guidance and risk updates.

SAR Review

Table 11: *SAR Review: Accountants.*

TIME PERIOD	No. SARs REPORTED	No. OF ENTITIES REPORTING SARs
01 January 2018 to 31 December 2023	84 SARs	64 accounting firms

Reporting is from a small number of accounting firms. The most common reason for reporting was suspected tax offending, followed by the accountant being suspicious about the source of funds, or a client's bank accounts receiving cash deposits. In addition, there were reports related to the refusal of a client to provide information or complete CDD requirements, and clients suspected to be victims of a scam or fraud. Other reasons included clients with known gang links or a criminal background, transactions that did not make economic sense, understating income in tax returns, and the use of shell companies without purpose.

The varied reasons for suspicion and the small proportion of accountants reporting SARs provides opportunities for closer engagement with this sector to deepen understanding of obligations under the AML/CFT Act.

Tax transfers present a low money laundering risk. Accounting practices (including accountants, bookkeepers, tax agents, and insolvency practitioners) carrying out relevant tax transfers under the Tax Administration Act 1994 on behalf of their customers are exempt from most – but not all – obligations under the Act.

During the period January 2018 to December 2023, there was one non-publicised formal warning for multiple and ongoing non-compliance of requirements and obligations under the Act. Specifically, compliance with CDD, PEP and independent audit obligations did not meet the minimum requirements of the Act.

[35] The captured activities of a DNFBP are on page 44 and also at s5 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 – see definition of 'designated non-financial business or profession'.

Threats

- Drug offenders used services provided by an accountant to set up shell companies[36] which were used to launder proceeds of their offending.
- Fraud offenders used services provided by an accountant to establish a company used for rental property investment. The company's accounts received cash deposits and fraudulently obtained Covid-19 payments. An accountant made 12 fraudulent applications on behalf of several companies to defraud the Covid-19 Wage Subsidy Scheme.

CASE STUDY

A business deposited $17,400,000 cash into their bank account over 10 years. It was depositing up to $80,000 cash per week, while not issuing any invoices, or having records of the purchaser or products sold. The business owners advised their accountant that the cash was from the sales of hydroponics and pet food, and the accountant dealt with the income on this basis. The business owners are alleged to be involved in significant cannabis-related crime.

CASE STUDY

A NZ-based TCSP (trained as a tax adviser) established NZ-based trusts and limited partnerships for an overseas-based business entrepreneur. These structures were used to disguise the beneficial ownership of the trusts and companies, over which the offshore individual and his spouse had effective control. These legal persons were used to launder proceeds of a large fraud undertaken in a foreign jurisdiction, and to place part of these funds in New Zealand. The entrepreneur was convicted on money laundering in a foreign jurisdiction. $10 million is subject to confiscation proceedings before the New Zealand Courts.

[36] Note: Risk Associated with Legal Persons and Legal Arrangements, and TCSP sectoral vulnerabilities, are described in Chapter 4. Refer to that chapter, noting accounting practices can provide TCSP services.

High Value Dealers (HVDs)

HVDs include businesses trading in motor vehicles, precious metals and stones, jewellery, boats and ships.

HVDs were previously subject to limited obligations under the Act; specifically, if they accepted cash payments of $10,000 or more (or a series of related cash payments that collectively were valued at $10,000 or more), they were required to conduct customer due diligence and report large cash transactions.

In May 2023, AML requirements changed to prohibit cash transactions above $10,000 for items such as jewellery; watches; gold, silver, or other precious metals; diamonds, sapphires, or other precious stones; motor vehicles, boats and ships. No businesses have been prosecuted as yet for conducting transactions involving amounts which exceed $10,000.

HVDs (that have these limited obligations under the Act) are now restricted to businesses that trade in paintings, prints, protected foreign objects, protected New Zealand objects, sculptures, photographs, carvings in any medium, or other artistic or cultural artefacts.

High-value cash transactions allow criminals to avoid interacting with the banking sector. Criminals will target businesses that are unlikely to refuse their custom or are unaware that they should refuse business for cash. High-value goods are often chosen for their resale value, and some items can be easily transported offshore or hidden for safekeeping.

> The change in legislation requires the banking sector to closely scrutinise HVD customers. The banking supervisor should pay attention to these customers. Police investigations which identify HVDs who received cash exceeding the permitted threshold should respond to that behaviour when appropriate.

SAR Review

Table 12: *SAR Review: HVDs.*

TIME PERIOD	No. SARs REPORTED	No. OF ENTITIES REPORTING SARs
01 January 2018 to 31 December 2023	66 SARs	17 HVDs

Prior to the law change, most SARs were reported by vehicle dealerships. A few were by precious metal dealers, and one was by a jeweller. The most common reason for reporting was either cash spending or structuring of payments for high-value items. Other reasons included suspicion that the customer was committing fraud; an unusual sale or purchase pattern – where a high-value vehicle was purchased and traded within a short period of time; reactive reporting in relation to Police interest; or an individual with identified gang links being interested in purchasing a vehicle. Other reasons included multiple credit cards used to purchase vehicles.

The New Zealand drug market is cash-based, which makes businesses that buy and sell high-value goods vulnerable to money launderers. High-value items such as vehicles, motorcycles, boats, jewellery and watches feature prominently in money laundering and proceeds of crime investigations. It is also recognised that New Zealand has a strong and unregulated private sales market, accounting for a portion of those seized items. High-value goods are attractive and desirable to criminals, as evidenced by the recent occurrence of ram-raids and aggravated robberies targeting jewellery stores.

Between January 2018 and December 2023, vehicles were the second most commonly restrained asset (cash was the most commonly restrained). Investigations identify that drug dealers laundered illicit proceeds through the purchase of vehicles with cash and registered these in the name of nominees. Vehicles registered in the names of nominees were used as trade vehicles. Drug offenders and associates also purchased jewellery, luxury branded clothing, artwork, and gold bars with cash.

Threats

- Tax offenders purchased high-value vehicles such as Maseratis with proceeds from tax offending.
- Individuals involved with international money laundering purchased high-value vehicles from dealerships by transferring funds from offshore bank accounts directly into the dealerships' bank accounts.

Mr K was arrested for drug-related offending and five charges of money laundering. Mr K had not had legitimate employment for seven years prior to his arrest and led a cash-intensive lifestyle. He used nominee bank accounts to facilitate the purchasing of large assets (homes, boats, vehicles), spending cash on renovations, and placing assets in the names of others.

Casino

New Zealand has three casino operators and six casino venue licences. Under S10 of the Gambling Act 2003, new casino venue licences are prohibited and existing casinos are unable to expand their gambling activities.

SkyCity Casino Management Ltd (SkyCity) holds licences to operate four casinos; however, only three operate. Its main casino is in Auckland and it has two smaller casinos – one in Hamilton and one in Queenstown.

Christchurch Casino is operated by Christchurch Casinos Ltd. Dunedin Casino is operated by Dunedin Casinos Ltd. Both have more limited international exposure in contrast to SkyCity.

Casinos have a reputation for being attractive for criminals to launder proceeds of crime. This occurs through an ability to convert illicit wealth, including cash, into winnings which provides an explanation of legitimacy. The services and products identified as being exploited by criminals to launder illicit income are through the use of casino-stored value instruments; the purchase of chips from 'clean' players at a higher price; the exchange of cash for casino chips, use of casino deposit accounts, and TITO (ticket in – ticket out) ticket purchases.

Although casinos continue to be vulnerable to money laundering, the risk posed by in-person laundering at casinos has been assessed to have decreased since the last NRA. This has been identified through investigations and intelligence.

In addition to physical casinos, online gambling is available in New Zealand. SkyCity and Christchurch Casino-branded online casinos are based in Malta, from where they service New Zealand based customers. These online casinos share ownership with their physical casino counterparts but are run separately because online gambling is not permitted in New Zealand (excluding Lotto and Entain, which was the TAB).

Other overseas-based online casinos servicing NZ-based customers do not have AML/CFT requirements in New Zealand but have various requirements in their home jurisdictions. Despite money laundering risk having decreased in physical casinos, money laundering risk through online gambling has increased, and has been identified in both drug and fraud investigations.

SAR Review

Table 13: *SAR Review: Casino.*

TIME PERIOD	No. SARs REPORTED	No. OF ENTITIES REPORTING SARs
01 January 2018 to 31 December 2023	640 SARs	3

32% of SARs were sampled. Analysis identified that the most common reason for reporting was that funds were suspected to be related to a fraud. The second most common reason was that funds were withdrawn at the casino without any associated gambling activity.

It is recognised that casinos provide the ability to withdraw larger volumes of funds than ATMs – this service can be used by criminals. Other reasons for reporting included refinement of smaller cash denominations into larger ones, which the casino considered an attempt to obscure the origins of cash; or suspicious source of funds based on the cash's appearance/state (e.g., smelling like cannabis); or the general behaviour of the customer.

Some SARs were reported in response to requests for information by Police; and some due to a failure to complete CDD or provide ID; as well as because of individuals with gang links, adverse media or who were suspected to be engaging in tax evasion.

AML/CFT concerns identified in the Australian casino sector have highlighted links between casinos and organised crime – this resulted in casinos reviewing their business models. In 2021, SkyCity decided to cease all junkets. SkyCity has also agreed to introduce mandatory carded play by mid-2025, which will reduce the ability for customers to transact anonymously in their casinos using cash. These are both positive developments that will further impact on the risk presented by this sector.

In February 2024, civil proceedings were filed against a casino for failing to meet its obligations relating to its risk assessment; establishing, implementing and maintaining an AML/CFT compliance programme; monitoring accounts and transactions; conducting enhanced customer due diligence; and terminating existing business relationships. These failures variously spanned from February 2018 to March 2023.

In September 2024 following a settlement agreement agreed by both parties and the casino admitting all five causes of action, they were ordered to pay a pecuniary penalty of $4.16 million.

Criminals were involved in selling cannabis, methamphetamine and GBL. A review of their bank account activity identified large incoming transfers from offshore online gambling sites. Analysis of their gambling activity identified over $90,000 had been sent offshore using the stored value cards "Paysafecard", which are able to be purchased from various dairies, petrol stations, convenience stores, and supermarkets across New Zealand using cash. The cards can be redeemed at online stores, including online payment platforms, to fund online gambling activities.

New Zealand intends to permit and regulate online casinos in New Zealand, resulting in an expansion of the online casino sector. For online gambling, ML/TF risks are different than physical casinos. Online gambling does not involve cash like physical casinos. The extent to which AML/CFT requirements would be applied to online casinos in New Zealand is not yet determined.

The banking sector, supervisors and the FIU should pay attention to online gambling bank accounts and payments to those accounts. These accounts present elevated risk from ML as identified through drug and fraud investigations.

Threats

- At physical casino locations, drug dealers can launder the proceeds of their offending through the purchase of casino chips or through other casino services.
- Drug dealers also transferred funds to online gambling websites to launder drug proceeds. Criminal proceeds are placed on stored value cards such as Paysafecards to be redeemed online and transferred offshore, funds were layered through online gaming activity, and any winnings received electronically into their New Zealand bank accounts thereby appearing legitimate.
- Fraud offenders laundered proceeds of fraudulently obtained Covid-19 payments through online gambling websites.

Sectors with recognised vulnerabilities, which have been misused by criminals

Non-Bank Deposit Takers

There are 14 licensed NBDTs including three building societies, four credit unions, and regulated finance companies supervised by the Reserve Bank. NBDTs are not banks; they however require the use of a bank to support their business and transact for their customers. Becoming a customer of an NBDT is often seen as a membership as opposed to being a customer and therefore, they often focus on a particular type of customer as their core customer base.

It is noted that with the set of 14 NBDTs supervised by the Reserve Bank, 2.3% of those customers are non-resident individuals.

Some NBDTs operate with higher transaction volumes than the smaller banks and therefore have similar types of vulnerabilities as the banks. SAR reporting from this sector identifies smaller volumes and values of reporting but generally the reporting is of a nature consistent with that of the banks.

Within the NBDT sector, Police identify the following types of behaviour:

- Credit Union members depositing cash proceeds of drug dealing into their accounts.
- A methamphetamine dealer received direct credit payments from his customers into his credit union account. Over a 6-month period in 2023, $25,000 was identified proceeds of methamphetamine dealing that was transferred to the dealer via direct credit.
- Another methamphetamine dealer obtained a credit union mortgage to purchase real estate then personally deposited cash into her credit union account to service the mortgage.

These include large cash deposits or withdrawals, possible state-funded benefit fraud, suspected mule account activities, frauds or scam related transactions, tax evasion and the use of a source of funds of an unknown origin.

Within the 727 NBDTs supervised by the DIA, many offer personal loans; debt consolidation; and other types of products that may attract cash deposit repayment. There is a gap in the full understanding of the DIA-supervised NBDTs. Improved understanding of the risk and the activities undertaken across the DIA-supervised NBDTs is required to accurately access the vulnerability of those reporting entities.

Currency exchange services

There are 35 active reporting entities within this sector, plus eight additional entities within the Currency Exchange Hotel Sector. A number of the reporting entities providing currency exchange services also provide MVTS services, including the banks.

In relation to currency exchange services, both MVTS and banking are considered the most vulnerable sectors given the range of services and products they offer.

Entities that operate exclusively as currency exchange providers typically present a lesser risk. However, currency exchange providers at airports may be used by international travellers arriving or departing New Zealand to sell or purchase cash prior to, or immediately after international travel.

Given that illicit drugs are imported into New Zealand, a criminal in a foreign jurisdiction will likely prefer currencies other than New Zealand Dollars.[37] This may result in the purchase of foreign currency for payment (which may involve the physical carriage over the border or payment through post).

In addition to fiat cash products available through the currency exchange sector, prepaid travel cards (which include pre-loaded non-bank cards) can be purchased and loaded with multiple currencies; the cards are easy to conceal when crossing a border. These types of products and services enabling the transnational movement of funds present a vulnerability to New Zealand.

Reporting from the currency exchange sector is limited; however, 30% of SAR reporting related to a refusal to provide information as to source of funds, or that the customer appeared nervous or suspicious when completing the transaction. The lack of quality reporting from this sector indicates that awareness could be improved to drive quality reporting. In addition, a more in-depth understanding as to the contemporary vulnerabilities of prepaid travel cards would add value to understanding of products available within this sector, and other sectors that provide similar products.

[37] See illicit drugs threat, page 20.

Non-casino gambling

Entain New Zealand entered a partnership agreement with TAB New Zealand in July 2023, making it a reporting entity under the Act. Entain operates from TAB outlets, on-course facilities, hotels and clubs across New Zealand. Play can occur via an online app, face-to-face placement of bets, and via self-service terminals. Like the casino sector, non-casino gambling has recognised risk associated with money laundering due to the cash intensity of some activities.

In 2023, Entain's UK-listed entity was required to pay £615M to defer prosecution over failures of their Turkish subsidiary for long-standing issues related to corruption; social responsibilities; and AML processes and procedures. In New Zealand, Entain has significantly reduced its international clients, increased training and other measures to mitigate risk – all of these are positive; however, inherent risk remains.

Non-bank credit cards

There are nine active reporting entities in this sector. They offer open loop and closed loop credit cards. Closed loop cards are typically used at a specific retailer and are not usually part of an association or global card network. Open loop cards are typically issued by or part of global card networks (such as American Express, Diners Club, Visa and Mastercard) and can be used at multiple retailers or to withdraw cash from ATMs. Some open loop cards are accepted at multiple retailers but only in New Zealand.

Non-bank credit cards present several ML/TF risks including cash loading, transfer of funds across borders. Open loop cards may be used in high-risk jurisdictions for TF and PF and for the purchase of high value goods. Products and services may be accessed worldwide with use of these cards.

It is noted that some non-bank credit cards also offer other services such as international money transfer (through online platforms) and foreign exchange for individuals or business. These often fall under the category of payment providers; or, if transactions involve virtual assets, they may be categorised as virtual asset service providers (crypto, digital wallets).[38] A SAR review from this sector identifies very modest levels of reporting, with nearly all reporting related to cash payments being made against the card.

Cash transport

Cash transport entities vary in size. The larger entities have capacity to transport significant volumes of cash and to move funds across national borders. This sector is closely connected to banks – providing transport service to ATM networks, bank branches, businesses (including HVDs) that receive high volumes of cash, cryptocurrency ATMs providers, DNFBPs, and individuals. The sector is also connected with cash-intensive business sectors, such as hospitality and retail.

Given cash is a recognised 'key threat driver', due to its importance with drug crime and given the possibility of cash moving through the HVD sector, there should be increased engagement with the cash transport sector.

There have been a small number of SARs from this sector, which relate to complex customer structures, cash being collected for payment of wages, and one instance where a bank customer had requested a $1M cash withdrawal. Improved engagement with this sector will deepen understanding of risk.

Non-bank safe deposit boxes

Seven entities operate in the non-bank safe deposit box sector. Banks also offer safe deposit services. Safe deposit box services provide a secure way for individuals and businesses to store valuable items such as jewellery, important documents, collectibles, and electronic storage devices. Access to the actual safe deposit box requires the customer to go to the safe to physically place or remove the property they have stored in the vault. Police investigations have identified these services have also been used to store cash, drugs and firearms. Some facilities offer the option to store precious metals (gold/silver/platinum bullion), as well as trading and exchange options. Vulnerabilities in this sector emerge where basic CDD and any EDD is not undertaken. Also, reporting entities don't know their customers, or the products being stored. Customer behaviour for AML/CFT purposes isn't monitored. Occasionally safety deposits have been used by overseas customers, which has an elevated risk. A small number of SARs have been received which relate to storage of cash, jewellery and bullion.

Non-bank non-deposit taking lenders

There are 727 active reporting entities in this sector. These types of lenders provide the likes of vehicle purchase finance. In recent years lending by non-bank institutions has grown more rapidly than lending by registered banks. Non-bank non deposit taking lenders provide finance, including personal loans and mortgages. Although offering mortgage finance, market share is very small (1-2%). Most customers within this sector are domestic with very limited numbers of international customers. Risk in this sector relates to the repayment of debt – the use of proceeds of crime to repay vehicle finance in particular is not uncommon.

[38] See Virtual Assets, pages 41-42.

Improved understanding of sector required - to deepen understanding of vulnerability

Payment providers

There are 93 active entities within this sector. Remote access is ubiquitous with services designed for ease of access – providers offer mobile and internet-based payment systems, digital wallets, electronic money and alternative banking platforms. The online nature of services means that providers may be based outside New Zealand, with differences between AML/CFT obligations in their home country and requirements in New Zealand.

Internet payment services (also known as payment platforms, payment gateways or virtual banks) are increasingly interconnected with new and other traditional payment services. Funds can be received, transferred, or paid using a variety of payment methods, including cash, money remittance, new payment methods, bank wire transfers and credit cards. Some internet payment system providers issue prepaid cards to their customers, giving them access to cash withdrawal through the worldwide ATM networks facilitating cross-border transactions. Pre-funded internet-based payment accounts are often used for online auction payments; a well-known example is the ability to have funds attached to a Trade Me account.

Mobile payment services allow non-bank and non-securities account holders to make payments with mobile phones. Pre-funded accounts are common across several types of payment providers. Recipients may or may not be required to register with the payment service providers to receive a funds transfer.

Alternative banking platforms are systems that provide the functionality of a bank but operate outside the traditional global banking space (or regulation). They can be highly connected internationally which, given the crime threat in New Zealand, means these products have high vulnerability.

Given the diversity of the payment provider sector, there is a wide variety of business models, functionalities, and structures. However, despite these differences they all fall within the definition of issuing or managing means of payment.

Some common risks associated with all types of payment providers include:

1. Speed of transactions
2. Difficulty in monitoring transaction activity
3. International movement of funds through non-bank channels
4. High value transactions
5. Potential for high levels of anonymity in setting up accounts and sending/receiving funds
6. Third party / arm's length transactions that disguise ownership
7. Regulatory arbitrage, where entities seek jurisdictions with lax or lower reporting obligations to take advantage of loopholes or otherwise circumvent regulations.

Note: This payment provider sector has been defined as distinct from Virtual Asset Service Providers. While there are similarities in the risk profile, virtual asset service provider transactions involve virtual assets which increases the level of risk further.[39]

The payment provider sector is technology-based, with new payment products and services (NPPS) developing rapidly and increasing in functionality and use globally. The technologies in this sector are still developing and or early in implementation. There are concerns regarding consistent regulation or regulatory avoidance/arbitrage, when online entities set up operations in jurisdictions with poor regulations but provide their services in other jurisdictions.

The payment provider sector presents several unknowns in terms of ML/TF/PF risk. As the sector continues to mature, the risks associated with it need to become more understood.

[39] See Virtual Assets, pages 41-42.

Stored value cards

There are five active reporting entities in the sector. Stored value cards are prepaid payment cards (either physical or electronic) that have a monetary value attached to them. Stored value cards differ from debit or credit cards in that the value is attached to the card
(rather than to an underlying account from which debits are made or a line of credit provided). Examples are gift cards, prepaid voucher cards, or transit cards.

As with non-bank credit cards, there are open and closed loop stored value cards. For example, Whitcoulls prepaid gift cards can only be used at Whitcoulls – these are closed loop cards. Open loop cards often have significantly more functionality than closed loop cards, including more options for reloading (via a payment terminal or electronically), an ability to be used overseas, the ability to withdraw cash at ATMs, and other functionalities of a payment instrument tied to a bank account.

Most stored value cards offered within the sector are only accepted at retailers in New Zealand. However other stored value cards are issued by or are part of a global card network that can be used at multiple retailers in NZ and in other countries. Stored value cards which can be used to access funds internationally are particularly vulnerable to ML/TF abuse. In addition to anonymity and the ease of adding funds, there are logistical benefits of transporting stored value cards loaded with high fund values rather than transporting large, bulky amounts of cash.

While the stored value card sector is small, it overlaps somewhat with payment providers and prepaid cards issued by Currency Exchange providers. There is also an exemption from AML/CFT obligations for stored value instruments, subject to various thresholds and conditions. There are new technologies involved and being developed with stored value cards. Open loop stored value cards, particularly those with global reach and ease of access, are vulnerable to several high-risk ML/TF/PF activities.

Sectors assessed as being least vulnerable

The following sectors are less vulnerable compared to banks, MVTS, VASP and the described sectors that are being misused by criminals. However, these sectors operate within the banking system, and the primary risk identified is that some of these sectors provide services to customers located in foreign jurisdictions.

Although there is no identified direct convergence with high-risk crime threat, these sectors should recognise that transnational money laundering involving New Zealand continues to occur and clients, customers, and transactions that involve foreign jurisdictions should be managed with care. In addition, products and services provided by these sectors are also the subject of scams and frauds which are high-risk threats (note though, it has not been identified that the proceeds of these types of offences are laundered through these sectors).

Derivative issuers

There are 18 licensed derivative issuers (three are registered banks and two are money remittance and foreign exchange businesses).

This is seven fewer than existed when the 2019 NRA was undertaken. 2023 data identified a gross value within this sector of $21.81B across six million transactions.

This therefore is a highly complex sector with participants engaged in speculative trading. 25% of customers involved in this sector are based offshore (mostly Australia) and offshore customers do not require New Zealand bank accounts.

A feature of this sector is the use of offshore intermediaries; limited face-to-face onboarding; acceptance of credit cards to facilitate payments; and customers based in high-risk countries – or customers (who are legal persons) controlled by or owned by people in high-risk countries.

Of SARs sampled from this sector, most (75%) related to suspected frauds or scams.

One company was ordered to pay a penalty ($770,000), and another was formally warned relating to AML/CFT Act breaches.

Discretionary Investment Management Service (DIMS) Providers

There are 50 licensed DIMS providers (three are registered banks). This activity is often a type undertaken by Financial Advice Providers or licensed Managed Investment Scheme providers.

The primary service provided by a DIMS provider is making decisions for a customer in line with an agreed investment strategy. This requires in-depth knowledge of a customer's financial situation, and with this requirement DIMS providers[40] are less attractive to criminals. In 2021, approximately 2% of customers who used this sector were legal persons. Although this sector has some vulnerabilities, these do not compare to the vulnerabilities of the high-risk sectors.

One licensee has been issued a warning for not compliance with AML/CFT regulations.

Financial Advice Providers (FAPs)

There are 1492 entities or individuals with a FAP licence; less than 50% have AML/CFT reporting obligations.

[40] DIMS providers may have cryptocurrency in their portfolio, and therefore may manage such assets on behalf of their clients.

FAPs are connected to the mortgage brokering and insurance sectors – the services that they connect a customer to are provided by another reporting entity (e.g., a bank).

25% of SARs reviewed from this sector related to suspected frauds or scams. Others related to issues that arose with customer due diligence obligations or the payment type being unusual for the product purchased. It is noted that there are customers within this sector who are resident in jurisdictions with low levels of AML/CFT compliance – one such jurisdiction is currently blacklisted.[41] These customers should be reviewed during the supervision of this sector.[42]

22 warnings have been issued across this sector for AML/CFT regulation breaches.

Providers of client money or property services (previously Brokers and Custodians)

There are 66 entities providing clients with money or property services. This is a service where a provider holds, transfers or makes payments with client money or property on behalf of a customer. Brokers and custodians are usually connected to other licensed services such as a FAP, a bank, or the NZX.

Vulnerabilities within this sector include the reliance on third parties to undertake CDD – with more than 80% of onboarding being non-face-to-face and with some reporting entities offering services almost exclusively to non-resident customers.

Eight formal warnings have been issued for AML/CFT legislative breaches.

Equity crowd funding

There are five crowdfunding entities licensed; one is licensed for peer-to-peer activity. Crowdfunders offer services as an intermediary between investors and companies (start-ups, craft breweries etc.). 97% of investors are individuals; the balance consists of trusts. 3% of customers are based offshore. Companies can raise up to $2M in a 12-month period through a licensed platform, and cash is not used. The sector is small and there has been no evidence of this sector being abused for ML/TF.

One licensee was issued a warning for AML/CFT regulator breaches.

Issuers of securities

There are 109 reporting entities identified as issuers of securities. This sector is considered to have low vulnerability when contrasted with the high-risk sectors.

Licensed Supervisors

There are five Licensed Supervisors. This sector is connected to the real estate sector via the Public Trust. Licensed Supervisors provide the supervision of one or a combination of debt securities; managed investment schemes (including KiwiSaver); and retirement villages. They are not involved in the day-to-day management of these activities, more that they supervise the activities of their customers. This is a low-risk sector.

Managed Investment Schemes (MIS)

There are 65 licensed MIS managers. This sector is split between retail and Wholesale Fund Managers. Retail funds include standard KiwiSaver funds,[43] Unit Trusts, Superannuation Schemes and workplace savings schemes, forestry partnerships, and property investment schemes. Wholesale fund managers are not required to hold a MIS license.

Some of these schemes are investing in crypto-assets. This sector has a small number of reporting entities with overseas ownership,[44] or overseas customers (some of whom are from a blacklisted country).

MIS managers should continue to enquire carefully into the source of wealth to prevent illicit wealth entering this sector from offshore fund owners and customers. These offshore owners and customers present higher risk.

Peer-to-Peer Lending

There are seven Peer-to-Peer lending services licensed by the FMA; one is also a crowd-funder. 2023 data shows $2.15B in gross transaction value. This sector simply connects lenders to borrowers via an online platform.

[41] A blacklisted country is a country recognised as having an absence of AML/CFT or PF controls. Three countries are currently blacklisted - Iran, North Korea (the DPRK) and Myanmar. See page 29.

[42] See high-risk countries, page 29.

[43] One provider has a cryptocurrency KiwiSaver fund.

[44] See high-risk countries, page 29.

There have been no instances involving ML/TF associated with this sector. This sector is considered a low vulnerability given most transactions are low-value.

One Licensee has been issued a warning for AML/CFT breaches.

Life insurance

There are four licensed providers of life insurance[45] that provide redeemable life insurance policies such as cash surrender policies or policies with investment features. Between 1 July 2023-30 June 2023, there were 637,008 transactions through this sector with a combined value of $166M.

There has been very limited reporting and no identified instances of ML/TF from across this sector. In 2023 it was identified that 3.8% of customers from this sector are non-resident policy holders.[46]

Debt collection

A debt collection agency provides a service of collecting payments from debtors on behalf of their client. This is primarily because the client is unable to communicate with the debtor, the debtor refuses to pay the client, or the client may want to outsource some of their debt collection for efficiency.

Debt collection agencies are exempt from conducting CDD. In addition, they are reliant on the information provided by their client so it can be difficult for debt collection agencies to assess risk (in relation to the debtor) independently. This sector is exempt from essentially all reporting obligations except for SARs. The risk analysis performed for this exemption identified that the exemption is not of concern. There were five SARs reported during the period January 2018 to December 2023. All were in relation to unexplained large deposit and/or unexplained source of wealth.

This sector has not been implicated in any ML investigations but we must be aware of risk related to large cash payments to satisfy debt payment.

Factoring

There are 13 active reporting entities in this sector. A 'factor' is an intermediary agent who provides finance to companies by purchasing invoices for accounts receivable. For example, a company provides goods, but their invoice has not been paid. The factor will purchase this invoice at a discount to provide cashflow to the business and receive payment from the customer in accordance with the terms of payment. There is a degree of connection to other business sectors due to factoring being business-to-business.

This sector caters for both domestic and international markets. The process of international factoring has the same principles as domestic factoring; the difference is the buyer and seller are in different countries.

Principal ML risks within the factoring sector are:

- payments against invoices where there is no actual movement of goods or services provided. where
- the value of goods is overstated to facilitate the laundering of funds.

Payroll remittance

There are five active entities in this sector, which involves payroll transactions into employee bank accounts. Payroll remittance businesses provide services to other businesses for the purposes of payroll administration; these include meeting Inland Revenue's Pay As You Earn (PAYE) tax obligations.

A likely ML typology would be use of ghost (fake) employees to launder money. This occurs where a fictitious employee is added to the company payroll and receives a salary. Identifying a ghost employee can be challenging for a payroll remittance company. Some businesses in this sector are local franchises of larger overseas companies servicing the New Zealand market. There may be employees of New Zealand companies who are located overseas and receive their pay through these services.

Financial leasing

There are 53 active reporting entities in this sector.

Financial leasing involves financing the purchase of tangible assets (note the Act does not apply in relation to financial leasing of consumer products).

The leasing company is the legal owner of the goods, but ownership is effectively conveyed to the lessee, who incurs all benefits, costs, and risks associated with asset ownership.

Financial leases may also be referred to as 'Rent/Lease to Own'. The size and type of entities in the sector varies

[45] These are the non-exempt life insurers.
[46] See high-risk countries page 29.

considerably, from local subsidiaries of large global companies offering leasing for major IT infrastructure projects, to smaller domestic companies offering commercial equipment and vehicle financing.

The risk within this sector primarily relates to the repayment of the finance obtained. This is demonstrated through a review of 50 SARs reported during the period January 2018 to December 2023, which identified suspicion related to unknown source of wealth, structured payments, possible tax evasion, possible gang finance and cash payments.

Although the review of this sector for the NRA has not identified elevated risk, there are indicators that criminals may repay finance obtained through this sector with illicit wealth.

Tax pooling

There are three active reporting entities in the sector, down from five in 2019. Tax pooling is a government-approved system that allows approved intermediaries to operate tax pooling accounts with Inland Revenue. The purpose of tax pooling is to allow taxpaying entities to mitigate the financial risks associated with errors in their provisional tax estimations.

By aggregating tax paying entities into a tax pool, those who have overestimated their tax obligations (and thus overpaid) can take money out of the pool and those who have underestimated (underpaid) can put money into the pool. Those who would otherwise be assessed as underpaying can avoid the Use of Money Interest rate applied to underpayments of tax. Tax poolers have a partial exemption from most AML/CFT obligations under the Act. The risk of tax pooling products and services for money laundering is limited by the customer type, the regulation by Inland Revenue, and the close relationship between the payments/refunds and actual tax debt.

Two SARs have emerged from the sector – both related to suspicious tax refunds.

RISK ASSOCIATED WITH LEGAL PERSONS AND LEGAL ARRANGEMENTS

Risk associated with legal persons (LPs) and legal arrangements (LAs)[47]

Legal structures are involved in an extensive range of commercial activities across New Zealand. They play an essential role in the operation of our economy.

Legal structures are easy to form, and can quickly access financial services including banking facilities and other types of financial products. The key advantages of conducting business through a legal person are liability protection and tax advantages. Both encourage and enable economic activities for the betterment of our economy.

LEGAL STRUCTURE

'Legal structure' is used as a general umbrella term to refer to any legal persons, trusts or other legal arrangements through which a wide variety of commercial activities can be conducted, and assets can be held.

LEGAL PERSON

Corporate bodies, foundations, limited partnerships, associations, cooperatives, or similar entities – other than natural persons – that have legal personality and can establish a permanent customer relationship with a financial institution or otherwise own property.

LEGAL ENTITY

Used interchangeably with 'legal person'. A 'legal entity' also has a separate legal personality.

LEGAL ARRANGEMENT

Trusts, express trusts, or similar legal relationships, charitable entities, unincorporated societies, or other partnerships which provide separation of legal ownership from beneficial ownership. The settlor (a natural or legal person) places property (including real, tangible and intangible) under the control of a trustee for the benefit of a beneficiary (or beneficiaries) or for a specific purpose. The trustee holds legal title and owns a fiduciary duty to the beneficiary who is the beneficial owner of the trust property.

The 2019 NRA identified that LPs and LAs were both highly vulnerable to being misused to launder money or facilitate the financing of terrorism. This is because LPs and LAs were recognised as being attractive vehicles for criminals to place, layer, move and reintegrate proceeds of crime to obfuscate the origin and ownership of the proceeds. These types of structures offered additional protections because nominees could be engaged to control the structures at 'arm's length' to conceal the criminal's interest in property held or controlled by the LP. Similarly, trusts (LAs) were recognised to afford protections in the absence of a trust registry (which records beneficiaries), therefore at risk of being exploited by criminals settling illicit wealth into a trust. Also, due to the lack of trust transparency, it could be challenging for authorities to quickly identify beneficial interest in trust assets.

New Zealand's Mutual Evaluation Report 2020-21 identified that there were substantial gaps in ensuring the availability of adequate, accurate and timely beneficial ownership information for legal persons and legal arrangements. Access and availability of such information would enable authorities to establish beneficial interest and ownership of trust-held assets, for the purpose of identifying and confiscating concealed proceeds of crime.

[47] This chapter must be reviewed using the context provided in Chapters 2 and 5.

As identified in the 2019 NRA assessment, neither LPs and LAs have been identified as enabling the financing of terrorism[48] or to finance proliferation[49] since that prior assessment. Given the complexity and the interconnectivity of the global financial system, it is accepted that there is a possibility that New Zealand companies have or will at some future time be misused for such activities.

In particular, New Zealand LPs could be attractive for both TF and PF due to the ease in which they can be formed; the perception of a veneer of legitimacy given New Zealand's reputation as a country with political and economic stability; and finally the perceived 'gaps' with beneficial ownership transparency as described in the 2021 Mutual Evaluation report.

With regards to money laundering, this NRA identifies that contemporary leading threats to the New Zealand AML/CFT system include fraud and transnational ML. LPs and LAs have and are being misused by both domestic and foreign criminals in laundering activities associated with these types of crime. Also, there have been instances where LPs and LAs have also been used to launder the proceeds of drug crime. This demonstrates that legal persons and legal arrangements formed in New Zealand remain vulnerable to money laundering activities, by both domestic and foreign criminals.

Types of legal person

The majority of legal persons in New Zealand are limited liabilities companies (LLCs). For this reason, LLCs are most vulnerable.

- Unlimited companies form a much smaller number and without the liability protections of LLCs, are potentially less attractive to criminal abuse.
- Co-operative companies hold their own shareholder registry, with shareholder information not publicly accessible but the small number of co-operative companies largely mitigates risk. Given the threat of fraud and transnational money laundering, these companies have a higher level of vulnerability than unlimited companies.
- Overseas registered companies can have access to New Zealand's financial system; however, the number is small, and the registration requirements of these companies are stricter than that of a New Zealand LLC.
- Public records on limited partnerships record only the general partner; however, the Companies Office has information on all partners, which is available for law enforcement purposes. The Companies Office monitors the Companies Register and removes companies of concern or risk.

Table 14: *SAR Review: New Zealand Registered Legal Persons 2020 – 2024 (YTD at 31 August 2024).*

Registration

COMPANIES	2020	2021	2022	2023	2024*
LTD	58,372	64,759	54,331	55,870	38,227
COOP	3	5	8	2	2
UNLTD	24	27	9	11	5
ASIC	166	203	216	210	144
NON ASIC	55	57	54	57	40
GRAND TOTAL	58,620	65,051	54,618	56,150	38,418

OTHER INCORPORATED ENTITES	2020	2021	2022	2023	2024*
Incorporated Societies	663	771	703	891	550
NZ Limited Partnership	372	535	384	376	232
Overseas Limited					
Partnership	1	1	1		2
GRAND TOTAL	1,036	1,247	1,088	1,267	784

[48] Refer to Chapter 5: Terrorism Financing for added context.

[49] Refer to Chapter 6: Proliferation Financing for added context.

Table 14 (continued): *SAR Review: New Zealand Registered Legal Persons 2020 – 2024 (YTD at 31 August 2024).*

Removals

COMPANIES	2020	2021	2022	2023	2024*
LTD	30,457	38,056	41,098	41,455	31,446
COOP	4	7	5	6	1
UNLTD	29	26	17	15	20
ASIC	98	178	152	115	70
NON ASIC	53	72	56	40	26
GRAND TOTAL					

OTHER INCORPORATED ENTITES	2020	2021	2022	2023	2024*
Incorporated Societies	509	1,201	1,115	1,095	511
NZ Limited Partnership	172	200	185	183	157
Overseas Limited					
Partnership	1	1	-	-	-
GRAND TOTAL	682	1,402	1,300	1,278	668

What could make a LP attractive to a criminal?

The LP creates a legal personality separate from the criminal. The LP can allow ownership but also concealment of ultimate beneficial ownership. Importantly, the LP can provide access to the banking system. Higher value criminals, and transnational criminals may split company formation, the location of intermediaries, bank accounts, and the location of LP assets across more than one jurisdiction. This can make it difficult for authorities to fully observe and reconstruct legal structure and these structures' asset ownership.

According to The World Bank's 2020 "Doing Business" report, New Zealand was voted 1st out of 190 economies in the world for ease of doing business. It was also ranked 1st for starting a business.

Appointment of nominee directors

Some TCSPs in New Zealand offer nominee director services to foreign clients, given the requirement for all New Zealand LPs to have a resident New Zealand director. These services offer the establishment of a company, the opening of bank accounts, and fulfilling the resident director requirements.

The key benefits are summarised as:

- **being a point of contact** for authorities and a domestic bank (if an account is established).
- providing a service of **ensuring compliance** with domestic regulatory requirements.
- **offering personal privacy and anonymity**.
- the nominee director will not hold shares in the company, therefore has **no recognised beneficial ownership.**[50]
- through formal agreement with the beneficial owners, the nominee director undertakes a pure nominee role therefore has **no authority over the company's operations or administration**.

This NRA recognises that transnational money laundering presents threat to New Zealand, and in this context, offering nominee services has risk of personal liability for appointed

[50] in the context of legal persons, beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owners of a legal person.

nominee directors. Understanding why a client requires anonymity is central to an understanding of risk. A nominee director needs to ensure that the foreign client they represent is not a nominee for an undisclosed third party and that the services they provide relates to a bona fide commercial purpose.

The increasing prevalence of global scams and frauds and the recognised threat of transnational money laundering elevate the personal liability of nominee directors and shareholders. The global law enforcement community is working more effectively in response to transnational frauds, scams and transnational money laundering.

As yet, no New Zealand nominee directors have been prosecuted for money laundering.

Money laundering investigations and prosecutions are accelerating around the world. Through the learnings from these prosecutions, lawmakers are developing and designing new money laundering offences in support of the global AML/CFT effort. Strict or absolute liability offences are emerging in some countries; these criminalise the behaviour of persons (natural and legal) who deal with proceeds of crime, in circumstances where it was reasonable to suspect that the property was proceeds of crime.

Reasonable grounds to suspect is deemed to have been established when for example a person undertakes a nominee role and deals with proceeds of crime and then fails to prove (rebut the onus) that they could not have suspected the property was the proceeds of crime. This would require the nominee to undertake a much deeper level of due diligence associated with the services they offer, given the onus will be on them to prove that they could not have suspected that they were dealing with illicit wealth.

Appointment of nominee shareholders

The purpose of holding a shareholding in the name of a nominee (on behalf of a beneficial owner) has commercial justification in certain circumstances. From a criminal perspective, using a nominee shareholder provides a mechanism to disguise and conceal the beneficial ownership of property on behalf of a criminal. This has logical advantage in that concealment also affords security – making illicit wealth more difficult to detect, track, trace and connect to the ownership of a criminal or connect to their crime behaviours.

Disguising beneficial ownership of property using nominee services can therefore enable laundering to successfully occur.

CASE STUDY

A New Zealand criminal established a legal arrangement – an investment trust (IT) in New Zealand. Foreign-derived proceeds of crime were settled into the trust. The IT instructed a nominee (natural person) to open a capital markets account in the name of the nominee and to conduct transactions on instruction and on behalf of the IT. A 'deed of trust' outlined the role of the nominee, and stipulated that all investments and associated returns were exclusively and beneficially owned by the IT. The beneficial owner behind the IT was convicted for money laundering.

Purchasing or conducting activities through a shell company

A shell company does not undertake any activity or own any assets. A shell company will likely have a registered address of a law firm, accountancy practice or a TCSP. Shell companies are not in themselves illegal but can be established for illegal purpose. Understanding the ultimate beneficial ownership of any company, and its purpose and intentions, is important before establishing a financial relationship with it.

CASE STUDY

Domestic shell companies

Sept 2023 – A Hong Kong financial regulator summoned a 'struck off' New Zealand shell company to appear in a Hong Kong court, in relation to an HKD $170M ($36M NZD) fraud. The NZ company was deregistered in New Zealand after it was identified by Chinese Taipei authorities to be involved in a foreign-based Ponzi scheme. The primary offender was sentenced to 11 years imprisonment in Chinese Taipei.

CASE STUDY

Use of foreign shell companies

A Head Hunter gang member was subject to proceedings before the High Court. To fund the defence of the proceedings, six cash deposits were paid into the account of Tucker and Co, which was a law firm that instructed a barrister to represent the Head Hunter. In relation to the same proceeding – between June 2020 and August 2021, funds were deposited into the bank account of Dominion Law Trustee Limited; these funds involved $44,000 cash, $72,311 in international remittances and $58,050 in domestic transfers. Dominion Law were also instructing solicitors representing the Head Hunter. The international remittances were reconstructed and had origin in cash deposits into New Zealand bank accounts which were then remitted to Hong Kong. The funds were then transferred from the Hong Kong account back to the Dominion Law account in New Zealand. The transfer to Dominion Law via Hong Kong was an attempt to obscure and disguise the origin of the funds. In a judgment of the High Court in relation to these monies, the High Court stated:

"The process of depositing cash funds in New Zealand, moving these funds between multiple accounts, remitting them offshore, to what appears to be a shall company, and then remitting them back to New Zealand is, in my view – evidence of money laundering."

Purchasing a New Zealand registered shelf-company

Like a shell company, a shelf company is one set up by a TCSP and is available for sale 'off the shelf'.

The company will not hold any liabilities or assets. It is established and ready to undertake business. Although company formation in New Zealand is efficient, the advantage of a shelf company is that it could have been established some years ago, and its age may be perceived to provide a degree of credibility and corporate history.

Who formed the company, where it was formed, when it was formed and why it was purchased are all important details when dealing with or establishing a relationship with an acquired shelf company.

Mossack Fonsecca, a Panamanian law firm, sold shelf companies. A criminal, resident in New Zealand, who had previously committed frauds in a foreign jurisdiction purchased companies from Mossack Fonsecca. The companies were established in Hong Kong and held in the name of a nominee director resident in China. The Hong Kong company channelled funds (suspected to be the proceeds of foreign crime) in the form of loans via a New Zealand law firm to a New Zealand company to undertake property development. The criminal was convicted of money laundering.

Using a cash-intensive business to co-mingle cash

Cash-intensive businesses can be used to receipt illicit cash that is co-mingled with cash derived from limited business activity. When introduced via the business, the illicit cash adopts the guise of legitimate earnings. For example, a nail or beauty salon, or a barbershop, may be used to introduce illicit cash, co-mingled with legitimate business takings to launder the cash.

A Mongrel Mob member was recorded as an employee of a company. He received salary but did not undertake any employment. Profits from selling methamphetamine were deposited into the company accounts to cover the wage drawing. The salary income was then used in support of finance applications with a financial institution to purchase property. The company was used to launder proceeds of crime and provide legitimacy to drug income received by the Mongrel Mob member.

Trusts

A significant value of property across New Zealand is held in trusts.

New Zealand does not have a central registry of trusts. This limits understanding of the abuse of New Zealand formed trusts. In 2021, the Financial Action Task Force (FATF) identified that New Zealand needed to proactively improve the transparency of legal arrangements, including of express trusts, and recommended New Zealand implement

a beneficial ownership[51] register for trusts. This proposal is currently subject to policy development.

Trusts can conceal the beneficial ownership of property of a criminal, be used to mask their activities, and disguise the ownership of property.

A senior member of a prominent New Zealand gang had a controlling influence over a charitable trust, other trusts and companies. These were formed to receipt cash from criminal enterprise and hold wealth derived from criminal activities undertaken by the gang. This included the gang headquarters in Auckland valued at more than $4M, held in the name of an investment holding company. The gang member also controlled a company which was formed by a solicitor – the sole director and shareholder of the company and person who held the shares on a bare trust on behalf of the gang member. The finance company provided loans to other gang members (repaid in cash). The company operated in breach of both the Financial Service Providers Regulations Act 2008 and the AML/CFT Act.

The disadvantage of a trust is the requirement for legal documents to be created, which are then provided to financial institutions or are retained by law firms. Trust deeds are useful in evidencing the origin of trust property and the controlling minds of the trust.

> **The perception that a 'trust' has an ability to preserve property from confiscation is a fallacy. New Zealand proceeds of crime law regularly confiscates trust-held assets when it can be evidenced that a criminal has beneficial interest and effective control over property, irrespective of the property being held in a legal structure.**

Previous changes to trust law include establishing the Foreign Trust Register, which was done by IR in 2016 following the Government's Inquiry into Foreign Trust Disclosure Rules. The inquiry found that the existing foreign trust disclosure rules were not fit-for-purpose in the context of preserving New Zealand's reputation as a country that cooperates with other jurisdictions to counter money laundering and aggressive tax practices.

In 2022, Inland Revenue (IR) estimated there were 300,000 – 500,000 express trusts in New Zealand. In 2023, Inland Revenue determined in its Trust disclosures information from the 2022 tax year release that:

- Total assets reported from 150,000 trusts totaled$454B.
- The investments made by trusts in shares had more than doubled over the last 10 years ($30B in 2013 to $64B in 2022).

A foreign trust is a trust arrangement with assets settled onto the trust by a non-resident settlor. Commonly these assets are held offshore. In 2016 there were 11,671 foreign trusts with resident trustees. This reduced to 3400 in 2019, and currently totals 2254. The declining number is because of the comprehensive foreign trust regime that was introduced in 2017 and the ongoing compliance focus in this area.

The foreign trust registry collects information on persons connected to the trust, settlements onto the trust and distributions from the trust at registration and annually. The registry is open to Police and the Department of Internal Affairs.

A law firm established four trusts for four criminals who were involved in the importation and sale of methamphetamine, and money laundering. The trusts established bank accounts which received cash via ATM deposits. One trust purchased a property in the names of a lawyer and nominee trustees; other trusts purchased vehicles. Cash funds receipted through the law firm's trust account for the benefit of the trusts exceeded $1.2M.

[51] In the context of legal arrangements, beneficial owners include: the settlor(s); the trustee(s); the protector(s) (if any); each beneficiary, or where applicable, the class of beneficiaries and objects of a power; and any other natural person(s) exercising ultimate effective control over the arrangement. In the case of a legal arrangement similar to an express trust, 'beneficial owner' refers to the natural person(s) holding an equivalent position to those referred previously. When the trustee in any other party of a legal arrangement is a legal person, that beneficial owner of the legal person should be identified.

Table 15: *Top ten jurisdictions from which persons are connected to foreign trusts.*

	CONNECTED PERSONS' JURISDICTION	COUNT
1	Argentina	423[52]
2	Australia	296
3	Mexico	247[53]
4	United Kingdom	150
5	Italy	101
6	Venezuela	96[54]
7	Switzerland	92
8	Uruguay	84
9	Monaco	80[55]
10	South Africa	79[56]
	United States	79

Other legal arrangements

Low-risk legal arrangements include commercial trusts (unit trusts) such as Māori land trusts, deceased person estates, and employer or superannuation trusts that are similar to commercial trusts and generally limited to salary or employer contributions.

Vulnerabilities – Trust and Company Service Providers (TCSPs)

Key gatekeepers to prevent the misuse of New Zealand established legal persons and legal arrangement are trust and company service providers.

There are 246 reporting entities within this sector. This contains company formation agents; administrators and managers of trusts, companies, and limited partnerships; as well as providers of virtual office services. Some of the providers source customers through overseas based TCSPs, who act as their agents for New Zealand TCSPs.

The locations of these overseas TCSPs vary; however, Switzerland and Australia are common locations. Cross-jurisdictional structures can be more complex, offering advantages to the sophisticated transnational criminal.

Given the recognised transnational money laundering threat,[57] providing services offshore (persons in foreign jurisdictions) and acting as a nominee director, shareholder or general partner presents higher risk.

TCSPs can provide services associated with the ongoing management of trusts, companies, limited partnerships and other legal arrangements. In addition, they can provide services of being a registered address for a company, partnership, or arrangement. Providing a registered office for correspondence is commonly known as providing a 'virtual office service.' This service creates a layer of physical distance between the activities undertaken by the legal structure and provides an appearance of legitimacy as the office address is often in a premier commercial building.[58]

SAR Review (TCSPs)

Eight TCSPs have submitted SARs.[59] A review of the 82 SARs submitted identified that 40% of the reporting related to:

- a refusal of the client to provide verified ID, or details of the beneficial owner of the funds; or
- the client having gang or criminal links.

Other reasons included suspicion regarding the purpose of an offshore client wanting to form a New Zealand company; concern regarding the client being involved in a scam or fraud; the client behaving cagey and/or evasively when asked questions as part of CDD requirements; producing forged proof of address or identification documents; identity fraud identified during onboarding; and questionable source of wealth.

A review of requests from foreign FIU counterparts seeking information from New Zealand in support of foreign intelligence or analysis identifies that approximately 80% of such requests relate to legal persons or arrangements established in New Zealand. Of that, 20% relate specifically to New Zealand formed trusts.

This reflects that New Zealand legal persons and arrangements are featuring in offshore suspicious financial activities that are being reported to foreign FIUs.

[52] Argentina has a corruption perception index (CPI) of 37 (0=highly corrupt. 100 = no corruption).
[53] Mexico, recognised as a source country for methamphetamine (see chapter 2), has a CPI score of 38.
[54] Venezuela is a country recognised as having a very high risk of corruption, CPI score 13. Also ICRG Grey listed – see page 29.
[55] Monaco is currently subject to ICRG Grey listing due to strategic AML/CFT deficiencies. Also ICRG Grey listed – see page 29.
[56] South Africa is currently subject to ICRG Grey listing due to strategic AML/CFT deficiencies. CSI score of 41.
[57] Refer to Chapter 2, page 19.
[58] Refer to Chapter 3, page 44.
[59] Other reports were submitted by law firms and accounting practices (who offer TCSPs services). See Chapter 3, pages 44-46 and 48-49..

TCSP thematic

The DIA undertook a TCSP thematic that looked at several TCSPs and law/accounting firms providing formation/nominee services.

Most of the TCSPs sampled were not relying on an overseas intermediary to complete CDD processes, instead opting to review the CDD documents themselves. This is recognised as a good practice. Additionally, several TCSPs indicated that they considered the overseas intermediary to be their customer, rather than the legal person/arrangement that they were acting as a formation agent or nominee for – regulations have clarified that the customer is the person for whom they provide nominee services, as opposed to the intermediatory.

Unlike law firms and accountancy practices that provide TCSP services, there are no barriers to entry as a TCSP, no registration requirements and no professional standards to comply with. There could be TCSPs operating without the knowledge of the TCSP supervisor (DIA), and given the threat of transnational money laundering, this is a concern.

Summary

LPs and LAs both present risk for ML/TF and PF.

This NRA preserves the previous risk assessment of them being high-risk, although recognises various measures have been implemented that are lowering risk.

It is recognised that risk remains high[60] because of:

- The transnational money laundering threat described in this NRA.
- Challenges globally with fraud.
- The consequences associated with the misuse of LPs and LAs in relation to TF and PF together with the various examples which cite misuse of LPs and LAs domestically.

Finally, the global connectivity of legal persons and arrangements can have consequences and enable crime in other countries.

Strengthening transparency of beneficial ownership of New Zealand LPs and LAs is important to reduce risk domestically and in other parts of the world.

Supervisory insights:

- A New Zealand based TCSP provided formation and nominee services via an intermediary based in Switzerland. The TCSP received instructions from the director of the overseas intermediary and was fully reliant on that intermediary for completion of CDD. This led to the reporting entity having inadequate CDD records and unknowingly providing services to high-risk customers. Source of wealth/funds information was not obtained or held by the TCSP.
- A New Zealand based accounting practice provided formation and nominee services via an intermediary based in the UK. This entity was operated by a professional accountant. The accounting practice relied on the intermediary based in the UK for completion of CDD. The steps taken to ensure CDD was conducted satisfactorily were insufficient. Also, on inspection, the practice was found to be providing services to high-risk customers and insufficient records were obtained by the intermediary.

[60] Also see Chapters 2, 5 and 6.

TERRORISM FINANCING

Terrorism financing risk assessment[61]

Financing of terrorism is low threat with regards to domestic terrorism. Elevated threat occurs in the international environment (international threat); however, overall TF threat is considered low.

It must be recognised that deaths from global terrorism in 2023 were at the highest level since 2017 and that New Zealand has financial connectivity to countries with high terror crime occurrence. Far-right extremism within the international environment has emerged as a global problem threat. The consequences of this type of terrorism as experienced by New Zealand and in foreign countries is devastating. Although risk is considered low, complacency is also a risk, and New Zealand must remain vigilant to prevent individuals or terror organisations raising or moving funds through New Zealand's financial system.

Terrorism impacts the safety and security of many countries around the world. Preventing terrorism is a global responsibility.

In New Zealand the risk of a terrorist event occurring is low. Low means 'a realistic possibility'. To help define 'low', it is useful to understand that medium means 'feasible and could occur' and very low means 'unlikely'. A low threat level of 'realistic possibility' requires the AML/CFT system in New Zealand to be highly vigilant to suspicious financial behaviours to ensure every opportunity to detect and prevent terror-related crime is identified and responded to. This requires the continuous collection and combining of counter-terrorism related intelligence (including that collected by foreign intelligence agencies) and financial intelligence, which means the detection of terrorism financing in New Zealand is a shared responsibility between Police, the security intelligence agencies and all reporting entities across New Zealand's AML/CFT community.

As a sweeping generalization, classic terrorism financing has not been confirmed to be occurring in New Zealand, although a number of suspicious activities and individuals have been identified. This does not necessarily indicate a change in threat, however the security situation could change rapidly with minimal warning. NZ is fortunate that there is no intragenerational terrorism threat, and does not share borders with high-risk jurisdictions.

The national threat level is formally reviewed annually but can change at any time based on the current intelligence picture. It considers the domestic terrorism context and relevant international threat factors. Although the national threat level for terrorism is low based on domestic terror threat, the terrorism financing threat must also include the financing of foreign terror threat. It is recognised that foreign terror threat is high in many parts of the world and widespread.

New Zealand has taken a range of measures in response to foreign and domestic terror threat. New Zealand has 22 non-UN designated listed entities designated in support of UN Security Resolution 1373.[62]

New Zealand has, to date, not frozen or seized assets in response to the resolution. This reflects that such assets have not been identified in New Zealand. However, reporting entities are critical in the identification of such assets and property. Groups designated in New Zealand include those with links to the Philippines, South America and Indonesia.

Terrorist financiers around the world have been known to use local diaspora communities to raise and move funds to support terrorist activities.

UN Security Resolution 1373 was adopted on 28 September 2001 following the 11 September terror attacks in the United States. The resolution required countries to implement laws that enabled the freezing of assets of designated entities.

[61] Also see Chapter 3: Vulnerabilities and NPO risk assessment in Chapter 5: Terrorism Financing.

[62] https://www.police.govt.nz/advice/personal-community/counterterrorism/designated-entities/lists-associated-with-resolution-1373

Raise, move and use

Terrorists adapt their behaviours to navigate AML/CFT measures as they raise, move and use funds. Although the risk associated with terrorism financing in New Zealand is low; the key vulnerability related to foreign terror activities and operations is the ability to move funds through New Zealand's borders.

As recognised in this NRA, the most vulnerable sectors are banking, MVTS and VASP – all of which provide services enabling cross-border movements of funds. These sectors are also the most vulnerable to terrorism financing.[63]

RAISE

Funding by third parties, receiving or soliciting donations, committing crime e.g., fraud and drug crime. Employment of legitimately acquiring funds.

MOVE

Send cash, remit funds via MVTS or the banks, misuse charities and NPO, smuggle cash, or smuggle high-value items such precious metals and stones.

USE

Purchase equipment to commit a terror act, travel to a conflict or other high-risk jurisdiction for training or to commit terror activities. Acquiring funds.

Much of the world funds that are used to finance terror acts include the physical carriage of cash or other high-value commodities, such as precious metals, across borders. Vigilance needs to be maintained at New Zealand's borders for both proceeds of crime and funds associated with terrorism being moved.

The 2019 NRA recognised that there was a possibility that New Zealand persons could sponsor terror through providing financial support directly or indirectly to Da'esh – also known as Islamic State of Iraq and the Levent (ISIL), the Islamic State of Iraq and Syria (ISIS), or the Islamic State (IS). IS was originally a branch of Al Qaeda. The prior NRA also recognised the possibility that persons in New Zealand could fund the activities of Hezbollah and right-wing extremist organisations.

Concerns in 2024 reiterate those of the 2019 NRA, highlighting that threat is presented by lone actors radicalised via the internet and white nationalist groups promoting extreme far-right nationalist ideology. The online presence of terrorist groups and the international connectivity via the internet means it is inevitable that people in New Zealand will have opportunity to be radicalised to the point that they may offer financial support to extremists.

Recent terror concern in the Middle East has occurred in countries such Israel, Lebanon, Jordan, Yemen, Pakistan, Iran and Iraq. Within these jurisdictions, there is much humanitarian work undertaken by non-government organisations (NGOs) and non-profit organisations (NPOs)[64] that require funding for their activities. These organisations therefore present some risks that they can provide a financial corridor for moving funds into geographical locations where terrorist and terror organisations are present. This can occur unwittingly.

Hamas[65], for example, was designated in its entirety as a terrorist organisation in February 2024. This is a large state-funded organisation that has the capability to move money

[63] See Chapter 3: Sector vulnerabilities summary, pages 34-42.

[64] An NPO is a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural education, social or fraternal purposes, or for the carrying out of other types of 'good works'.

[65] Harakat-al-Muqawama al-Islamiya.

around the globe. To date, it has not been identified that the financing of Hamas has occurred from New Zealand. However, funds have moved between New Zealand and Palestine, in 2022 and 2023. More funds were received into New Zealand from Palestine than were remitted to Palestine. From the transaction review, most were reported via the MVTS sector (60%) with the balance reported via the banks. A number of the transactions sent to Palestine involved charities.

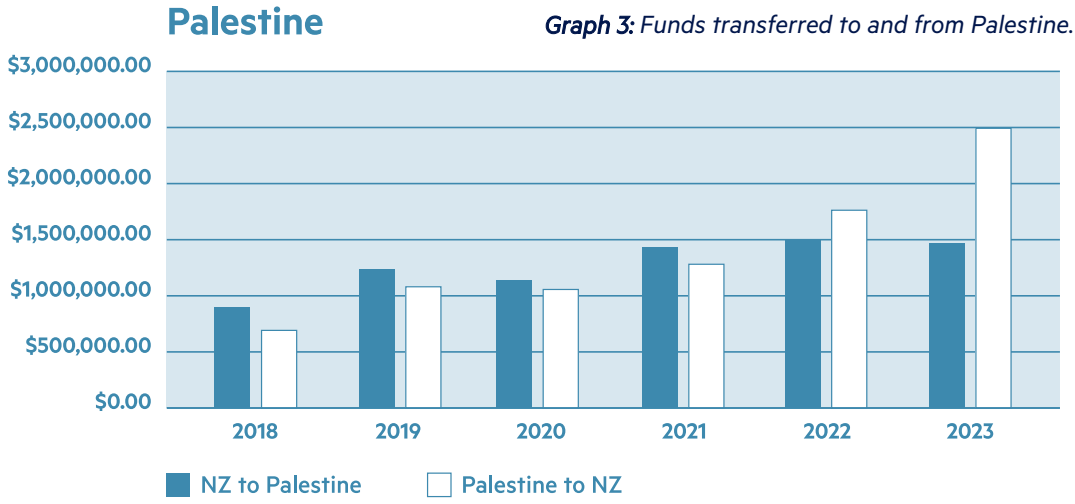
The 7 October 2023 attack in Israel by Hamas-led militants killed 1200 people and was the largest single terror attack since 9/11. The consequences have been immense and are still occurring with an estimated 25,000 Palestinians killed in the retaliatory miliary response.

Source of funds sent to Palestine

- 45% Electronically held funds
- 33% Cash
- 22% Credit card

Transferring funds through these sectors for humanitarian aid should not be discouraged; however, such transactions require careful scrutiny to ensure funds are used for their intended purpose.

It is recognised in this NRA that the MVTS sector has been misused by criminals, demonstrating that this sector presents vulnerability. It is important from a TF perspective that this sector has a clear understanding of risk and is subject to robust supervision.



Graph 3: *Funds transferred to and from Palestine.*

Table 16: *International Fund Transfers (IFTs) to and from Palestine.*

YEAR	NZ TO PALESTINE	PALESTINE TO NZ
2018	$869,750.14	$674,885.63
2019	$1,190,707.00	$1,065,336.63
2020	$1,110,427.79	$1,058,209.35
2021	$1,449,680.83	$1,293,999.87
2022	$1,494,252.98	$1,777,772.90
2023	$1,475,494.35	$2,471,941.74
GRAND TOTAL	$7,590,313.09	$8,342,146.12

How are terrorist organisations funded?

Internationally

In the global environment, cash is extensively used by terrorists and their supporters to fund terrorist-related operations. As financial institutions (including banks and money remitters) have enhanced their AML/CFT systems, the ability for terrorists to reliably use financial systems has become more challenging in terms of risk, cost and time. In response, terrorists (and other transnational criminals) have more frequently turned to cash to transfer funds.

In June 2022, New Zealand designated the 'American Proud Boys' as a terrorist entity. It has been identified that New Zealanders were purchasing Proud Boys' merchandise. It is unknown how this merchandise was funded.

CASE STUDY

In an overseas example from the Asia-Pacific region, a citizen from one country travelled to another country on multiple occasions with gold and cash that were not declared when she crossed borders. The gold and cash were intended to finance foreign fighters and to provide financial support to ISIS. This demonstrates the importance of preventing the smuggling of large amounts of cash across borders.

Cryptocurrency[66] has a reputation of offering anonymity. For those involved in crime and terrorism, anonymity is important. For this reason, the raising and moving of funds domestically and internationally using cryptocurrency has been observed.

The individual responsible for the Christchurch terror attack made donations to extreme right-wing organisations using cryptocurrency. Internationally, ISIS has been identified as the owner and controller of virtual assets. There is therefore potential that cryptocurrency can be raised and moved to finance terrorism.

Stored value cards or travel cards are a popular method of legitimately moving money offshore. In the experience of other countries, these have been used to support terrorism financing, and foreign terrorist fighters have used them before and after departure to their destination. These cards can be loaded domestically with cash or via non-reportable electronic methods, are easily carried (or posted) offshore and are not subject to reporting requirements. Funds can be redeemed through multiple offshore ATM withdrawals, restricted only by ATM withdrawal limits. Cards can also be regularly reloaded remotely and anonymously by third parties. These types of products therefore have elevated risk.

The lone self-funded terrorist is difficult to identify, and therefore payments made to the likes of extreme right-wing groups is important intelligence to help identify and prevent the occurrence of crimes motived by extremism.

Narrations in transactions which are possible indicators include:

- Particular references: "6 million more"
- Donating $14.88 or using 14.88 in references
- Acronyms for groups overseas – e.g., NSN (nationalist socialist network)

Domestically

New Zealand has experienced two terror attacks in the last five years. The Christchurch terror attack happened in March 2019; 51 people were murdered along with the attempted murder of 40 others. This attack was motivated by white nationalist, anti-immigration sentiment and white supremacist beliefs. A second incident occurred in Auckland in 2021 where eight people were injured in an ISIS-inspired attack.

Lone self-funded terror attacks undertaken at relatively short notice are regarded as the most likely type of terrorism expected in New Zealand. Funding may be limited to purchasing a knife or vehicle, acquiring legally or illegally obtained firearms, axes, hammers, screwdrivers etc. It is recognised that it is challenging to identify these types of criminals through isolated transactional activity; what is required is the identification of a number of indicators that collectively provide grounds for concern.

Many countries identify that self-funding from legitimate sources is the most used method of raising funds used to finance terrorism, particularly for foreign terrorist fighters travelling to conflict zones. It generally occurs in small volumes, and transactions are most often conducted in cash

[66] See Chapter 3, pages 41 and 42.

or through legitimate financial channels. In observed cases, funds are mainly derived from income, sale of personal items, credit cards, loans, state funded benefit (welfare) payments and pension funds or superannuation.

Christchurch case study

Prior to the attack, the individual lived in Dunedin. Living expenses and the financing of preparation and property used in the attack were funded by money from inheritance income. He was an additional cardholder for a credit card registered in a family member's name in Australia. He was, however, the exclusive user of that account.

The individual travelled extensively between 2014 and 2017, including 89 border movements. Financial records identified travel to an additional two countries in Europe.

While living in New Zealand, the individual made at least 14 donations to far-right, anti-immigration groups and individuals. Some of these donations, totalling AU
$6,305.78, were made directly from the individual's Australian bank account through a payment service provider. There were an additional five donations made using Bitcoin. The largest Bitcoin donation was US$1,377. The VASP involved in these transactions no longer operates in New Zealand.

Accounts were operated in New Zealand and Australia. Unusual activity included the lack of employment income – he advised one bank that he was 'seeking employment' yet remained unemployed. His banking activity included exceptionally high firearms spending in proportion to his overall spending. These accounts did not contain the right-wing donations and only limited travel expenditure.

Finally, the individual's financial behaviour was not stable, consistent or predictable. The significant funds he received afforded him the ability to travel, and to avoid the common, more predictable, lifestyle requirements such as employment. When there is an absence of consistency, it is difficult to identify changes in behaviour. It may be that this level of inconsistency would have been the best indicator for the banks. It is critical that the banks understand their customer.

SAR review

974 SARs related to suspicion of TF have been submitted in the last five years.

The FIU identified that reporting entities are not routinely using the TF indicators when submitting reporting, making it challenging to accurately identify TF-related reporting.
The vast majority of all reporting has occurred from the banking sector. Other reporting entities include money remitters and VASPs. A review of reporting identified a shift from primarily Islamist-related reasons for suspicion, prior to 15 March 2019, to reporting focused on right-wing extremism. General themes in reporting include:

- Payment reference of concern (e.g., 1488).
- Cash deposited into a bank account followed by remittance offshore.
- Purchase of army / outdoors / hunting clothing and equipment including firearms.
- Payments to crowdfunding platforms.
- Payments to right-wing groups and individuals associated with right-wing groups.
- Payments being made to offshore accounts where the account holder is travelling or has travelled to a conflict zone.
- Screening match for customer / recipient - or Sanctions Related, or Offshore Terrorism Links.
- Attempted / remittance to offshore sanctioned charity / charity.
- Cash withdrawn in a high-risk jurisdiction.

Many SARs were due to the bank seeing a number of indicators in the banking activity of the account holder – this is positive.

Recognised indicators

CUSTOMER BEHAVIOUR

- Using the same address or phone number for multiple customers.
- Using false identification or fraudulent documents.
- Requesting multiple cards linked to common funds or purchasing multiple stored value cards.
- Emptying out bank accounts and savings.
- Selling assets including personal belongings.
- Receiving funds from and sending to unrelated businesses that do not align with the client's business profile. This behaviour includes an absence of regular salary payments and business-related activity.
- Utilising financial services at retailers to buy equipment that could be used for terrorist activity.
- Parties to the transaction are linked to known terrorist organisations, entities, or individuals engaged or suspected to be involved in terrorist activities.

Transaction monitoring

- A sudden increase in business/account activity, inconsistent with customer profile.
- Numerous and frequent transfers into a personal account described as donations, humanitarian aid, or similar.
- Absence of expected transactions such as regular income or unemployment benefits, normal debit, and credit account activity and/or paying bills.
- Transactions to accounts associated with known terrorist organisations, entities or individuals that are engaged, or suspected to be involved in terrorist activities.
- Transactions referencing numerical combinations or terms associated with terrorist ideologies.

High-risk jurisdictions

- Transfers to and from high-risk jurisdictions, at multiple branches of the same reporting entity.
- Multiple customers conducting funds transfers to the same beneficiary in a high-risk jurisdiction.
- Funds transfers to multiple beneficiaries located in high-risk jurisdictions.
- Vague justifications and a lack of documentation for requests to transfer funds to high-risk jurisdictions or entities.
- Transactions to locations bordering high-risk jurisdictions.
- Parties to the transaction are based in countries or returning from conflict zones known to support terrorist activities.

> Foreign fighters may use ATMs within a conflict region to withdraw cash using debit, stored value or credit cards. False identification documents or the use of accounts held by family members may also feature in this type of transaction activity.

High-risk jurisdictions

The 2023 Global Terrorism Index[67] identifies the ten countries most impacted by terrorism.

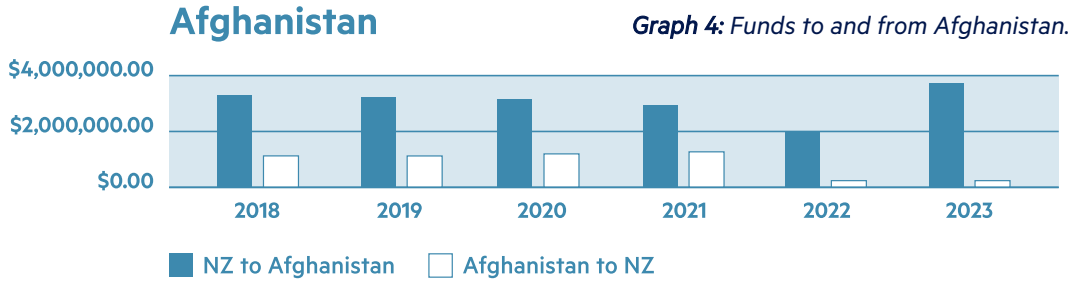
Prescribed transaction reporting and SARs confirm that New Zealand remits and receives modest values of funds from these countries. The risk of terrorism within a jurisdiction is an element when examining the purpose of a transaction.

Table 17: *2023 Global Terrorism Index.*

RANK	COUNTRY	SCORE (OUT OF 10)	RANK CHANGE
1	Afghanistan	8.822	↔
2	Burkina Faso	8.564	2 ↑
3	Somalia	8.463	↔
4	Mali	8.412	3 ↑
5	Syria	8.161	1 ↑
6	Pakistan	8.160	3 ↑
7	Iraq	8.139	5 ↓
8	Nigeria	8.065	3 ↓
9	Myanmar (Burma)	7.977	1 ↑
10	Niger	7.616	2 ↓

Regionally, the impact of terrorism is far higher in Sub-Sahara Africa, the Middle East and North Africa, and South Asia. These three regions accounted for 94% of all deaths from terrorism in 2023. Globally in 2023, there were 8352 deaths from terrorism.

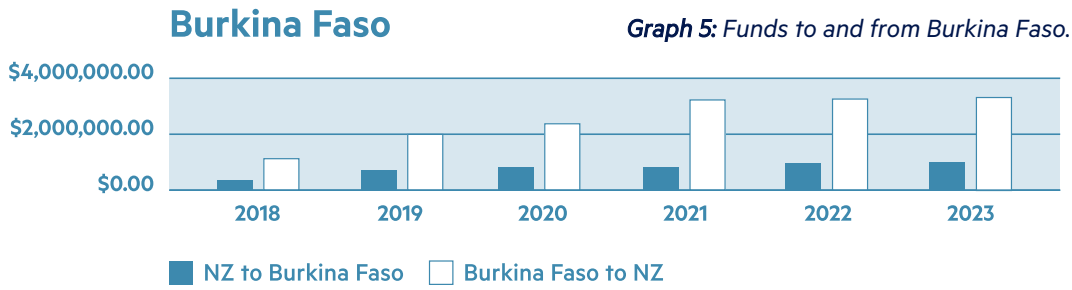
[67] 2023 Global Terrorism Index - https://www.economicsandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf.



Graph 4: *Funds to and from Afghanistan.*

Table 18: *Afghanistan.*

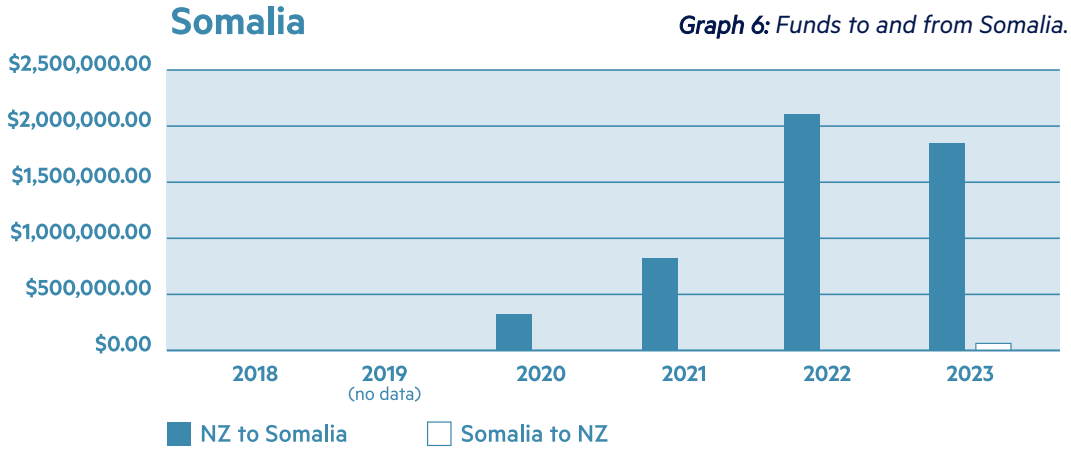
YEAR	NZ TO AFGHANISTAN	AFGHANISTAN TO NZ
2018	$3,311,877.92	$1,086,705.81
2019	$3,285,622.83	$1,113,362.42
2020	$3,215,422.97	$1,148,997.09
2021	$2,998,638.44	$1,259,405.12
2022	$2,022,662.51	$209,167.76
2023	$3,737,662.77	$245,214.61
GRAND TOTAL	$18,571,887.44	$5,062,852.81



Graph 5: *Funds to and from Burkina Faso.*

Table 19: *Burkina Faso.*

YEAR	NZ TO BURKINA FASO	BURKINA FASO TO NZ
2018	$263,688.07	$946,131.43
2019	$602,598.94	$1,953,643.94
2020	$856,987.66	$2,305,990.72
2021	$739,635.85	$3,203,006.79
2022	$1,047,368.17	$3,343,651.46
2023	$1,013,198.50	$3,364,913.56
GRAND TOTAL	$4,523,477.19	$15,117,337.90

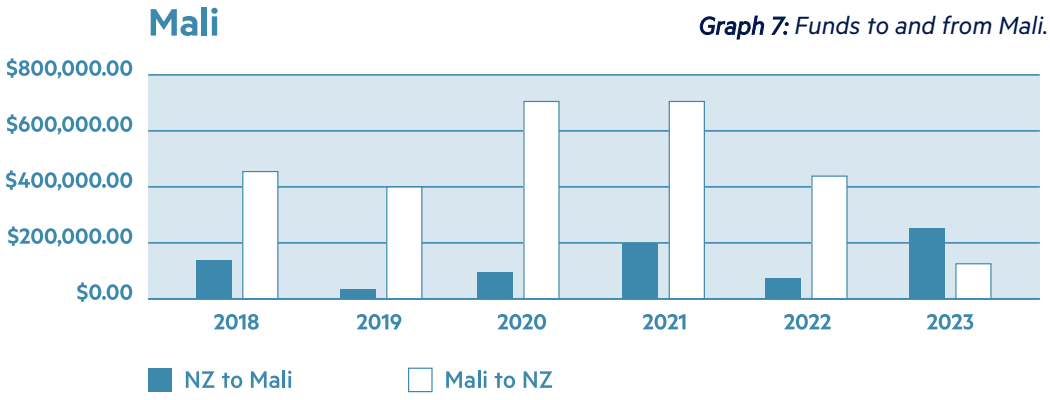


Graph 6: *Funds to and from Somalia.*

Table 20: *Somalia.*

YEAR	NZ TO SOMALIA	SOMALIA TO NZ
2018	$7,002.97	$4,100.00
2020	$324,761.90	-
2021	$828,669.63	$15,011.56
2022	$2,070,062.57	$27,415.68
2023	$1,809,668.80	$49,991.71
GRAND TOTAL	$5,040,165.87	$96,518.95

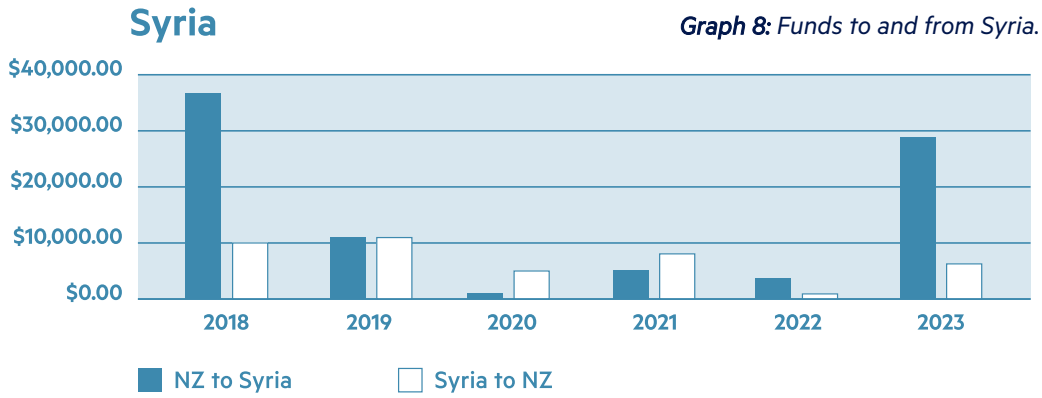
For the period 1 Jan 2020 to 31 Dec 2023, there was a small number of SARs that referenced Somalia. These related to cash being remitted offshore by Somalian nationals in New Zealand. In addition, there was reporting that referenced Somalia, and investment in cryptocurrency, preceded by cash deposits. Lastly, Somalia was referenced in the remittance of Covid-19 wage payments.



Graph 7: *Funds to and from Mali.*

Table 21: *Mali.*

YEAR	NZ TO MALI	MALI TO NZ
2018	$155,955.05	$463,272.65
2019	$26,613.76	$400,756.51
2020	$115,386.67	$680,293.59
2021	$191,501.63	$711,217.02
2022	$100,881.29	$450,791.05
2023	$249,871.53	$124,825.73
GRAND TOTAL	$840,209.93	$2,831,156.55

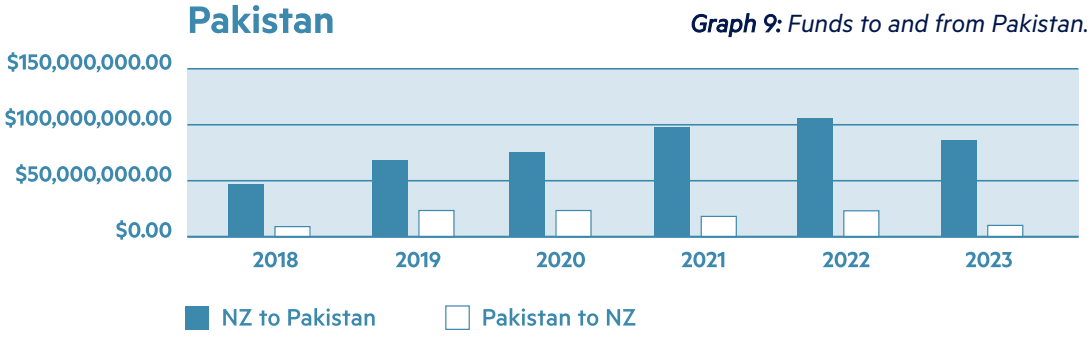


Graph 8: *Funds to and from Syria.*

Table 22: *Syria.*

YEAR	NZ TO SYRIA	SYRIA TO NZ
2018	$37,626.28	$10,413.73
2019	$10,869.45	$12,039.61
2020	$1,000.00	$4,523.10
2021	$4,384.25	$8,506.87
2022	$3,572.00	$1,500.00
2023	$28,976.12	$6,604.12
GRAND TOTAL	$86,428.10	$43,587.43

For the period 1 Jan 2020 to 31 Dec 2023, SARs were submitted in relation to individuals and one charity sending funds to Turkey, Syria, or Lebanon. Some SARs related to online banking being accessed from Syria; some were regarding suspected scam victims. There was also a SAR involving intended travel to Syria.

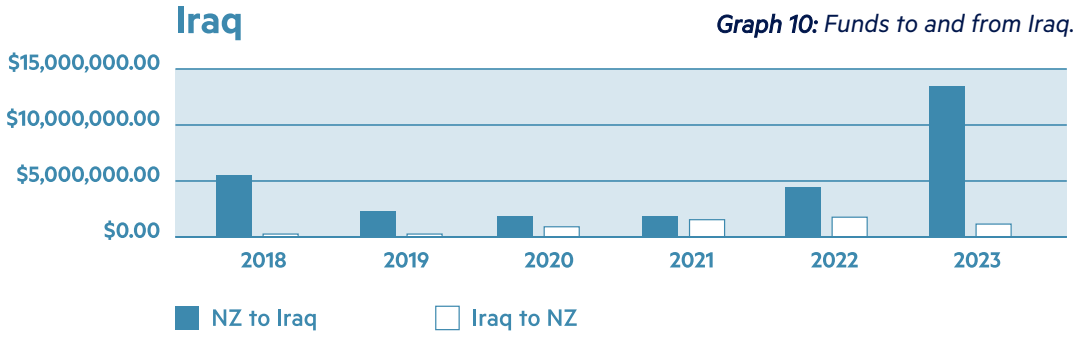


Graph 9: *Funds to and from Pakistan.*

Table 23: *Pakistan.*

YEAR	NZ TO PAKISTAN	PAKISTAN TO NZ
2018	$46,731,899.91	$10,223,140.59
2019	$65,918,636.29	$22,582,480.27
2020	$74,569,478.49	$21,844,283.58
2021	$96,505,424.71	$18,342,566.18
2022	$104,542,296.19	$23,133,791.70
2023	$83,045,727.21	$10,979,043.57
GRAND TOTAL	$471,313,462.80	$107,105,305.89

For the period 1 Jan 2020 to 31 Dec 2023, there were 398 SARs referencing Pakistan. The vast majority was regarding remittance to Pakistan.

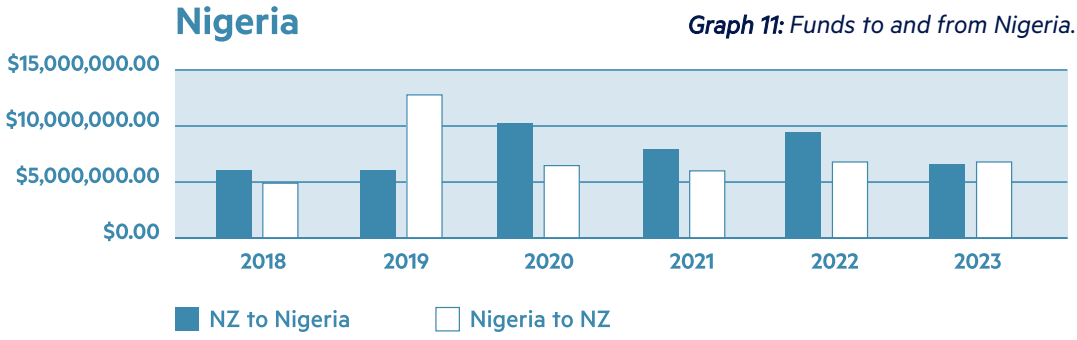


Graph 10: *Funds to and from Iraq.*

Table 24: *Iraq.*

YEAR	NZ TO IRAQ	IRAQ TO NZ
2018	$407,689.49	$5,500,107.24
2019	$387,092.65	$2,326,356.20
2020	$931,246.31	$1,919,968.49
2021	$1,539,872.01	$1,795,338.99
2022	$1,792,975.45	$4,304,726.81
2023	$1,266,186.73	$13,244,480.00
GRAND TOTAL	$6,325,062.64	$29,090,977.73

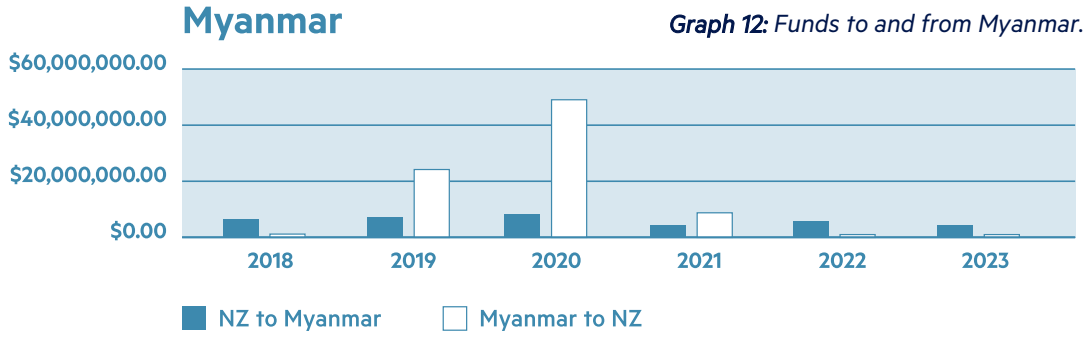
A sample of 40 SARs that were submitted during the period 1 Jan 2020 to 31 Dec 2023 were reviewed. Most related to remittances to Iraq involving cash. However, two identified cash drawings from ATMs in Iraq. One related to a cash withdrawal in New Zealand of tens of thousands of dollars which was intended to be physically taken to Iraq.



Graph 11: *Funds to and from Nigeria.*

Table 25: *Nigeria.*

YEAR	NZ TO NIGERIA	NIGERIA TO NZ
2018	$5,920,355.91	$5,018,949.36
2019	$6,014,084.50	$12,673,840.23
2020	$10,076,898.37	$6,596,907.03
2021	$7,821,654.04	$6,059,702.70
2022	$9,271,344.71	$6,785,794.35
2023	$6,436,804.73	$6,665,872.60
GRAND TOTAL	$45,541,142.26	$43,801,066.27

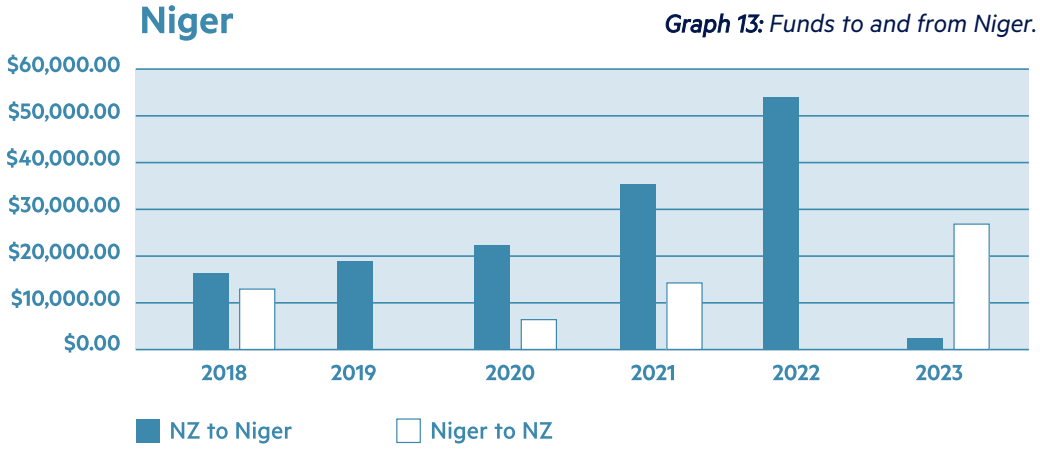


Graph 12: *Funds to and from Myanmar.*

Table 26: *Myanmar.*

YEAR	NZ TO MYANMAR	MYANMAR TO NZ
2018	$6,458,503.96	$959,745.40
2019	$7,945,244.59	$24,782,771.91
2020	$8,728,435.45	$49,797,337.47
2021	$4,588,863.97	$9,478,658.30
2022	$5,760,085.15	$251,101.17
2023	$4,572,530.42	$95,522.92
GRAND TOTAL	$38,053,663.54	$85,365,137.17

Myanmar was blacklisted by the Financial Action Task Force (FATF) in October 2022. Iran and the Democratic People's Republic of Korea (the DPRK or North Korea) are also blacklisted jurisdictions considered high-risk for ML/TF/PF.[68]



Graph 13: *Funds to and from Niger.*

Table 27: *Niger.*

YEAR	NZ TO NIGER	NIGER TO NZ
2018	$16,453.15	$13,060.52
2019	$19,007.01	$0
2020	$21,911.90	$6,182.96
2021	$35,667.11	$14,412.31
2022	$54,329.96	$0
2023	$2,058.09	$27,048.70
GRAND TOTAL	$149,427.22	$60,704.49

[68] Refer to Chapter 6: Proliferation Financing.

Table 28:

	SOURCE OF FUNDS			SECTOR		
DESTINATION	CASH	CREDIT CARD	ELECTRONICALLY HELD FUNDS	MVTS	BANK	OTHER
Afghanistan	61%	17%	23%	82%	18%	-
Burkina Faso	1%	1%	99%	9%	87%	4%
Iraq	62%	13%	25%	60%	22%	18%
Mali	14%	21%	65%	49%	51%	-
Myanmar	49%	10%	41%	76%	24%	-
Niger	1%	12%	87%	47%	53%	-
Nigeria	4%	29%	67%	55%	32%	13%
Pakistan	5%	10%	85%	30%	63%	7%
Somalia	24%	51%	24%	97%	2%	-
Syria	100%	0%	0%	100%	-	-

This table depicts the sources of funds[69] transferred from New Zealand to the ten countries most impacted by terrorism, and the sector through which they were transferred, for the period January 2018 to December 2023.

The source of funds remitted offshore differed by destination country. Cash was the primary source of funds remitted to Afghanistan, Iraq, Myanmar, and Syria. The sources of funds across all ten countries were cash (10%), credit card (12%), and electronically held funds (78%).[70]

Over half of all funds sent to these high-risk jurisdictions from New Zealand were through the banking sector; however, the use of the MVTS sector featured heavily in the high volume-low value transactions that are recognised as being higher-risk for TF. This demonstrates the risk within the banking and MVTS sectors.

Although VASPs and virtual assets do not feature in this review, virtual assets; fintech; crowdfunding and social media can be used by terror organisations to raise and move funds across borders. Although virtual assets can enable cross-border movement of wealth, terror organisations are likely to convert VAs to cash before use. The process of off-loading VAs presents risk.

[69] Source of funds (SOF) is recorded by the reporting entity when the transaction takes place.
[70] Caveat: the transaction source includes bank accounts held by remittance companies, so the original source of funds could be cash in these cases.

Relationship between crime which domestically threatens New Zealand's AML system & terrorism

Terrorist organisations are known to actively participate in crime and transnational crime to raise finance. This NRA identifies the increasing prevalence of cyber-enabled frauds and scams and the impact of transnational drug crime on New Zealand.[71]

These crimes are recognised as high-threat crime related to money laundering. It is possible that some of this offending may be motivated by terrorists and terrorist organisations to raise and move funds to financially support their operations. Countering domestic crime threat has relevance to countering the financing of terrorism.

Outlook

The outlook for across the international environment is also uncertain. The conflict in Gaza has heightened the possibility of terror attacks across the Middle East and North Africa region, and in states perceived as supportive of Israel. Ongoing deterioration of security in sub-Sahara Africa may result in increased conflict and terrorist activity and therefore movements of funds into those areas is higher risk than into countries and regions with low occurrence of terrorism. Sectors involved in cross-border remittance activity into these areas will have continued heightened risk.

Right-wing extremism continues to pose a threat to democratic societies. The ideas associated with the far-right have been present for decades; however, the growth and spread of these ideas is on the rise. The identification of the raising of funds to promote the ideology associated with far-right extremism requires a highly vigilant AML/CFT system. This, combined with strong international coordination, supports the identification of networks and individuals who may present a threat.

Non-Profit Organisation (NPO) sector

A non-profit organisation is one that does not operate for profit; personal gain; or benefit of the people who run it, their friends or relatives. The FATF definition of an NPO is a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural or educational, social or fraternal purposes, or the carrying out of other types of good works.[72] These organisations play a vital role in providing charitable services around the world as well as helping within regions of conflict in which terror organisations also operate.[73]

> Globally there remains a threat of misuse of the NPO sector by terrorist organizations. While, in context of the size of the global NPO sector, the probability of this occurring is recognised to be low, the impact (or consequences) of abuse of the NPO sector by a terrorist organisation will have a significant impact on donor trust and confidence in the sector. In the absence of donor funds, the operation and vital 'good works' of NPOs cannot be delivered. For this reason, it is critical that terrorist organisations are prevented from misusing this sector to raise and move funds.
>
> *The Risk of Terrorist Abuse in NPOs - FATF 2014.*

No NPO in New Zealand has been implicated in terrorism financing. In the domestic context, NPOs present extremely low or non-existent risk associated with domestic terrorism

[71] Refer to Threats, Chapter 2.
[72] FATF recommendation 8 does not apply to the NPO sector. FATF has adopted a functions definition of an NPO. This definition is based on those activities and characteristics of an organisation that put it at risk of terrorist abuse rather than based on the simple fact that it is operating on a non-profit basis.

[73] Refer to page 78, footnote 67 of this chapter.

financing. This assessment has focused on NPOs with international connectivity.

There are currently 28,970 registered charities in New Zealand. In the financial year ending 30 June 2023, registered charities had $81 billion of assets and received $ 24 billion in income.[74] Of these charities, 167 undertake overseas operations.

New Zealand NPOs require registration and administrative oversight. Schools and other organisations, for which donors (persons who make a donation) can claim a tax credit, have additional oversight through the likes of the Ministry of Education. Most of the other tax-exempt NPOs that are not registered charities fall into organisations who promote amateur sports.

What could make an NPO attractive for a terrorist organisation?

- NPOs can have an ability to raise and move funds into an area where both the NPO and terrorist organisations are operating. This means there is a higher vulnerability when the NPO is providing service activities near geographic areas with active terrorist threat.
- NPOs have a global presence and are often established in high-risk areas and conflict zones. NPOs have access
- to often large volumes of donations, which are derived form a wide range of sources, often in cash, and often from a wide range of jurisdictions.
- NPOs' funds could be susceptible to theft, when NPOs are distributing funds within countries in which terrorist organisations also operate.

While it is vital to protect NPOs from terrorist abuse, it is also important that the measures taken do not disrupt or discourage legitimate charitable activities and should not restrict an NPO's ability to access resources – including financial resources to carry out the legitimate activities. Rather, measures should promote transparency and engender greater confidence in the sector, across the donor community and with the general public that charitable funds and services are reaching their intended legitimate beneficiaries.

NPOs with overseas connectivity

Data captured via NPO annual returns is limited. Information which identifies how the goods or service were provided, the beneficiary, and how it was confirmed that the goods or service was received by the intended recipient is not captured.

From 88 charities, an estimated $19.7M was distributed offshore in 2023 through 247 disbursements to the following continents or regions:

ASIA	87	disbursements
OCEANIA	73	disbursements
AFRICA	41	disbursements
EUROPE	37	disbursements
SOUTH AMERICA	9	disbursements

Although some of these continents or regions contain terror-related conflict zones, information is not captured from the charities as to the destination and purpose of these disbursements.

NPOs engaged in service activities – such as providing housing, education or healthcare – are more vulnerable than NPOs with focus on the arts, recreation or sports.

Key risks

- Diversion of funds – where persons within the NPO or when foreign partners of third party fundraisers divert funds to support terrorist entities through NPO operational or financial processes.
- NPOs or their officials knowingly or unknowingly maintaining a relationship with a terrorist entity which may result in a range of outcomes – from abuse of the NPO to providing logistical support to the terrorist entity.
- Abuse of programmes where the flow of funds from the NPO programmes is legitimate but then are abused at the point of delivery. For example, a programme purchases vehicles to transport children to school, but upon delivery, the vehicles are used by a terrorist entity.
- Sham NPOs where terrorist entities represent themselves as providing good works to deceive donors into providing support. Complex deceptions are difficult for non-government organisations to detect, hence the need for government oversight and supervision of the NPO sector.

[74] This information is taken from self-reported data and does not include information from charities who are yet to file their annual returns.

Current mitigation

Charities Services investigation work is primarily complaint-driven and has an exclusively domestic focus. Investigations tend to relate to the misappropriation of funds, including loans to related parties.[75] In addition, investigations have focused on the management of charities, the identification documents used as part of the registration process, and the attempts to register shelf charities by overseas individuals. Although these investigations do not specifically relate to possible terrorism financing, these activities demonstrate the type of supervision and investigation that preserves the integrity of the NPO sector.

An American lawyer sought to establish a series of charities. The purpose was to sell the charities as products associated with tax minimisation in a foreign jurisdiction. The registrations were declined.

All charities are reviewed and become subject to a 'risk rating' when seeking registration. Participating in overseas operations, or exposure to possible TF risk is not a feature of this risk rating exercise. Ongoing auditing occurs to ensure compliance with accounting principles – this auditing should also identify donors and the existence of other counter- terrorism financing measures such as ensuring that offshore disbursements are spent in a manner consistent with the NPO-stated activities.

SAR Review

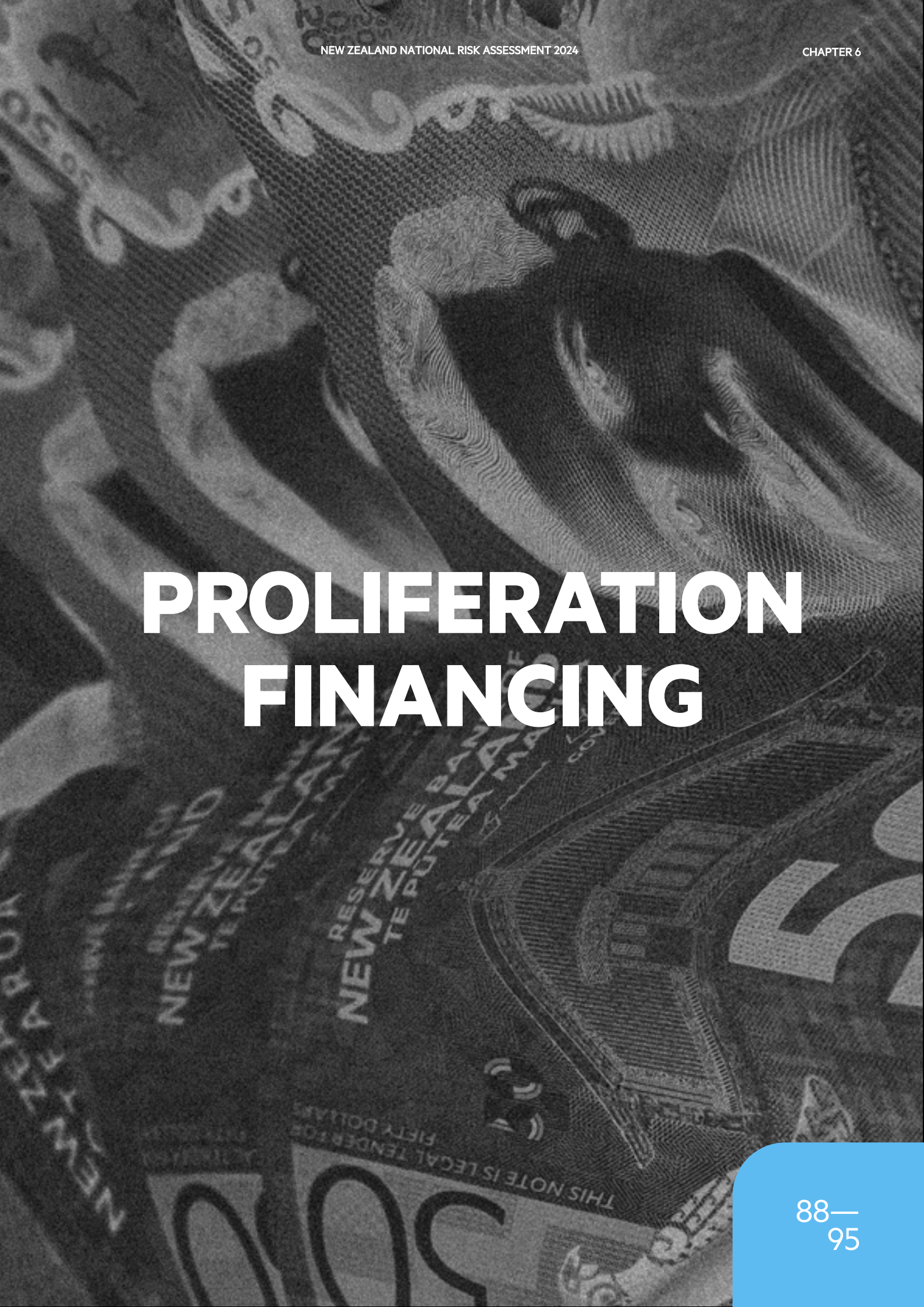
Between January 2020 and December 2023, 532 SARs that include reference to a charity were submitted. 102 SARs were sampled, of which only 36 were related to suspicious activity on a charity account, or suspicious activity in relation to a charity. No reporting related to suspected terrorism financing; however, reasons included remittance of funds to an offshore charity,[76] suspected misappropriation of charity funds, suspected misuse of a charity to evade tax obligations, and large cash deposits into a charity bank account.

Summary

Charities and NPOs with international connectivity and operations present higher TF risk that those with pure domestic focus. There is no known occurrence where a New Zealand NPO has been involved in terrorism financing. Improved reporting requirements as part of the annual return process for NPOs that undertake offshore operations and activities would improve optics and risk understanding related to TF risk. Risk of the New Zealand NPO sector being misused to support or finance terror activities is considered low.

[75] On page 68, refer to the 'A senior member of a prominent New Zealand gang had a controlling influence over a charitable trust…' case study.

[76] Including funds remitted to Palestine.



PROLIFERATION FINANCING

Proliferation Financing (PF) Risk Assessment

This is the first PF risk assessment New Zealand has undertaken. It explains PF, addressing risk by identifying and assessing risk associated with potential breaches and non-implementation of targeted financial sanctions related to PF.

This assessment also reviews New Zealand's vulnerabilities in enabling PF, and provides information to support government and private sector understanding of associated risk in deterring and detecting PF.

Defining proliferation financing

PF is so much more than the exchange of funds for weapons of mass destruction (WMDs):

1 **REVENUE-RAISING ACTIVITIES**

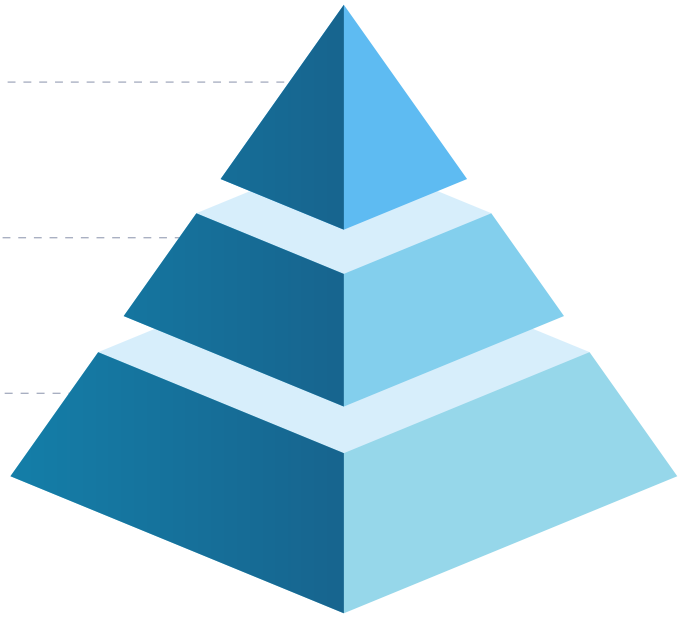
The activities that generate revenue to finance the procurement and development of WMDs

2 **TRADE IN PROLIFERATION-SENSITIVE GOODS AND TECHNOLOGIES**

The financial products and services associated with trade in goods that are directly useable or modifiable for use in the development of WMDs

3 **LEGAL PERSONS AND LEGAL ARRANGEMENTS**

Any kind of legal person or legal arrangement that facilitates activities included in the above two categories, as well as any assets or financial services provided to individuals or entities subject to targeted financial sanctions



Graph 14: *Defining proliferation financing.*

PF explained

The Financial Action Task Force (FATF) have defined proliferation financing as:

"The act of providing funds or financial services that are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, biological weapons and their means of delivery and related materials".

Those involved in PF are often sophisticated criminals who actively seek out vulnerabilities within countries around the world. They use these vulnerabilities to fund the development of nuclear, chemical, and biological weapons.

Proliferators of weapons of mass destruction – such as the Democratic People's Republic of Korea (the DPRK or North Korea/NK) and Iran[77] – fund their programmes through illicit means, evading international sanctions in the process.

It may be easy to dismiss PF and say "We don't have a nuclear industry", and/or "We don't produce high-tech goods. Why is it relevant to us?" But often the physical movement of goods is divorced from the financial activity supporting this movement. Even though there might not be high-tech manufacturing in New Zealand or the production of nuclear-related goods, financing of the production of the goods may pass through banks that are located in New Zealand, or companies registered in New Zealand.

Trade in Proliferation-Sensitive Goods and Technologies could include procurement of sensitive goods, technologies, and materials that can be used for developing nuclear weapons or chemicals for chemical weapons. This includes sourcing of expertise to construct these weapons.

Revenue-raising activities are a critical element of PF. This is because technology and the components associated with the manufacture of the described weapons are very expensive; funding is often generated through crime[78] or business activities and then invested in weapons manufacture. This is particularly relevant to the DPRK which is largely prohibited from engaging in economic activity outside of its borders.

Some activities they engage in to raise revenue are illicit, others are entirely legal unless they're carried out on behalf of, or to benefit the DPRK.

CRIME RAISING ACTIVITIES – DPRK

- Cybercrime
- Counterfeiting and fraud
- Wildlife trafficking

LICIT RAISING ACTIVITIES – DPRK

- Restaurants
- Building and construction – in some African countries
- IT services
- Sales of minerals and natural resources

Jurisdictions most at risk have political ties or connection, host embassies, and/or industries attractive to the DPRK.

Legal persons and arrangements (companies etc.)s can be used to support procurement of and trade in sensitive goods and revenue-raising activities. These, along with the export of certain types of materials, have the most relevance to PF risk in New Zealand.

Risk therefore can occur through poor corporate transparency, including transparency regarding beneficial ownership.

The DPRK conducted its first nuclear test in 2006. It produces enriched uranium and weapons-grade plutonium and has developed sophisticated nuclear weapons and ballistic missiles. The DPRK tested a likely thermonuclear device in

[77] UN Sanctions against Iran have lapsed and as yet FATF have not provided specific guidance on next steps with Iran.

[78] See Chapter 2: Criminal Threats to New Zealand's AML/CFT/PF System.

2017. It agreed to a moratorium on nuclear and long-range missile testing in 2018; it resumed long-range missile tests in 2020.

Iran's nuclear ambitions have been a focus of international diplomacy for decades. It runs large, increasingly sophisticated ballistic missile and space launch programmes. Iran initially received foreign assistance for these programmes, particularly from North Korea, but today can run these programmes by itself. It supplies missiles and rockets to partner and proxy groups in Iraq, Lebanon, Syria, and Yemen.

International Funds Transfers (IFTs)

TO AND FROM THE DPRK

Diplomatic relations between New Zealand and the DPRK are very limited. There have been no transfers or funds to or from the DPRK. There has been no trade between New Zealand and the DPRK although it is possible that some exported products enter the DPRK via China.

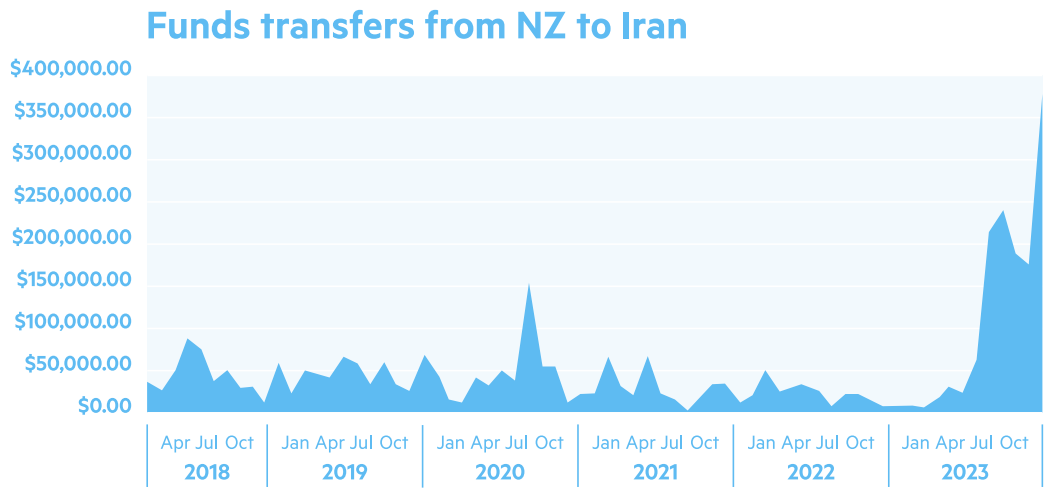
TO AND FROM IRAN

New Zealand has an embassy in Iran. In the 1980s, Iran was one of New Zealand's significant trading partners but sanctions have impacted on trade. The Ministry of Foreign Affairs and Trade advises that all persons and companies obtain legal advice prior to doing any form of business with Iran, given the existence of sanctions. Limited funds currently move between New Zealand and Iran.

China is both New Zealand and the DPRK's largest trading partner. Over the past three years, payments from China to New Zealand have averaged $19B annually. These payments will largely relate to goods and services exported to China.

China has a defence treaty with the DPRK (the only defence treaty China has with any nation).

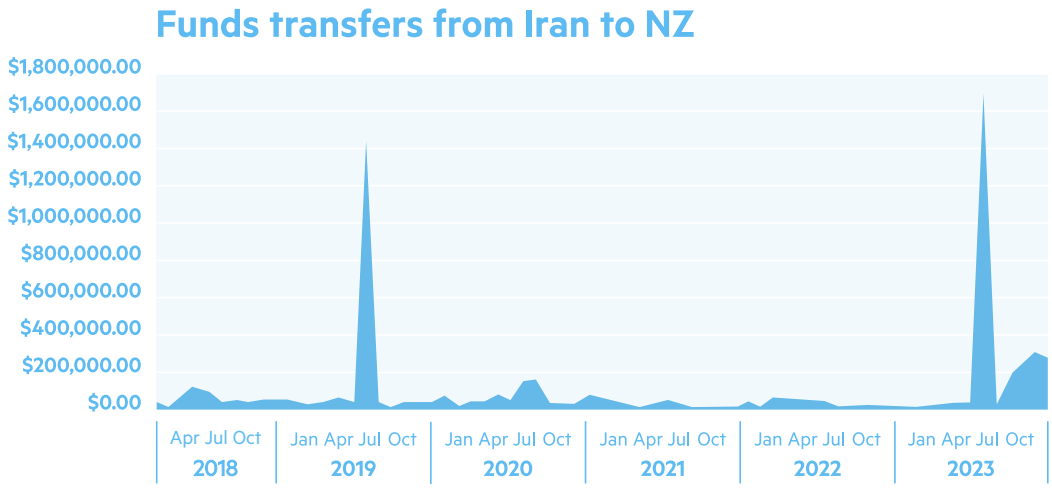
In 2018, a New Zealand company was prosecuted for breaching UN sanctions and exporting aircraft parts to the DPRK. The parts related to an aircraft that had been earlier sold and exported to China. After being exported to China, the aircraft was found to be operating in the DPRK, where the parts were directly supplied.



Graph 15: *Funds transfers from NZ to Iran.*

YEAR	IFT – NZ TO IRAN
2018	$408,735.00
2019	$491,855.00
2020	$562,693.00
2021	$353,400.00
2022	$251,772.00
2023	$1,346,310.85
GRAND TOTAL	$3,414,765.85

Table 29: *Funds transfers from NZ to Iran.*



Graph 16: *Funds transfers from Iran to NZ.*

The two large payments were made to a non-bank currency exchange business. This demonstrates the occurrence of financial activities between Iranian and New Zealand financial service providers.

YEAR	IFT – IRAN TO NZ
2018	$463,892.00
2019	$1,865,888.69
2020	$692,981.80
2021	$308,366.00
2022	$362,435.00
2023	$2,831,833.13
GRAND TOTAL	$6,525,396.62

Table 30: *Funds transfers from Iran to NZ.*

International research – typologies

- Dealers in precious metals and stones (DPMS) are vulnerable to attempts by the DPRK to both procure and sell precious metals and stones.
- The real estate sector appears to be targeted by the DPRK, mostly for income-generating purposes. DPRK use of real estate includes property development (33%of real-estate cases) and the leasing or rental of commercial (50%) or residential (17%) properties for rental income. While the buying of property for rental purposes is subject to AML/CFT regulation, the subsequent renting or leasing activities fall outside the regulations' scope and provide a potential regulatory and awareness gap for the DPRK to exploit.
- Gatekeeper professions play an important role in facilitating DPRK sanctions evasion so more awareness of sanction obligations in these sectors is needed.
- At least 25% of cases reviewed during international research on PF indicates that the DPRK in-sourced gatekeeper services, meaning that it either performed these services itself or provided gatekeeper services to others. More research is needed to understand the exact ways and extent to which the DPRK operates in these sectors.

IN NEW ZEALAND
In New Zealand, there are no known instances where the DPRK has been involved in real estate work, conveyancing, or work involving a commercial lease transaction.

SAR review

Approximately 800 SARs, where the reporting entity has referenced PF, have been submitted to the FIU – the majority by banks and relating to domestic firearms acquisition, which was mischaracterised as weapons proliferation.

Most SARs related to well-known New Zealand firearms dealerships; this demonstrates PF is not fully understood across the reporting community. However, some of the reporting provides insights into risk.

Examples of SARs

- An individual in New Zealand received $700k from three Asian countries. $140K was sent to third parties in three other countries including parties engaged in the development and manufacturing of key X-ray system components, thermal imaging products, and night vision systems. Over $500k was sent to a law firm in New Zealand.
- A company in New Zealand attempted to send funds (approx. USD $2k) to a sanctioned Chinese Defence Manufacturing company in Beijing, China. Although it transpired this reporting was not directly related to PF, this is the type of reporting that is encouraged given it could have related to PF.

Examples citing DPRK include

- A New Zealand romance scam victim who shared banking log-in details with a party in the DPRK.
- A young person who, when attempting to establish an account, stated they would receive transfers from the DPRK and was acting under direction of an unknown third party.
- An account holder attempted to deposit $30 NZD equivalent in North Korean won notes into personal account. He said he had been given the notes by a friend.
- A DPRK citizen deposited funds into his account through Smart ATMs. Their card was transacting overseas at the time of the deposits. Funds were withdrawn in Thailand at ATMs.
- A NZ charitable trust received donations that were transferred to an Australian charity that purchases medical supplies for hospitals in North Korea.
- A customer in a foreign country attempted to send funds to an individual in New Zealand but the sender's name was alerted on the sanction list – they had the same name as a legal representative of a DPRK foreign trade bank. Customer became nervous and halted transaction.
- A company received funds from a second-hand car parts dealer in Dubai known to sell to high-risk jurisdictions including the DPRK.

Examples citing Iran include

- Transfers of funds to a VASP in Iran.
- The most common theme related to bank accounts held by an Iranian national receiving multiple or large cash deposits. Receipt of funds was likely through a Hawala-type arrangement.[79]
- There were also a few SARs in which offshore entities (in particular, based in Malaysia) with a known connection to Iran sent funds to personal accounts of Iranian nationals in NZ.
- Interesting SARs included those where cash was deposited into the bank accounts of Iranian nationals and then used to buy jewellery – this included the use of a child's account to deposit cash and purchase jewellery.
- There were also Iranian nationals in NZ running a Hawala-type arrangement through their personal accounts – one was doing so with cryptocurrency.

Overseas experience – risks

Proliferation financiers can take advantage of jurisdictions with poor business formation and beneficial ownership transparency requirements.

In particular, proliferation financiers seek jurisdictions that do not collect beneficial ownership information during incorporation or foreign-entity registration, or when ownership changes. They seek these out to carry out illicit schemes anonymously through ostensibly legitimate legal entities.

The anonymity afforded to these legal entities inhibits law enforcement investigations into illicit activities and underscores the need for competent authorities to have timely access to adequate, accurate, and up-to-date beneficial ownership information.

[79] See MVTS, Chapter 3 (pages 38-40).

Other risks include

- Exploitation of the maritime sector to transport goods needed as inputs for proliferation programs and revenue-generating activity (including the trade of important global commodities like oil and coal).
- Malicious cyber activities and misuse of virtual assets, and cyber theft of virtual assets. Countries vulnerable are those where VASPs operated with strong AML/CFT regulation and supervision.
- Use of third parties including foreign nationals and companies, many of whom wittingly participate in these schemes or have compliance failures that allow exploitation by proliferation networks.
- Obscuring the end-user of purchases through mislabelling goods or consolidating and repackaging shipments for ultimate delivery to the DPRK.

Overseas example of list scanning limitations

A purchase of chemical equipment ended up in Syria. The description provided on the wire transfer simply said: “laboratory spare parts”.

Proliferators often order goods that are within controlled thresholds. This means there is a movement of goods that does not appear on export control lists but can still contribute to WMD programs.

It is questionable whether the information that financial institutions receive (through SWIFT or trade finance documentation) is sufficient to check against lists of controlled goods. Scanning generally returns a high number of false positives (up to 85%), resulting in considerable time and effort spent on clearing those false hits. In addition, concealment and deceit techniques of sanctioned/designated entities and individuals means list-scanning does not identify them. This is because they use shell companies and the names of associates or family members when undertaking financial activities. Finally, the lists contain names of known proliferators; as they are widely published, they are not useful for preventing new (or newly disguised) proliferators from accessing the financial system.

Beyond ‘list issues’, another recognised vulnerability is the uneven implementation of beneficial ownership controls internationally. European Union countries require collection of data and transparency when it comes to who owns companies and trusts. Some other major countries, including the United States, do not. Proliferators make extensive use of shell companies and get away with hiding behind non-transparent corporate structures.

VASPS CAN BE VULNERABLE

The DPRK targets cryptocurrency exchanges. In 2018, in one attack on a cryptocurrency exchange, North Korean hackers stole close to $250 USD million in cryptocurrency. North Korean agents launder cryptocurrency (mined, stolen, and received through ransomware) via a complex web of online transactions.

Risk findings

Risk of a potential breach or non-implementation of targeted financial sanctions (TFS):

Risk emerges when designated entities and individuals access financial services, funds and/or other assets in New Zealand. This can occur when reporting entities do not understand risk and then do not implement adequate policies and procedures to address proliferation financing risks.

For example, this can occur:

- through weak customer onboarding procedures
- in the absence of ongoing monitoring processes
- in the absence of staff training
- because of ineffective risk management procedures
- through a lack of implementing proper sanctions screening systems or irregular or inflexible screening procedures
- through a general lack of compliance culture.

There is current risk in TFS implementation as reporting entities are currently not required to do a risk assessment of how their services and products are exposed to PF risk.

In addition, the legal framework in New Zealand has limitations on capturing beneficial ownership information of legal arrangements such as trusts.[80] This poses a challenge to improve transparency of beneficial ownership information. Trusts can also be misused by proliferation financiers (in addition to being vulnerable to money laundering and terrorist financing).

Risk of evasion of targeted financial sanctions

Trade, raising funds and the establishment of legal persons for the purpose of PF can all be undertaken by third parties on behalf of Iran and the DPRK to support the evasion of the targeted sanctions. This presents challenge for all countries including New Zealand.

Evasion of targeted financial sanctions occurs when proliferation financiers and designated persons and entities circumvent them by using companies, structures or nominees. These disguise or conceal the purpose and intent of financial activities and the beneficial ownership of funds or assets moved or used. These same structures can be used to raise funds through scams, frauds and other schemes which generate income.

New Zealand is recognised as having a developed AML/CFT system. Recent high-profile cases relating to foreign-generated illicit wealth demonstrate a growing maturity. New Zealand is therefore not likely to be attractive for proliferators. New Zealand is not a country with widespread vulnerabilities; it is a relatively small economy, with an AML/CFT system that provides a degree of effectiveness.

Vulnerable sectors for PF are most likely those described in relation to TF and money laundering risk; this risk occurs through the requirement to transfer funds or goods out of New Zealand to enable PF. Legal persons and legal arrangements present risk due to transparency concerns with these arrangements; however overall, there has been limited identification of PF sanction breaches – so overall PF risk is considered low.

Key challenges for New Zealand

Reporting entities may be challenged in identifying transactions related to procurement, fundraising, and movement of money for illicit WMD programs.

These challenges occur because:

- reporting entities see limited information about the goods purchased or sold, for which payment is made; or
- the information provided in relation to payment could be incomplete, misleading or dishonest.

Our limited understanding of risk is recognised to negatively impact the implementation of targeted financial sanctions. However, this is mitigated somewhat by defensive SAR reporting. This SAR reporting will be improved through an enriched understanding of PF and associated risk.

[80] See Chapter 4: Risk Associated with Legal Persons and Legal Arrangements, pages 63-70.

NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

Te Kāwanatanga o Aotearoa
New Zealand Government

New Zealand National Risk Assessment 2024 *on*
Money Laundering, Terrorism Financing and Proliferation Financing

New Zealand Police Financial Intelligence Unit