NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

National Risk Assessment

OF MONEY LAUNDERING AND TERRORISM FINANCING

New Zealand Police Financial Intelligence Unit

2019

Contents

Foreword 3
Executive summary 4
Threat from predicate offences 10
Transnational threat 13
Terrorism financing threat 17
Sector risk assessments 25
Financial sector vulnerability 28
Gatekeeper professionals vulnerability 32
Cash economy vulnerability 39
Vulnerability to international threats 44
Risks and outlook 50
Glossary 54

Foreword

AML/CFT is about maintaining the integrity of our financial system to ensure New Zealand communities are free from the impacts of all forms of money laundering and terrorism financing. By denying criminals access to the financial system we also deny them opportunities to realise the financial benefits of their crime and engage in further offending. In doing so, we protect New Zealand from the corrupting effects money laundering and terrorism financing has on all elements of society.

This National Risk Assessment updates our understanding of risk, and has been undertaken in consultation with the public and private sectors. This revised understanding provides us a greater opportunity to respond and deploy in the most effective way to combat money laundering and terrorism financing. We understand that risk evolves and it is everyone's responsibility to be vigilant in the identification of emerging threats as this will help inform future assessments.

Organised crime is rapidly evolving and remains the primary driver of money laundering in New Zealand. Methamphetamine and other drugs, generate significant illicit proceeds for domestic crime groups who are aligned to complex transnational networks. In addition to drugs we recognise that fraud and other income generating crimes continue to occur across New Zealand, and that terror related crime is not something that New Zealand is immune from. Money is what drives these criminal behaviours and it is money that is the biggest vulnerability in terms of effective disruption and detection of these activities.

We want New Zealand to be the safest country and the hardest place in the world for criminals to do business. We also want to continue to improve our collective ability to detect, disrupt and prevent abuse of the New Zealand financial system. The AML/CFT framework of which there are many participants is critical in helping us keep New Zealand communities safe and secure.

Finally, thank you to all those individuals, agencies and reporting entities as you all contribute with enhancing New Zealand's resilience to money laundering, terrorism financing and associated offending.

Craig Hamilton
National Manager Financial Crime Group

Executive summary

Introduction

Money is the driving factor in a range of crimes including; drug distribution, fraud, theft, corruption, tax offending, human trafficking, cybercrime, and environmental crimes. Terrorists are also dependent on financial support. These crimes cause direct financial losses to individuals, community harm, and in some cases loss of human life. Successful money laundering allows criminals to enjoy profits and furthers the cycle of criminality by making funds available for reinvestment in crime. High profile money laundering and criminality cases also cause reputational damage, particularly on New Zealand's brand as a good place to do business.

Businesses operating in the financial, legal, property, and high value goods markets are at the frontline for countering illicit activity in New Zealand. Businesses that implement measures to prevent, disrupt and detect crime make a significant contribution to the global fight against crime, money laundering, weapons proliferation and terrorism. The Anti-Money-Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 envisages a cooperative relationship between the private sector and government agencies to effectively prevent and disrupt illicit use of New Zealand's financial system.

Law enforcement is the last line of defence against money laundering and terrorism financing. The New Zealand Police Financial Intelligence Unit (FIU) collects and analyses information from the financial sector and others to produce intelligence that supports investigations of money laundering, terrorism financing and the wide range of offences that generate criminal proceeds.

Cooperation between government and business is the key to success for the AML/CFT regime. Each party has different roles, knowledge and expertise. The FIU is dependent on high quality suspicious activity reporting (SAR)[1] from businesses. To deliver high quality reporting, businesses need to be confident they know the scale and nature of the criminality threats they face in their day to day operations.

AML/CFT Risk Assessment System

The AML/CFT regime in New Zealand has a three-tiered risk assessment system. The FIU's National Risk Assessment performs the function of describing the scale and nature of the criminality risks faced by New Zealand. In turn, the AML/CFT supervisors produce more detailed assessments of the risks faced by each sector. Information from those assessments is included throughout this National Risk Assessment.

In 2017, the supervisors completed a new suite of Sector Risk Assessments drawing on this document. These reports are summarised in the section titled Sector Risk Assessments. Finally, businesses produce their own assessment of the risks posed by their customers and the services provided to them. The expected outcome of the three-tiered approach is a well-informed, robust, and agile system for preventing and detecting money laundering and terrorism financing. This National Risk Assessment draws on information from reporting entities, Police and partner agencies and reflects a collaborative assessment of risk.

Description of Money Laundering and Terrorist Financing

Money laundering is the process by which criminals convert the proceeds of crime to realise and enjoy the financial benefits of their offending. While there are many methods to undertake money

[1] Under the Anti-Money Laundering and Countering Financing of Terrorism (Requirements and Compliance) Amendment Regulations 2017, suspicious activity reports (SAR) replaced suspicious transaction reports (STR). The term SAR is used throughout this document to refer to both STRs and SARs.

laundering, the core principle from a risk perspective is the criminal abuse of vulnerabilities within the financial, legal and property systems.

Money laundering is commonly described as having three stages:

- **Placement:** Introducing illegal funds into the formal financial and business system (for example depositing cash from drug sales into accounts, co-mingling it with business takings or using it to purchase assets);
- **Layering:** Moving, dispersing, or disguising illegal funds or assets to conceal their true origin (for example using a network of complex transactions involving multiple banks or accounts, or companies and trusts); and
- **Integration:** Investing the disguised funds or assets in further criminal activity or legitimate business, or enjoyed as high-value property assets and luxury goods. At this stage, the funds or assets appear to have been legitimately acquired.

Terrorism financing is the process by which terrorists and sympathisers raise and move funds to conduct terrorist acts and operations. There is a distinction between money laundering and terrorism financing in that terrorism financing may seek to move money from the legitimate economy to use it for a criminal act, while money laundering seeks to move proceeds from a criminal act to the legitimate economy. Nonetheless, many of the methods and financial channels used are the same. Like money laundering, terrorism financing is generally described as having three stages:

- **Raising funds:** Terrorism financiers raise funds through legitimate earnings, donations and/or criminal offending;
- **Transferring funds:** Once raised, funds for terrorist causes need to be moved to the place where they will be used, which often requires funds to be moved internationally. This can be done by physically couriering cash or high value commodities, moving funds through the international financial system, or alternative mechanisms for moving value; and
- **Using funds:** Terrorist groups need to use the funds either to commit terrorist acts or to fund ongoing operations. Any use of the funds by a terrorist group to support the organisation and its cause is terrorism financing.

The role of a national risk assessment

This is a public version of New Zealand's Money Laundering and Terrorism Financing National Risk Assessment. Understanding risk is a key component to building an effective national response to money laundering and terrorism financing, and is a cornerstone of the Financial Action Task Force (FATF) risk-based approach concept[2].

This 2019 edition of the National Risk Assessment comprehensively sets out the current understanding of the national-level risks of illicit financing. Sector risk assessments have also been produced by the three AML/CFT supervisors (the Department of Internal Affairs (DIA), the Financial Markets Authority (FMA) and the Reserve Bank of New Zealand (RBNZ)).

This National Risk Assessment uses a model based on international guidance[3], where risk is a function of threats, vulnerabilities and consequences. Discrete assessments of New Zealand's principle threats and vulnerabilities within money laundering channels are set out in individual

[2] For information on the FATF Risk-Based Approach, see the FATF website at: http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc(fatf_releasedate)
[3] FATF guidance "National Money Laundering and Terrorism financing Risk Assessment", February 2013

sections, while consequences, or the potential impact on law enforcement work and international reputation are considered throughout.

Terrorism financing threat, vulnerability and consequences

The threat of terrorism in New Zealand is lower than many of our partner countries. Consequently, there have been no prosecutions or convictions for terrorism financing in New Zealand.

However, New Zealand's reputation for perceived low-corruption and high integrity, while being enviable, is also a vulnerability. Given the level of international scrutiny on terrorism financing, overseas terrorism financers may seek to abuse New Zealand structures using similar methods as international money launderers.

There are severe global impacts and potential loss of life associated with terrorism. The consequences for New Zealand's reputation are considerable should overseas terrorist groups:

- use New Zealand's businesses, companies, payment platforms and charities to support terrorism financing, or
- find local supporters to assist in terrorism financing.

Despite the comparably low threat, given the high consequence of terrorism financing globally, New Zealand takes its contributing role in preventing misuse of financial services and professional services very seriously.

Financing of terrorism within New Zealand

Funding for terrorist activity within New Zealand is most likely to relate to lone actors or small cells, using simple methods of organisation with corresponding small-scale and simple funding arrangements. Regardless, in some circumstances these threats can have capability for complex, coordinated and high impact attacks. The global experience of lone actor and small cell attacks have tended towards self-financing through legitimate means such as wages, government benefits, loans, credit cards and business takings. In other jurisdictions, such actors have also used criminal offending to self-fund activity or received small payments from domestic/global networks.

Money laundering threats in New Zealand

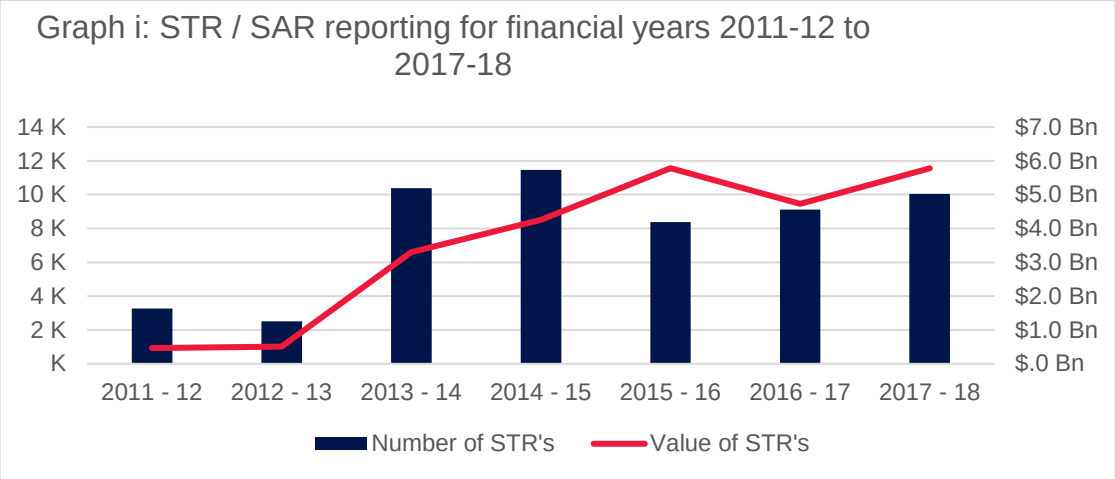
Proceeds of crime generated both domestically and internationally pose money laundering threats to New Zealand's financial, legal, property and retail sectors.

Domestic money laundering threat	The major groups of crimes which are predicates to money laundering domestically are drug offending, and to a lesser extent, fraud offending and tax offending. The FIU estimates NZD 1.35 billion is generated annually for laundering. This figure excludes transnational laundering of overseas proceeds and laundering the proceeds of domestic tax offending. The transactional value of money laundering is likely to be significantly more than this figure since money laundering involves placing, layering and integrating funds in different investments to cleanse the proceeds.
Offshore money laundering threat	New Zealand faces an unknown scale of money laundering generated from overseas proceeds of crime. The International Monetary Fund (IMF) estimates that approximately 2-5 % of global GDP (approximately USD 2 trillion) is proceeds of crime. Three key areas of known threat from offshore to New Zealand are in: • transnational organised crime groups linked to New Zealand, such as transnational drug distribution networks, • overseas criminal organisations not generally connected to New Zealand who may seek to move funds through New Zealand and/or New Zealand's legal structures, and

	• Money laundering networks which may also seek to move funds through New Zealand's financial system or New Zealand legal structures.

Improvements in law enforcement effort and measures for anti-money laundering

In 2013, more robust AML/CFT measures applied to financial institutions and casinos (as Phase I of the AML/CFT Act reforms). When the AML/CFT Act came into force on 30 June 2013, almost all financial institutions ceased to be reporting entities for the purposes of the Financial Transaction Reporting Act (FTRA) 1996 instead becoming reporting entities for the purposes of the AML/CFT Act. The implementation of the AML/CFT Act significantly increased financial institutions' capability to resist and detect money laundering and terrorism financing. As shown in the graph below, this has resulted in an increase in reporting to the FIU, both in terms of the number of reports and the value of reported transactions.

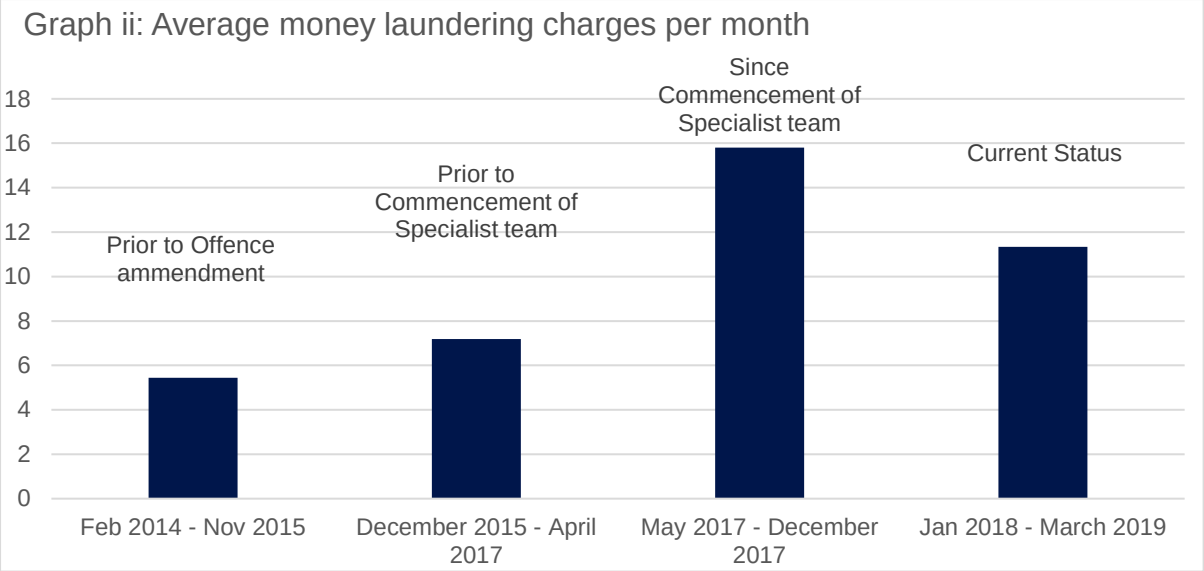


The Organised Crime and Anti-Corruption Legislation Bill received Royal Assent in November 2015. The Bill led to 15 amendment acts, most of which are already in effect. There were three AML/CFT-related amendments:

- The money laundering offence in the Crimes Act 1961 now specifies that intention to conceal is not a requirement of the offence. This will now comply with international obligations from the FATF and the United Nations Convention against Transnational Organised Crime.
- Removal of the minimum five-year imprisonment threshold from the crimes predicating the money laundering offence.
- Reporting entities are now required to report on all international wire transfers at or over NZD 1,000 and all physical cash transactions at or over NZD 10,000 to the FIU since 1 November 2017.

In April 2017 Police established dedicated Money Laundering Investigations Teams comprised of detectives and specialist employees who work closely with organised crime and asset recovery investigators to target the criminal act of money laundering.

Since these legislative changes and the launch of the Money Laundering Investigations Team, the number of money laundering charges has significantly increased as shown in the graph below.



Improvements in counter-terrorism activity

The New Zealand intelligence, diplomatic and law enforcement community is also building its counter-terrorism capability, including improved terrorism financing prevention and detection systems, asset freezing and sanctioning.

Commencement of sector supervision

Active supervision of AML/CFT is also a key component of effective implementation of AML/CFT measures. The AML/CFT Act supervisory regime started on 30 June 2013. The supervisors are:

- The Reserve Bank of New Zealand for banks, life insurers and non-bank deposit takers,
- The Financial Markets Authority for issuers of securities, licensed supervisors, derivatives issuers and dealers, fund managers, brokers and custodians, financial advisers, equity crowdfunding platforms and peer-to-peer lending providers, and
- The Department of Internal Affairs for casinos, non-deposit taking lenders, moneychangers, and other reporting entities not elsewhere supervised.

The Anti-Money Laundering and Countering Financing of Terrorism Amendment Act 2017 extended obligations to lawyers, accountants, conveyancing practitioners, real estate agents, and the Racing Industry Transition Agency [4] as well as obliging cash transaction reporting for businesses dealing in high value goods (e.g. auctioneers, bullion dealers). These obligations have come into force by a staggered implementation between 2018 and 2019. DIA is also the supervisor for the Phase II reporting entities. Phase II will continue to mitigate existing vulnerabilities in the professional services sector and will better align New Zealand with international standards.

Summary of remaining vulnerabilities to money laundering in New Zealand

The channels that currently offer opportunities to money launderers in New Zealand are those financial, legal, accounting, real estate, and retail or dealer services that:

- offer anonymity to the offenders,
- are available for moving large values and volumes of legitimate funds and which provide a screen for illicit transactions,

[4] Formerly the New Zealand Racing Board.

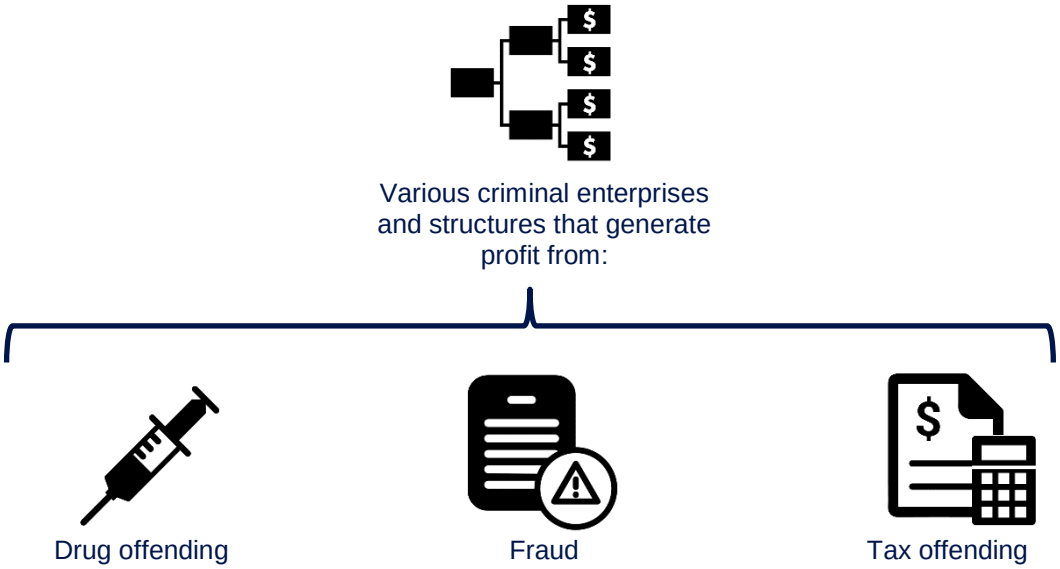
- are widely available internationally and also have poor AML/CFT controls internationally, and/or
- are cash intensive, which are particularly used to disguise drugs proceeds.

The highest priority observed vulnerabilities for New Zealand are:

International wire transfers	International wire transfers, which were assessed by the FIU in 2010 as the highest risk. The AML/CFT Act now subjects international wire transfers to greater AML/CFT controls, which has significantly mitigated the systemic vulnerabilities identified in 2010. Despite this, the scale of money moving through these channels continues to present opportunities to money launderers. The introduction of Prescribed Transaction Reporting in November 2017 has assisted in addressing this vulnerability.
Alternative payment methods	This assessment has found that alternative remittance systems, international trade-based transfers, and alternative banking platforms have each emerged as vulnerabilities to money laundering. These areas are vulnerable to domestic and international criminal proceeds and are closely associated with third party money laundering networks.
New technology	New Zealand's vulnerability to misuse of new technology is closely related to alternative methods of moving value and funds. New Zealand's exposure to high profile new payment technologies, including virtual assets, may not be as high as other countries due to lower uptake of high-risk services and high levels of scrutiny from the traditional financial sector. Nonetheless, the rapid development of payment technology creates a highly dynamic environment in which vulnerabilities may emerge quickly and create new alternative methods for moving value. In particular, risks relating to transnational money laundering are exacerbated by online alternative banking platforms nominally domiciled in New Zealand.
Gatekeeper professional services including formation of companies, trusts and charities	Historically there were low levels of AML/CFT controls within gatekeeper professional services which has allowed the emergence of transnational professional money laundering facilitators and complex networks. These vulnerabilities are compounded by difficulties in identifying the beneficial owners of New Zealand companies, charities and trusts. These services are also vulnerable to domestic laundering, opening money laundering channels in which professional gatekeepers may facilitate criminal transactions such as in the real estate sector. The AML/CFT regime has now been expanded to include gatekeeper professional services and this is expected to mitigate these risks.
Cash	Cash remains the dominant means of transacting for domestic drug crimes. Dealers in high value goods remain vulnerable to abuse to place cash proceeds as does casino gambling. The detection rates for illicit cash in the high value goods sector are expected to improve now that the AML/CFT regime has been expanded to include high value dealers.
Businesses	Many business industries are vulnerable to use as fronts for money laundering. In particular, cash intensive businesses are a common method of establishing an ostensive origin of cash proceeds. This type of laundering can have anti-competitive effects with negative consequence for legitimate competitors.
High value goods	Non-financial assets are also abused at all stages of money laundering. In particular, high value transportable goods can be used to store wealth or to move value between criminals. Similarly real estate assets are vulnerable to abuse in large money laundering transactions.

Threat from predicate offences

Figure i: Predicate offending threats profile:



A predicate offence is the underlying offence that generates proceeds of crime for money laundering. Some countries take a legislative approach of listing predicate offences for money laundering. The FATF standard is for all serious offences to be included as predicate offences, with a view to including the widest possible range of offences.

As such, any offence that generates any financial profit may in theory be a predicate to money laundering in New Zealand. However, low value proceeds of crime generated by many forms of offending are likely to be immediately consumed in the legitimate or criminal economy. There may be some theoretical form of money laundering in the conversion of the proceeds through consumption. However, criminals generating low values of proceeds of crime have little need to hide the criminal origin of their funds rendering them a nominal money laundering threat. In the great majority of tax evasion cases, there is little or no effort made to launder funds, rather they are simply applied to daily running costs of a business or personal expenditure.

Scale of domestic laundering

The analysis of threat used two methods adapted from research by Australian academic John Walker to generate an estimate of the scale of illicit proceeds for laundering. Using these methods, the FIU estimates that NZD 1.35 billion of domestic criminal proceeds is generated for laundering in New Zealand per annum from drug offending (NZD 750 million), fraud (NZD 500 million) and other offences such as burglary (NZD 100 million) [5]. These estimates exclude tax offending and overseas predicate offences. The estimates correlate fairly closely to the 2010 estimate of NZD 1.5 billion extrapolated from the Australian estimate and the 2009 mutual evaluation estimate of over NZD 1 billion. Given the nature of generating these estimates, these figures give only an approximate indication of the scale of money laundering, and are not precise enough to compare to previous estimates to indicate any change in laundering over time.

[5] John Walker "The Extent of Money Laundering in and through Australia in 2004", RMIT University and AUSTRAC, 2005. These are indicative figures only.

The actual transactional value of money laundering is likely to be several times the NZD 1.35 billion estimate of money generated for laundering, as launderers need to move funds through multiple transactions to place, layer and integrate proceeds of crime.

Main predicate offence types

Previous estimates and cases analysed as part of this risk assessment have identified three main domestic predicate offence types in New Zealand; drug offending, and to a lesser extent, fraud offending and tax offending. The analysis drew on crime statistics and reported cases from New Zealand Police Asset Recovery Units (ARU) involving restraint of assets worth more than NZD 1 million, to generate understanding of the risk associated with each of these crime types. Analysis identified seventy-two cases. Of these, the ARUs held sufficient information for analysis on 57 cases involving assets worth NZD 165 million (half of the total value of assets restrained at that time).

An organised crime structure and/or networked offending are common in predicate offending cases, but there is not a universal model. The business structures that are used to generate illicit profits take many forms, in much the same way as legitimate businesses do. The unifying principle is that offending is undertaken as a for-profit business enterprise.

In general, the main characteristics associated with the proceeds of crime by these offence types are:

Drug offending	
	This predicate offence generates large amounts of illicit cash, predominantly a cash business model with payments made at various stages, including manufacture, transportation and sales. Drug networks potentially generate a higher value of proceeds than other offences investigated by Police and involve a large number of offenders.
Fraud	
	Laundering activities are conducted to hide the proceeds of crime generated by the full spectrum of fraud offending. In the majority of cases, funds are generated in the legitimate financial sector before being laundered using financial and professional service providers.
Tax offending	
	The abuse of the tax system through intentional and dishonest behaviours generates a large amount of illicit funds. These funds, largely retained within the legitimate financial sector, are typically self-laundered or laundered using professional service providers. Money laundering is most likely to occur inherently in the way taxes are evaded rather than requiring a discrete action.

The table below details the profile of money laundering by each of the major predicate offence types identified through the cases analysed in this assessment.

Table i: Money laundering profiles by predicate offence threat

Threat	Method	Phase	Description
Drug offending	Self-laundering Money laundering by close associates ("smurfing" etc.) Money laundering through professional services and high value dealers Possible access to international money laundering networks	Predicate offending	Cash-based
		Placement	Cash deposits, cash purchase of property and high value commodities, cash remittance, co-mingling with business earnings
		Layering	Domestic transactions, may remit funds internationally, may use trusts, may use professional services – particularly in higher value cases
		Integration	Real estate, high value commodities
Fraud	Self-laundering; Laundering by professional service providers	Predicate offending	Non-cash based
		Placement	Likely to occur through electronic transactions, potentially involving the entity used to commit predicate offence (i.e. in business, company or market)
		Layering	Use of companies and business, likely to be professionally facilitated;
		Integration	Real estate, high value commodities
Tax offending	Self-laundering; Laundering by professional service providers	Predicate offending	Cash and non-cash based
		Placement	Likely to occur through cash deposits/purchases and also through electronic transactions, potentially in the vehicle used to commit predicate offence (i.e. in business, company or market)
		Layering	Use of nominees, trusts, family members or other third parties. Movement of funds offshore through networks set up by professional facilitators.
		Integration	Reinvestment in professional businesses; real estate, high value commodities

Transnational threat

Figure ii: Transnational threat profile:

Overview

Despite successive studies, reliable information relating to the scale of international money laundering is limited. The most commonly cited estimate of global money laundering is the estimate by the IMF of 2-5% of global GDP. The confidence of this estimate is very low, but it does serve to provide an indication of the scale of international money laundering and the global illicit economy that New Zealand is exposed to. Based on this estimate, approximately USD 2 trillion, or around ten times New Zealand's GDP, could be expected to be generated for laundering globally per annum.

This section considers the capability and intent of external money laundering threats to impact New Zealand. The section below on international exposure considers New Zealand's vulnerability to these threats as well as to external terrorism financiers and movement of domestic proceeds offshore.

Several external transnational money laundering threats to New Zealand exist. Given the limited reliable information on the scale of international illicit capital flows these are difficult to quantify. Nonetheless, the FIU has observed significant threat associated with the three transnational threats described in the table overleaf.

Organised crime connected to New Zealand networks	
	Organised crime connected to New Zealand networks may seek to move illicit proceeds to and from New Zealand to facilitate offending. Transnational laundering of this sort is closely associated with domestic drug markets, such as overseas based networks entering the New Zealand market with the intention of repatriating illicit profits. This activity drives domestic offending and harm to New Zealand communities by developing the criminal enterprise's links and influence in New Zealand.
Illicit funds associated with overseas criminals with no connection to New Zealand	
	Illicit funds associated with overseas criminals with no connection to New Zealand also create a threat by moving through the global financial system. Any type of overseas criminal may attempt to use jurisdictions with reputations of high integrity and stability to facilitate money laundering or terrorist financing. This transnational threat environment exposes countries with lower domestic threats, such as New Zealand, to new crime types, such as corruption, and sophisticated laundering techniques.
International criminal networks specialising in money laundering services	
	Criminal networks specialising in money laundering services to predicate criminals have been identified by FATF and other law enforcement agencies overseas as a growing concern. These networks give transnational criminals direct access to the international monetary system and sophisticated money laundering techniques. Money laundering networks active in the international system make use of alternative remittance and trade-based money laundering networks. This activity involves complex resilient networks facilitated by the abuse of legal arrangements and modern communications technology.

International requests to the FIU

The nature and number of international requests to the FIU offer some insight to the types of transnational threats posed to New Zealand. Analysis of those requests indicated that in the majority of cases the link to New Zealand was more likely to relate to use of New Zealand legal structures as shell companies, or in a few cases to facilitate offending through alternative banking platforms[6], rather than a substantive link to the New Zealand financial system.

In particular, where the requesting jurisdiction is remote from New Zealand, most requests relate to economic crimes facilitated by corporate structures. In these requests, money laundering, corruption and fraud are the most commonly identified offences. However, requests remain varied where the requesting country is closer to New Zealand, or has strong traditional cultural/economic ties. In addition to financial crimes and corporate structures, such countries may also request information relating to drug and organised criminality facilitated by abuse of New Zealand bank accounts, legal structures or alternative remittance[7].

[6] Alternative banking platform are systems that provide the functionality of a bank outside the traditional global banking system; and are particularly associated with web-based services outside the regulated sector. Alternative banking platforms are also known as payment platforms or virtual banks.

[7] Alternative remittance, also known as underground banking or informal funds transfer systems, is a distinct concept from alternative banking platforms. These are money service businesses that facilitate movement of funds outside of the formal banking system; often through alternative networks traditional to a national or regional group (such as hawala or fei ch'ien) and are often cash intensive.

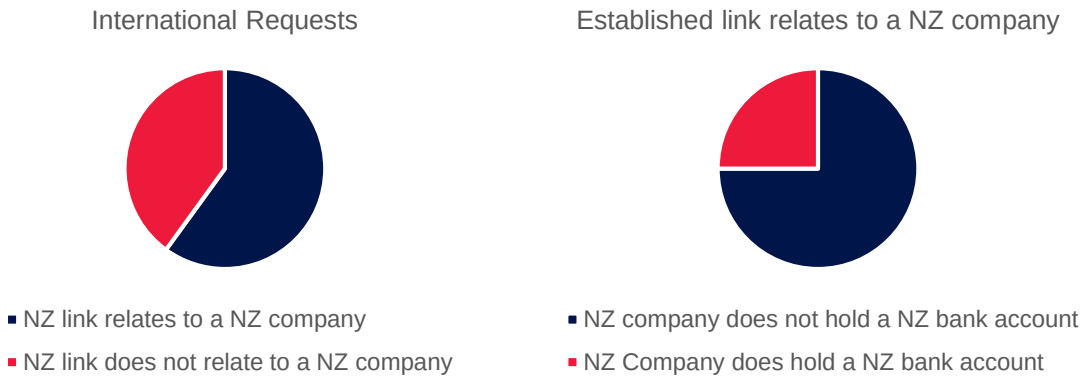
Methods associated with known threats

Use of New Zealand legal structures

Overseas criminals who seek to abuse New Zealand legal structures are a known money laundering threat. Typically, a New Zealand entity (such as a company, limited partnership or trust) is used within a complex network of companies and trusts from other jurisdictions as a vehicle for money laundering without any transactions occurring in New Zealand.

Overseas partners report money laundering facilitated by New Zealand shell companies largely originates overseas - flowing through bank accounts most commonly in Europe or offshore jurisdictions. In a sample of international requests to the FIU, 60% of requests where a link to New Zealand was established related to a New Zealand company. In 75% of those cases no New Zealand bank accounts were identified.

Graph iii: International requests to the FIU relating to New Zealand companies



New Zealand trusts have been less common in requests to the FIU. Nonetheless, there have been some instances, which have confirmed that arrangements such as trusts have the same vulnerabilities to transnational money laundering as companies.

Similarly, the New Zealand FIU has received information from overseas partners regarding offending relating to the abuse of New Zealand alternative trading and banking platforms with no substantive link to New Zealand. Such platforms have been associated with the facilitation of money laundering and predicate offending relating to ponzi, and investment frauds.

Use of New Zealand financial system as a conduit

In the instances where a New Zealand financial institution account was identified, the account was typically associated with a company or business. This indicates that overseas offenders prefer to use New Zealand company accounts rather than personal accounts when moving money through New Zealand.

Domestic intelligence also indicates that overseas-based criminals exploiting New Zealand shell companies, often operated by a New Zealand trust and company service provider (TCSP), have used New Zealand bank accounts.

Use of New Zealand trade as a conduit

Trade-based activities are a key facilitator for transnational money laundering. International movement of large values of illicit capital from many jurisdictions has a strong association with trade-based money laundering. This process threatens to enable the movement of proceeds from

corruption, tax offending and other financial crime to high integrity jurisdictions such as New Zealand. However, confirmed indications of trade-based money laundering are limited. The transnational threat environment similarly exposes countries with lower domestic threats to high threat crimes types and money laundering techniques.

Use of New Zealand Real Estate

Although transnational laundering through real estate has received a high degree of media interest in New Zealand, this typology has not been common in international requests to the FIU. Significant transnational money laundering has been identified in real estate markets in similar countries to New Zealand, such as Australia, the UK and the US. Given the similarities of the New Zealand real estate market to these countries' markets, it is possible that launderers active in the international market may be similarly attracted to New Zealand. Where cases of misuse of New Zealand real estate by overseas criminals has occurred, these have included offending involving high values of proceeds creating a significant money laundering threat.

Recent amendments to the Overseas Investment Act 2005 appear to have significantly reduced the proportion of residential properties being sold to overseas buyers, with property transfers to non-New Zealand citizens (or residents) dropping by 81% in the March 2019 quarter compared with the same quarter the previous year.[8] These controls are expected to significantly mitigate the risk of transnational laundering through New Zealand real estate.

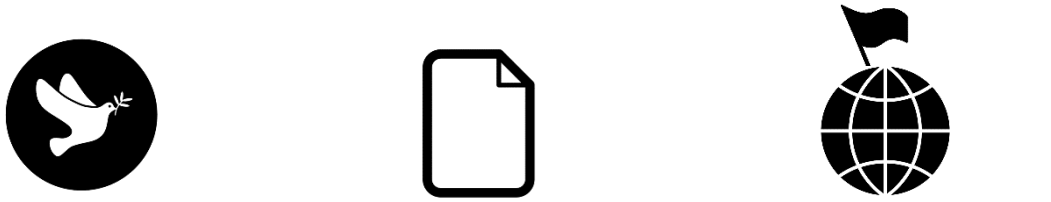
Table ii: Methods associated with various transnational threats

Threats	Description of likely methods
Drug offending connected to NZ	Remittance and alternative remittance; movement of funds through financial institution, designated non-financial businesses and professions (DNFBPs), businesses and assets. Trade-based laundering through merchandise trade.
Corruption and other economic crime	Trade-based laundering, remittance and alternative remittance, attempts to seek safe haven (either in person as fugitives or to store proceeds while maintaining control from offshore)
Organised criminal groups with trans-Tasman connections	Remittance and alternative remittance; movement of funds through financial institution, DNFBPs, businesses and assets. Trade-based laundering through merchandise trade.
Tax evaders and other economic criminals	Trade-based laundering using trade in services and legal structures.
Organised crime and economic criminals with no link to NZ	Use of legal structures and alternative payment platforms
International controllers	Remittance and alternative remittance, trade-based laundering
Economic criminals	Abuse of legal structures, movement of funds through financial institution, DNFBPs, businesses and assets, attempts to seek safe haven (either in person as fugitives or to store proceeds while maintaining control from offshore)

[8] During the first quarter of 2019, property purchases by overseas persons amounted to 0.6% of all property transfers; which is a significant drop from the same quarter the previous year when property sales to overseas persons amounted to approximately 3.3% of all property transactions – refer https://www.interest.co.nz/property/99475/stats-nz-says-number-residential-properties-sold-overseas-buyers-plummeted-march

Terrorism financing threat

Figure iii: Terrorism financing threat profile:



Terrorism financing is the process by which terrorists fund either terrorist acts or ongoing operations to perform terrorist acts. Terrorists need financial support to carry out their activities and to achieve their goals. While money laundering is the process of concealing the illicit origin of proceeds of crimes, terrorism financing is the collection or the provision of funds for terrorist purposes. In the case of money laundering, the funds are always of illicit origin, whereas in the case of terrorism financing, funds can stem from both legal and illicit sources. The primary goal of individuals or entities involved in the financing of terrorism is, therefore, not necessarily to conceal the sources of the money but to conceal the nature of the funded activity.

New Zealand has not historically experienced the level of terrorist activity that has affected many partner countries, and support for terrorist causes is comparably low. However, like any country, New Zealand remains exposed to terrorism financing. Even small-scale financing within New Zealand could have significant impact.

Overseas-based groups may seek to exploit New Zealand as a source or conduit for funds to capitalise on New Zealand's reputation as being low risk for terrorism funding. This vulnerability is expected to increase as New Zealand's economy is increasingly integrated into the global economy. The value of funds moved through the international system in connection with terrorism financing is likely to be much lower than other forms of illicit capital flows. However, should funds connected to terrorism financing move through New Zealand it would be likely to have a disproportionate effect on New Zealand's reputation, international relations and security.

Financing of terrorism in New Zealand

Financing of terrorism within New Zealand is likely to be small scale and involve low value of funds. Similar jurisdictions to New Zealand have experienced a trend towards small cells or lone actor terrorists who self-fund attacks or the preparation for attacks which do not eventuate in an attack. Such terrorists may also receive low values of funds from offshore terrorist networks. Although either financing scenario would be unlikely to involve large values of funding, the potential consequences are significant.

Two types of offshore group pose a financing threat to New Zealand; groups able to attract support with ideology and well-resourced groups with established networks. These groups pose two specific terrorism financing risks to New Zealand: that radicalised individuals will support overseas groups, and that terrorism financing networks will abuse New Zealand's vulnerabilities to transnational laundering.

Although New Zealand's limited experience may make specific actions to target the terrorism financing threat difficult, AML/CFT controls to counter transnational laundering, combined with

other activities to counter the threat of radicalisation, are likely to mitigate the deficiencies of specific counter measures for terrorism financing, provided these measures are flexible enough to counter both threats.

Table iii: Types of terrorism financing threat

Domestic Terrorism	
Given the low level of domestic support for terrorist causes and absence of terrorist networks, it is more likely financiers of domestic terrorism would manifest in New Zealand as isolated disaffected individuals or small groups. Small cells and lone actors are most likely to be self-financing and/or may receive financial support from close associates. It is also possible small payments may be received from overseas networks which terrorists are connected to or directed by using internet-enabled communications.	
Value per TF event	**Likely small or negligible**
Raise	Self-funding: - legitimate earnings - selling assets - Crime
Move	Funds transfers through banks Money value transfer systems Cash Financial activity through high-risk jurisdictions Stored value cards Use of nominees
Use	Vehicle rental Firearms purchases Chemical or other bomb components Travel Donations to extremist causes
Groups able to inspire support through ideology	
The threat of radicalised individuals inspired by terrorist groups is currently most notably manifested in religious extremism espoused by groups such as Da'esh or Al-Qaeda. However, it has also been associated with nationalist, far right or other political causes which may resonate in particular communities. Individuals may be inspired to contribute to overseas terrorist groups by travelling to conflict zones, which requires self or third party funding. Radicalised individuals may also choose to contribute to terrorism by raising and contributing funds using the common methods discussed below. Given the low level of domestic support for terrorist causes, it is more likely this threat would manifest in New Zealand as isolated disaffected individuals or small groups. This threat is also more likely to manifest using internet-enabled communications allowing such isolated individuals to communicate with other likeminded individuals and overseas terrorist networks.	
Value per TF event	**Likely small or negligible – potentially moderate**
Raise	Funding third parties overseas: - own legitimate earnings - donations - fraud From overseas: - kidnapping for ransom overseas - soliciting support - defrauding New Zealanders

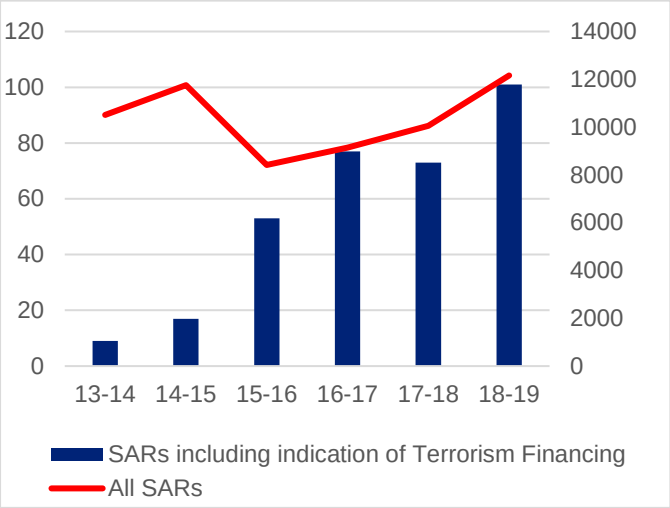
	- control/influence of territory
Move	Funds transfers through banks Money value transfer systems Cash Financial activity through high-risk jurisdictions Abuse of New Zealand structures Non-profit organisations or other donations
Use	Travel to conflict or other high-risk jurisdictions Overseas terrorist activity (attacks or logistical)
Well resourced groups with established networks	
Abuse of New Zealand's vulnerabilities to transnational laundering by terrorism financing networks may involve movement of large sums of funding for terrorism. State-sponsored groups or groups operating with state-like infrastructure are more likely to have access to such networks. This may occur through abuse of legal persons, alternative banking platforms, or New Zealand address services without transactions moving through New Zealand.	
Value per TF event	**Potentially large – especially when using legal persons outside of New Zealand's financial system**
Raise	From overseas: - state sponsorship - fraud or other criminal networks - control/influence of territory
Move	Funds transfers through banks Financial activity through high-risk jurisdictions Abuse of New Zealand structures Non-profit organisations or other donations
Use	Terrorist activity overseas (attacks or logistical)

Suspicious Activity Reporting (SAR) on terrorism financing

For the period from the commencement of the AML/CFT Act on 30 June 2013 to 30 June 2019 the FIU received a total of 330 SARs that had an indication of a possible relation to terrorism financing, which is 0.46% of all processed SARs for the period.

The total number for each financial year includes suspicious activity reports that were assessed by reporting entities as relating to possible terrorism financing, as well as those suspicious activity reports assessed by the FIU as relating to possible terrorism financing to date.

Graph iv: SARs indicating terrorism financing (by financial year)



The SAR statistics suggest there has been an increase in SARs related to possible terrorism financing. This increase is a reflection of the recent acts of terrorism around the world, which have increased awareness and alertness of terrorism generally, as well as the FIU's targeted training and guidance provided to the New Zealand financial institutions on indicators of terrorism financing. The slight decrease in 2017-18 correlates with the decline in territorial control by Da'esh in Iraq and Syria.

The marked increase in 2018-19 can be attributed to the heightened awareness and vigilance on the part of reporting entities and the FIU following the Christchurch terrorist attacks in March 2019. This underlying increased awareness should not in itself be read as a change of the terrorism financing threat.

Traditional terrorism financing methods and techniques

FATF and members of its global network have undertaken focused research on terrorism financing methods and risks[9] to demonstrate the sources of income for terrorist organisations and the range of methods used to move funds. This research demonstrated the range of ways terrorist organisations raise funds through legitimate activities as well as inherently criminal means. The relatively small value of funds that may be involved and the often legitimate origin of terrorism financing can make it difficult to detect.

Income generation

Legitimate earnings

Relatively small amounts of funds may be involved in terrorism financing, which terrorists and/or sympathisers may simply divert from legitimate income. In particular, lone actors, small cells and foreign terrorist fighters are noted to use legitimate wages, salary or other personal income to fund travel and supplies.

Legitimate business earnings are another source for terrorism financing. FATF reported that overseas law enforcement and prosecutors had noted a nexus between terrorism financing, and car dealerships and restaurants. Such businesses may allow for under-reporting of earnings, especially if they are cash intensive, providing an opportunity to divert a portion of funds to terrorism. FATF also reported that shipments of cars to the Middle East and other forms of abuse of trade had been used by some terrorist organisations[10].

Donations

Donations from supporters and the diversion of charitable donations are well known methods of terrorism financing. An analysis of terrorist financing-related law enforcement cases in the US since 2001 found that approximately 33% of these cases involved direct financial support from individuals to terrorist networks[11].

Once donations are raised, a network of facilitators will typically funnel donations to terrorist organisations through small transfers at money transfer shops or by using cash couriers who take the funds across borders. Donations to legitimate charities may also be diverted wholly or in part by terrorist sympathisers if the charity's supply chain is not protected from infiltration. In theory this could occur at any point from the collection of donations until the end use of funds.

In New Zealand, a very small number of disaffected individuals may choose to donate to a terrorist cause. It is also possible that donations raised in New Zealand for legitimate causes will be diverted, particularly where the funds are sent to conflict zones or jurisdictions with high corruption where it may be difficult for the charity to maintain end-to-end oversight of the funds. However, the Charities Service works closely with the sector so that charities exposed to such risks are able to mitigate them.

[9] FATF "Emerging Terrorist Financing Risks", FATF October 2015.
[10] Ibid.
[11] US Department of Treasury, United States National Terrorist financing risk assessment, US Department of Treasury 2015 www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdF

Fraud

Terrorism financing may also be raised through criminal offending. In other jurisdictions, various forms of fraud have been associated with terrorism financing. For example, FATF reporting notes the use of insurance frauds, such as simulation of traffic accidents, to fund terrorism[12]. Foreign terrorist fighters and other terrorists have also used loan fraud to fund terrorist activity[13]. Both fraud types are known in New Zealand, although no incidences of the proceeds being used for terrorism financing are known to the FIU.

Kidnapping for ransom

Kidnapping for ransom is a growing source of revenue for terrorist groups, including Da'esh. It may be particularly relevant for New Zealand as a kidnapping can occur in one jurisdiction and the ransom payment be made in another. Cash often plays a significant role in kidnapping for ransom. Following the delivery of a ransom payment in physical cash, cash couriers move the cash to the terrorist group. Ransom payments can also be paid through financial institutions, such as banks, exchange houses, insurance companies, lawyers, or alternative remittance systems such as hawalas.

State-sponsorship

States may choose to sponsor a terrorist group to further their own political goals, including undermining rivals. State sponsors may provide terrorists with funding, material support (such as weapons and equipment), logistical support and training. The resources that the state-sponsor can access may provide state-sponsored groups with a relatively high level of financing.

As with other forms of terrorism financing, state-sponsored groups and their patrons need to mask the purpose of the financing where funds move through the international financial system. This creates a threat to New Zealand as such groups and their sponsors may seek to use New Zealand's financial sector or legal persons to mask their involvement in the financial activity.

Control or influence over territory

When terrorist groups grow strong enough to gain territorial control or exert influence over areas with poor state control, they may be able to extract revenue from that territory. Reporting has indicated that extortion and illegitimate taxation has been a major revenue stream for Da'esh. As well as the local population, groups may extort international businesses or smugglers and other transnational criminals operating in or transiting, the group's zone of influence. Territorial control or influence also provides groups access to commodities for black market trade, such as illicit oil trading and drug trafficking, further blurring the line between terrorism financing and money laundering.

Movement of funds

Funds transfers through banks

Funds transfers through banks continue to be the most common way to move money for any purpose including terrorism financing. The banking sector remains vulnerable to terrorist financing given the difficulty in spotting the small number and value of terrorism financing transactions in the multitude of everyday banking transactions. Several FATF reports have referred specially to the use of the bank accounts of non-profit organisations (NPOs) to move funds to terrorist organisations[14].

Terrorism financing through the banking sector is often small-scale and can be difficult to distinguish from the large number of legitimate daily transactions. Australia has reported that cases

[12] FATF "Emerging Terrorist Financing Risks".
[13] Ibid.
[14] Ibid.

have involved structured deposits of cash into bank accounts followed by international funds transfers out of Australia[15]. More complex methods have used accounts of shell and front companies or accounts of associates to hide movement of funds. For example, associates can open an account and give the debit card associated with the account to a member of the terrorist organisation to enable access to cash via withdrawals from overseas bank ATMs.

The New Zealand banking sector acts as the major conduit for international payments. As part of the modern banking network, the sector provides financial access to high-risk jurisdictions. The Financial Sector section, and the RBNZ Sector Risk Assessment, discuss the sector's vulnerability further.

Money value transfer systems

Along with the banking sector, the remittance sector has been exploited to move illicit funds and is also vulnerable to terrorist financing. FATF has identified money transfer providers as especially vulnerable to abuse for terrorist financing where they are unregulated, not subject to appropriate AML/CFT supervision or where they operate without a license[16]. For example, the FATF report on Da'esh[17] notes that a common methodology for financing foreign terrorist fighters is to send money via money remitters who have agents operating in border areas close to territory held by the group.

Like banks, the New Zealand money remittance sector has global reach; although many service providers focus on specific regions. The Financial Sector section, and the DIA Sector Risk Assessment, discuss the sector's vulnerability further.

Cash

Like other criminals, any domestic terrorists may seek to use cash to obscure financing transactions. Cash may be used to obscure movement of funds between conspirators and/or purchases for terrorist use (such as weapons, chemicals or provisions).

Cash continues to be a widespread aspect of international terrorist operations, especially foreign currency, such as EUR and USD. Physical transportation of cash across an international border is still very common[18]. Cash may also be used in conjunction with other channels to move terrorism finances. For example, funds raised in cash may be moved off-shore, deposited in an overseas bank account with low AML/CFT controls, and withdrawn from an ATM in a third jurisdiction and diverted to terrorism without a recorded trail.

Although the New Zealand cash economy is smaller than many similar sized countries, cross-border cash movements valued at the equivalent of over NZD 800 million were reported to the FIU in 2016. The value of currency moved may allow for small amounts of cash to be diverted to terrorism, particularly through intermediate jurisdictions. However, less than 5% of reported funds are in higher risk EUR and USD and only a small amount of these funds are likely to be transported to high-risk jurisdictions.

Financial activity through high-risk jurisdictions

Terrorist financers may seek to use another jurisdiction as a channel to mask the ultimate destination of funds. Jurisdictions with poor AML/CFT controls, particularly those countries and territories that are non-cooperative with FATF, are likely to be attractive conduits to terrorism financiers.

Finance and trade hubs in regions affected by terrorism, or jurisdictions bordering conflict zones, may also act as conduits for terrorism financing. Most notably, reports have indicated that some

[15] Ibid.
[16] FATF "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", FATF February 2015.
[17] Ibid.
[18] FATF "Emerging Terrorist Financing Risks".

terrorism financing has occurred via professional money laundering through exchange houses in Middle Eastern regional hubs[19]. In these cases, terrorist sympathisers in exchange houses appear to have diverted profits from laundering proceeds of crime to regional terrorist causes. It is also possible that apparently legitimate funds could be funnelled through a regional hub before being diverted to a jurisdiction affected by terrorism.

The New Zealand economy's exposure to high-risk jurisdictions has increased in recent decades with integration into the global economy. Even comparably small financial flows to high-risk jurisdictions could hide a significant value of funds in a terrorism-financing situation because of the relatively small amounts of funds involved.

Abuse of New Zealand structures

Like international money laundering networks, larger scale terrorism financing networks may seek to use legal person and arrangement structures to mask their involvement. Using New Zealand legal structures to give the appearance of funds originating in New Zealand may be equally attractive to terrorism financers as to money launderers. In 2014, a website associated with Da'esh was reported to have used a New Zealand virtual office address. Similarly, large scale or complex terrorism financing may seek to use New Zealand alternative payment platforms to give the impression funds originate from a low risk jurisdiction.

Non-profit organisations

NPOs are another channel noted internationally as being vulnerable to abuse for terrorism financing purposes. The NPOs at most risk of terrorist abuse are those engaged in "service"[20] activities which are operating in close proximity to an active terrorist threat[21]. NPOs that send funds to counterpart or "correspondent" NPOs located in, or close to, countries where terrorists operate are vulnerable to exploitation. Unless proper due diligence is done on the counterpart NPO with sound auditing of how donated money is used, control over the use of donations can be at risk of diversion to terrorism.

International case studies have highlighted that TF can also occur in domestically oriented NPOs in lower risk jurisdictions. Given the international trend towards lone actor and small cell terrorism, it is most likely the threat of abuse of NPOs for domestic raising of funds for TF would relate to individuals in a position of financial trust, stealing charitable proceeds, or impersonating a charity to solicit donations. There have been no observed instances of this occurring in New Zealand.

The Regional Risk Assessment of Non-Profit Organisations and Terrorism Financing 2017 rated New Zealand's overall risk of terrorism financing through non-profit organisations as low. In particular, the report found that the terrorism financing threat to New Zealand NPOs is low with no identified links between NPOs and terrorism.

[19] See for example, Nick McKenzie and Rick Baker, "Terrorists Taking Cut of Millions in Drug Money" Sydney Morning Herald, 23 January 2014 http://www.smh.com.au/national/terrorists-taking-cut-of-millions-in-drug-money-20140122-3196s.html.
[20] 'Service' activities are those that focus on providing a service to a community or a group of people, for example housing, social services, education and health care.(This factor alone does not determine the overall risk rating and may be mitigated by other factors).
[21] FATF report "Risk of terrorist abuse in non-profit organisations", Paris, June 2014 www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html.

Table iv: Overview of vulnerability of New Zealand NPOs

Type of NPO	
Description	Vulnerability
Registered charities	
The largest class of NPOs in New Zealand with a population of approximately 27,000[22]. Characterised by many small operations, with a comparably small number of larger organisations[23]. TF vulnerability is highly concentrated in those charities that conduct operations offshore, in particular amongst the comparatively small number of charities with operations in high risk jurisdictions[24].	Moderate to High
Tax-exempt NPOs that are not charities	
Approximately 25,000 New Zealand NPOs fall within this category. The majority (23,000) of these are bodies for promoting amateur games and sports. There are around 2000 regional and local promotional bodies that could conceivably be abused for TF, however, the regulatory and local government oversight in place for these bodies likely reduces their attractiveness.	Moderate
Donee organisations[25]	
There are approximately 25,000 donee organisations in New Zealand, the majority of which (22,500) are registered charities. Of the 2,500 that are not registered charities the majority (2000) are schools, which are subject to oversight from the Ministry of Education making access for offenders more difficult. The comparably low level of international exposure effectively limits their vulnerability to TF.	Low
NPOs with income below NZD 1000	
Limited information is available on NPOs that have a net income below NZD 1000 as these entities do not file income tax returns, but the number is estimated to be between 10,000 and 20,000. While such entities may conceivably be able to engage in some small scale TF, they are likely to be lower risk due to their low availability, low international exposure and low overall attractiveness to offenders.	Low
Non-resident tax charities	
There are approximately registered 285 non-resident tax charities. These entities are overseas registered charities that have some form of financial operation in New Zealand. Despite being small in number, these entities are inherently higher risk given their vulnerability to movement of funds into or out of New Zealand. It is possible funds from such entities could be diverted to terrorist activity without New Zealand government oversight.	Moderate

[22] Having significant overlap with other major categories of NPO.
[23] Approximately 95% have an operating expenditure under NZD2 million.
[24] Of the 27,000 registered charities in New Zealand, approximately 1500 report they have overseas operations. Those with overseas operations tend to focus on jurisdictions within the Asia-Pacific region (>50%).
[25] A donee organisation must be a New Zealand society, institution, association, organisation, trust of fund. Its funds must be applied wholly or mainly to charitable, benevolent, philanthropic or cultural purposes in New Zealand. When an organisation is granted donee status for tax purposes, any gifts of money it receives qualify for tax advantages.

Sector risk assessments

In 2011 and 2017/2018 each of the AML/CFT Act sector supervisors – the RBNZ, DIA and the FMA (formerly the Securities Commission) – produced assessments of their respective sectors. These assessments used surveys and information from identified entities against a modified version of the model developed by the World Bank and Asia Pacific Group on Money Laundering (APG) to determine structural risk areas. The areas identified in the assessments were:

- size of sector;
- turnover;
- cash services;
- international transactions; and
- high-risk customers.

In 2014, the DIA published an additional series of risk guidance notes that refined the 2011 ratings and included additional sectors of:

- cash transport;
- casinos;
- currency exchange;
- Trust and Company Service Providers (TCSPs);
- money remittance;
- non-bank credit cards issuers;
- safe deposit boxes; and
- stored value cards.

Future iterations of the sector risk assessments continue to draw on risk assessments and annual reports by the individual reporting entities within each sector. The reports continue to provide supervisors with accurate information on which to base future risk assessments. The interaction between the various assessments allows a top down and bottom up understanding of money laundering and terrorism financing risks facing New Zealand. The relationship between the assessments completed by the separate sectors and the FIU is shown below:

Figure iv: Relationship between AML/CFT risk assessments

Systemic vulnerabilities

A number of systemic vulnerabilities are identified in the New Zealand AML/CFT regime by the sector assessments. These vulnerabilities include:

- cash transactions;
- large flow of funds;
- reliance of customer due diligence by third party;
- anonymity (of beneficiaries, beneficial owners etc.);
- attitude that customer due diligence is complete if customer holds an account;

- dealing with high risk jurisdictions;
- offending (i.e. fraud and corruption) within sector;
- trusts;
- lack of price transparency;
- rogue or complicit employees;
- industry's perception as a low risk;
- correspondent banking;
- use of intermediaries; and
- easily transferable value.

To support the systemic vulnerabilities identified by the sector supervisors, the FIU has identified from its data additional potential vulnerabilities. These include:

- under reporting;
- failure to understand risk;
- the use of fraudulent documents;
- poor training;
- terrorist sympathisers;
- direct links or sympathy to organised criminal groups;
- low or no AML/CFT coverage across a sector and/or product; and
- unnecessary layering between reporting entities and individuals conducting transactions – similar to transactions through third party service providers.

Summary of SRA findings

Table v: Findings of sector risk assessments in 2011, 2014 and 2017/2018

DIA Supervised Sectors (Phase 1)			
Sector	**2011 rating**	**2014 rating**	**2018 rating**
Money remittance	HIGH	HIGH	HIGH
TCSPs	HIGH	HIGH	HIGH
Casinos	MEDIUM TO HIGH	HIGH	MEDIUM TO HIGH
Currency exchange	MEDIUM	MEDIUM	MEDIUM TO HIGH
Safe deposit boxes	LOW TO MEDIUM	LOW	LOW
Cash transport	LOW TO MEDIUM	LOW	MEDIUM
Non-bank credit cards	LOW	LOW	MEDIUM
Factoring	LOW	LOW	LOW
Debt collection	LOW	LOW	LOW
Payroll remittance	LOW	LOW	LOW
NBNDTL	LOW	LOW	MEDIUM
Financial leasing	LOW	LOW	LOW
Tax pooling	N/A	MEDIUM	LOW
Stored value instruments	N/A	LOW	MEDIUM
DIA Supervised Sectors (Phase 2)			
Sector			**2018 rating**
Lawyers			MEDIUM TO HIGH
Accountants			MEDIUM TO HIGH
Real estate agents			MEDIUM TO HIGH
High-value dealers			MEDIUM TO HIGH
New Zealand Racing Board			MEDIUM TO HIGH
Conveyancers			LOW

FMA Supervised Sectors		
Sector	**2011 rating**	**2017 rating**
Derivative issuers	MEDIUM TO HIGH	HIGH
Brokers and custodians	MEDIUM	MEDIUM TO HIGH
Equity crowd funding platforms	N/A	MEDIUM TO LOW
Financial advisers	MEDIUM TO HIGH	MEDIUM TO LOW
Managed investment scheme managers	MEDIUM TO HIGH	MEDIUM TO LOW
Peer-to-peer lending providers	N/A	MEDIUM TO LOW
Discretionary investment management services	N/A	MEDIUM TO LOW
Licensed supervisors	N/A	LOW
Issuers of securities	LOW	LOW

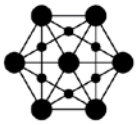
RBNZ Supervised Sectors		
Sector	**2011 rating**	**2017 rating**
Registered banks	HIGH	HIGH
Non-bank deposit takers	MEDIUM	MEDIUM
Finance companies	MEDIUM	LOW
Building societies	MEDIUM	MEDIUM
Credit unions	LOW	MEDIUM
Life insurers	LOW TO MEDIUM	LOW

Financial sector vulnerability

Figure v: Financial sector vulnerability profile:

Bank dominated (but still with significant opportunities for criminals outside of the banking sector)

Modern and open



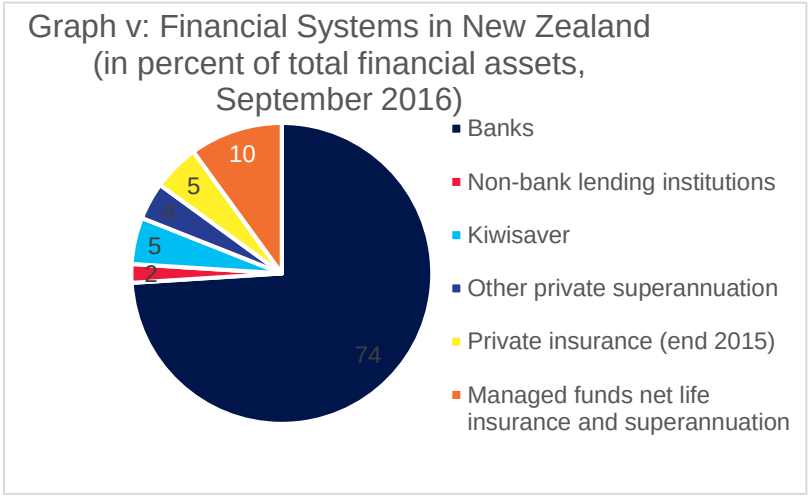
Connected to other money laundering and terrorist financing channels

The financial sector plays a central role in the New Zealand economy and its services cross over with the gatekeeper, cash and international channels for money laundering and terrorism financing. This central role increases financial institutions' risk exposure.

New Zealand has a well-regulated financial sector that operates within the context of New Zealand's small open economy. Since the mid-1980s New Zealand has transitioned from one of the most regulated economies in the Organisation for Economic Cooperation and Development (OECD) to one of the least, with reform in the financial system focusing on reducing compliance cost while maintaining or enhancing integrity. As a result, New Zealand has a small shadow economy by international standards. For example, 2010 World Bank research placed New Zealand's shadow economy as the fifth smallest on the list of OECD countries[26]. This significantly reduces the national money laundering and terrorism financing risk, but potentially increases the criminal incentive to abuse the financial sector.

Bank dominated sector

New Zealand's financial system is dominated by the banking sector, which accounts for about 75 percent of total financial assets[27]. This is a high proportion of financial assets to be accounted for by banks in comparison to other countries. Annual reporting to the Sector Supervisors indicates that the value of transactions through the banking sector total NZD 83 trillion per annum, compared to NZD 80 billion through remittance sectors and NZD 500 billion through brokers and custodians (which would almost exclusively be within the banking sector).



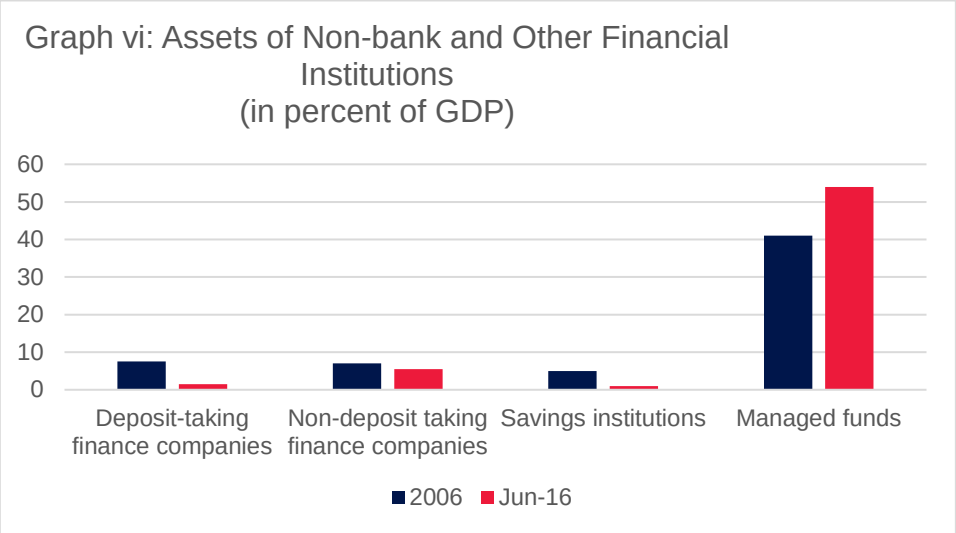
[26] Schneider, Friedrich, Andreas Buehn and Claudio E. Montenegro "Shadow Economies All over the World, New Estimates for 162 Countries from 1999 to 2007", World Bank 2010.
[27] "New Zealand Financial System Stability Assessment" ("FSAP Report") International Monetary Fund 10 April 2017.

The system is further concentrated to four subsidiaries of the largest Australian banks, whose share in the banking sector's total assets was 86% at the end of 2016[28]. As such, a significant portion of inherent money laundering and terrorism financing risk in the financial sector is highly concentrated on a small number of institutions. These banks' assets are focused on lending to the domestic private sector, in particularly to lending relating to the residential real estate market and farms. As real estate has been identified as being vulnerable and attractive to criminal investment, the national risk of high value money laundering in New Zealand may be further skewed towards real estate investments, compared to some other jurisdictions.

However, New Zealand banks offer a full suite of other retail services many of which are vulnerable to money laundering[29]. These services may be used to make large illicit transactions running a full spectrum from large transactions supposedly related to business activity to numerous small-scale cash placement.

While other vulnerable sectors such as money remitters and casinos are much smaller than banks, they also provide money laundering and terrorism financing opportunities. Each of these sectors are exposed to large numbers of high-risk transactions that offer criminals opportunities to place cash and/or move funds offshore. Casinos can offer criminals an end-to-end laundering opportunity that superficially establishes the origin of funds along with a suite of financial institution-like services. In both of these sectors, it is not uncommon for a number of transactions to be conducted outside a business relationship, which allows criminals to spread suspicious activity across different reporting entities to avoid detection.

The understanding of risk in derivatives and brokers/custodians has improved in recent years. Overall, the capital market in New Zealand remains relatively small and although it has grown in recent years, this growth is been driven by managed funds[30] which are assessed by the FMA as lower risk[31]. As shown in the graph below, the value of assets in managed funds is significantly higher than any other non-bank financial sector.

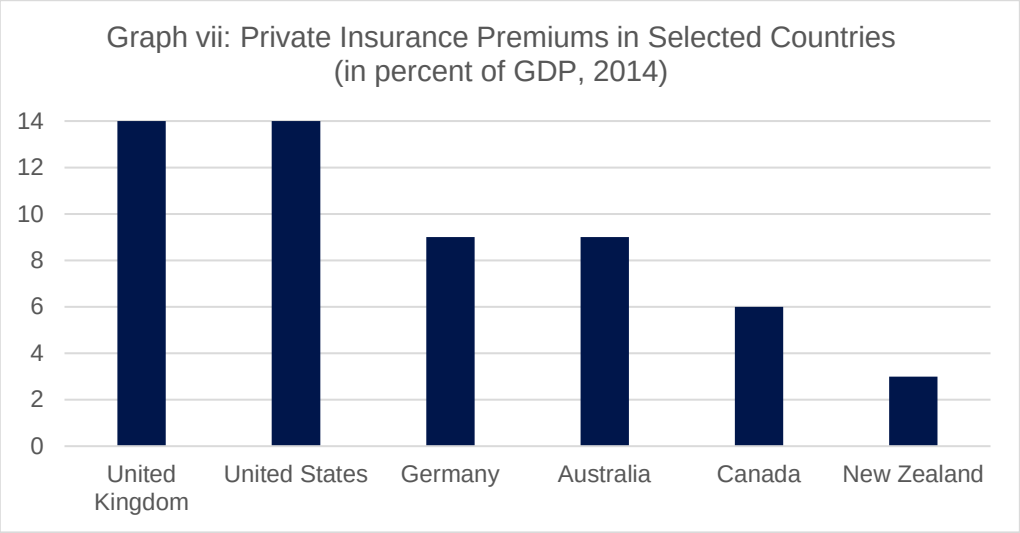


Growth in lower-risk KiwiSaver schemes, partial privatization of state-owned enterprises and low global and domestic interest rates have driven increases in stock market capitalisation. Between

[28] Ibid.
[29] "Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Sector Risk Assessment for Registered Banks, Non-Bank Deposit Takers and Life Insurers" Reserve Bank of New Zealand, April 2017
[30] FSAP Report
[31] "Anti-money Laundering and Countering Financing of Terrorism – Sector Risk Assessment 2017" Financial Market Authority 2017

2004 and 2014, the share of primary listings' holdings by domestic institutional investors increased 9 percentage points to around 40%. The number of transactions in secondary markets increased almost 300% on the NZX50 since 2010. However, share market capitalisation in 2016 was 43% of GDP compared to 105% in Australia[32].

New Zealand's insurance sector is also small, and although there are 96 licensed insurers, the market is concentrated with half of non-life premium income accounted for by the largest insurer. The Government also accounts for about half of non-life premium income by providing coverage of particular risks through the Accident Compensation Commission (ACC) and the Earthquake Commission (EQC). As savings have migrated away from insurance to investment products, vulnerability of the insurance sector has further decreased and life insurance, which is the only supervised insurance sub-sector, has also been assessed by the RBNZ as being low-risk[33].



Bank secrecy

Internationally, banking secrecy has traditionally been one of the major vulnerabilities for money laundering and terrorism financing. New Zealand does not have a reputation for banking secrecy. Bank and other financial accounts do not retain greater privacy rights than personal information held by other entities. The New Zealand Privacy Act 1993 specifically allows sharing of information, including financial information, for law enforcement purposes while the AML/CFT Act, the Criminal Proceeds (Recovery) Act 2009 (CPRA) and the Search and Surveillance Act 2012 include provisions to enable agencies to access information for law enforcement purposes.

Modern payment technology

New Zealand's major payment and settlement systems are electronic and the high value systems settle on a real-time gross basis. These systems are also fully integrated into the major international payment channels. These modern systems are symptomatic, and a driver, of the move away from the cash economy, which helps to reduce the macro-level exposure to cash laundering. However, these systems also allow fast movement of funds and facilitate online activity with less face-to-face interaction increasing opportunities for anonymity.

As with legitimate customers, money launderers and terrorism financiers may be attracted by the speed and convenience of new payment technology enabled transactions. Such convenience

[32] "Market Capitalisation of Listed Domestic Companies (%GDP)" World Bank Data https://data.worldbank.org/indicator/CM.MKT.LCAP.GD.ZS
[33] FSAP Report.

allows fast layering. Additionally, criminals can exploit the borderless nature of the internet whereby there are difficulties regulating financial services that operate online.

Financial payment technology continues to develop rapidly. The emergence of new payment technologies increase the opportunities for money laundering, in particular where they allow criminals to exploit developments that breakdown the barriers posed by international borders, or facilitate new anonymous means of payments between individuals. By contrast, new payments technologies offer opportunities to design in anti-money laundering and countering financing of terrorism (AML/CFT) risk mitigation at the time they are launched. For example some new technologies that have better recordkeeping and supporting systems may be better able to detect unusual or suspicious activity.

New payment technologies offered by third parties may exacerbate vulnerabilities in the financial sector by circumventing or obstructing AML/CFT controls. New payment technology may be an attractive means of distancing a money launderer's activity from a reporting entity for example by presenting new opportunities for non-face-to-face transactions. Alternatively, a third party may offer a new payment facility that places a layer between the money launderer or terrorist financier and the reporting entity.

Outside of traditional payment technology, New Zealand has had a mixed uptake of the new payment services identified as high risk internationally. Cash tokens and other bearer negotiable instruments are available and in particular financial institutions may be exposed to open-loop products, such as travel cards, issued by other institutions. Formal virtual asset service providers have only a small presence in New Zealand. Individuals who operate outside of regulations as informal exchanges using bank accounts, expose institutions to risk and provide criminals opportunities to obtain virtual assets for illicit purposes. Mobile phone-based money transfer services have been identified as an emerging issue.

Gatekeeper professionals vulnerability

Figure vi: Gatekeeper professionals vulnerability profile

Provide access to specialist services allowing sophisticated laundering

Provides legal structures and arrangements that allow anonymity

Conduct large transactions and manage large values of funds and assets

Lawyers, conveyancers, accountants and real estate agents provide a 'gatekeeper' role in providing professional services to clients. The services provided by lawyers, conveyancers, real estate agents and accountants are very important for the efficient functioning of New Zealand's business and financial systems. The types of services provided and the everyday nature of these services in the legitimate economy also make them attractive to money launderers and terrorism financiers. Money launderers and terrorism financiers exploit professional services because they:

- provide the impression of respectability or normality especially in large transactions;
- create a further step in the money laundering chain that frustrates detection and investigation; and
- allow access to services and techniques that they would not normally have access to, including facilitating setting up structures such as trusts and companies.

Increasing financial sector and law enforcement scrutiny of possible illicit funds further incentivises criminals' use of professional services when seeking to:

- hide criminal financial and business dealings;
- obscure the identity of the person(s) behind the criminal dealings; and
- hide illicit financial assets in property and other investments.

Analysis of 47 properties subject to criminal proceeds recovery action by the New Zealand Police Asset Recovery Unit (ARU) identified a number of professional services used to launder funds through trust accounts; purchasing of real estate; creation of trusts and companies; management of trusts and companies; management of client affairs; and transfer ownership of assets to third parties. In all of these cases, there was no evidence of complicity on the part of the gatekeeper professionals involved. Hiding the ownership of property was the most common money laundering method, generally by putting property in the name of a trust set up by a lawyer. The second most common method was transferring the criminal proceeds to a lawyer or real estate agent by electronic transfer.

Table vi: Overview of money laundering risk to gatekeeper professionals by money laundering stage

Money laundering stage	Typical way services used by launderers
Placement	Money launderers and terrorism financiers can use professionals at the placement stage of laundering notably when offending is within the sector but occasionally through cash deposits with professionals.
Layering	Professionals also create distance between illicit wealth and criminal activity at the layering stage. This might involve the further establishment of legal persons and arrangements in nominees' names or the professional acting on behalf of a client in a proxy role to obscure ownership. The layering process commonly involves several different professionals with the same money passing through facilities provided by these professionals. At the layering stage, illicit funds are less likely to involve cash and ultimately may not appear out of the ordinary.
Integration	Finally, professionals can support investment of illicit funds in property and other high value investments at the 'integration' stage when funds appear legitimate. For example, property titles placed in third parties' names or in the names of trusts or companies creates distance from the beneficial owner and protects the assets from confiscation or seizure.

Regulatory vulnerabilities

New Zealand lawyers and conveyancers adhere to high standards of practice and ethics that may, in turn, reduce the vulnerability of lawyers to criminal misconduct. Specifically, lawyers must not act in a way that unwittingly facilitates criminal offending, with current standards enforced by the New Zealand Law Society. Lawyers practicing on their own account and operating a trust account are subject to oversight, including risk-based inspections, by the New Zealand Law Society Inspectorate. This oversight aims to ensure proper conduct in operating a professional's trust account to protect clients' money and minimise exposure of the Lawyers Fidelity Fund; which also has some mitigating effect on money laundering and terrorism financing risk.

Accountants also have high standards of practice and must comply with standards enforced by professional bodies, such as the Chartered Accountants Australia New Zealand. These standards include that accountants must not act in a way that facilitates criminal offending.

In New Zealand, real estate agents must hold a current licence and comply with the requirements of the Real Estate Agents Act 2008. Agents are licensed, supervised and disciplined by the Real Estates Authority, which is an independent government agency. Real estate agents must also comply with the Real Estate Agents Act (Professional Conduct and Client Care) Rules 2012 and the Real Estate Agents (Audit) Regulations 2009, both of which prescribe high standards of ethics, transparency and financial accountability. The majority of real estate agents in New Zealand are also members of the Real Estate Institute of New Zealand (REINZ). REINZ members must abide by the REINZ Codes of Practice in addition to the statutory obligations outlined above, as part of their membership.

Historical low rates of suspicious activity reporting by professional services (under the FTRA 1996) indicate the general measures were not ensuring sufficient professional vigilance to mitigate the risk of money laundering and terrorism financing. Between the commencement of the FTRA 1996 and 1 December 2017, the FIU only received 190 suspicious activity reports from lawyers and 7 suspicious activity reports from accountants. Introduction of the second phase of the AML/CFT

reforms has gone some way to addressing this vulnerability and enhancing professional vigilance to mitigate the risk of the money laundering risk to lawyers, conveyancers, accounts and real estate agents. Since they became reporting entities under the AML/CFT Act, the FIU has received 137 suspicious activity reports from lawyers, 65 suspicious activity reports from real estate agents, and 14 suspicious activity reports from accountants.[34]

In addition, regulatory vulnerability in relation to companies and trusts create further incentives for criminals to use professional services. Companies and trusts can be quickly and cheaply set up to obscure beneficial ownership. Furthermore, criminals can place companies in the names of nominee directors and/or shareholders, who are often the facilitating professional. Parties to trusts may not be recorded anywhere except in the facilitating professional's records. This exposes professionals to criminals seeking to obscure their interest in illicit funds.

Structural vulnerabilities

There are several structural vulnerabilities in New Zealand, including that:

- professional services comprise many, small, widely available businesses increasing the market from which offenders can seek out a suitable local professional target;
- New Zealand companies and trusts are easy to establish and offenders can secure anonymity through the professional/client relationship;
- international online services are also widely available, are low cost and are accessible from anywhere in the world. Services remain available online or through professional introductions, and in cases marketed to offshore clients. In many instances, anonymity of privacy and secrecy of these services is actively promoted; and
- professionals' ability to distinguish between suspicious activity and legitimate activity depends on a good understanding of the risks, having appropriate processes in place to mitigate risk, or monitor transactions to detect unusual activity.

Service vulnerabilities

Use of trust accounts

The use of trust accounts held by New Zealand professional gatekeepers are attractive to criminals as they can:

- be used as part of the first step in converting the cash proceeds of crime into other less suspicious assets;
- permit access to the financial system when the criminals may appear otherwise suspicious or undesirable to a financial institution;
- be used in a cancelled payment or loan scheme to obscure the origin of illicit proceeds;
- serve to help hide ownership of criminally derived funds or other assets; and
- be used as an essential link between different money laundering techniques, such as purchasing real estate, setting up shell companies/trusts and transferring the proceeds of crime.

Real estate transactions

There are consistently high numbers and values of real estate assets restrained and forfeited in New Zealand cases, which often involve several properties. The inherent vulnerability for conveyancing and real estate transactions is high and exacerbated by the high annual volume of very large asset transfer.

[34] SAR stats are for the period 01/07/2018 to 06/06/2019 for lawyers; 01/10/2018 to 06/06/2019 for accountants; and 01/01/2019 to 06/06/2019 for real estate agents (these are the respective dates that each sector came under the Act).

The specialist knowledge needed to complete a real estate transaction in New Zealand means that most property transfers, including the receipt of settlement funds, are facilitated by experienced lawyers or conveyancers. In particular, the requirement from Land Information New Zealand (LINZ) to transfer title online significantly limits public access to conduct real estate transactions without a gatekeeper professional.

Professionals may be required to facilitate access to the real estate market for criminals acting as either vendors (who would generally seek a client relationship with a real estate agent) or purchasers. Criminals seeking to buy from, or sell to, third parties will need introductions to counter-parties, which is most commonly facilitated through agents (although private advertisement is not unknown). Professionals can also facilitate access to other providers for setting up services required in the transaction.

In most instances, professionals are used to facilitate the large financial transfers involved in real estate transactions. This is often facilitated through receiving payments from purchasers to trust accounts, particularly relating to settlement payments. The New Zealand Police has identified instances involving the proceeds of crime paid into lawyers' trust accounts in such transfers. In other cases, professional services have facilitated conveyancing involving real estate transactions conducted in cash or 'in kind' from the purchaser to the vendor. This creates an opportunity to disrupt illicit activity, as demonstrated in one case where a vigilant conveyancing lawyer detected and reported suspicious activity, leading to a successful prosecution and asset recovery.

Creation and management of trusts and companies

Trusts, companies and other legal persons or arrangements are extremely attractive vehicles for money launderers and terrorism financiers to hide a personal identity and that of the 'beneficial owner'. These structures allow for movement of criminal proceeds, while providing a veneer of legitimacy to illicit transactions and activity.

New Zealand legal, accountancy and TCSP professionals offer a range of services to establish and manage legal persons and arrangements for local and overseas customers. In particular, these services are attractive to money launderers and terrorism financiers because:

- New Zealand's reputation as a well-regulated jurisdiction provides a veneer of legitimacy and credibility;
- it is easier and cheaper to register companies in New Zealand than in other jurisdictions, meaning that New Zealand companies are essentially disposable;
- professionals or other third parties may provide resident director, or trustee, services for overseas customers;
- legal arrangements are versatile, allowing sale and transfer to other people, along with assets and bank accounts established in the name of a legal entity; and
  obscuring beneficial ownership is relatively easy using deeply nested and complex, legal arrangements across multiple jurisdictions.

Creation of trusts and companies was a common method used in the sample of professionally facilitated cases, while hiding beneficial ownership through methods like trust structures was used in all of the sample of real estate cases.

Legal persons vulnerability

A side effect of New Zealand's open economy and the ease of establishing legitimate businesses is that New Zealand legal persons are available for abuse by criminals. New Zealand has a very high number of businesses for the size of its economy. As of May 2019 there were over 630,000

New Zealand legal persons (mostly limited liability companies) which were registered at a rate of over 55,000 per year.

All relevant legal, accountancy and TCSP professionals are now required to conduct customer due diligence and record keeping in relation to the formation and administration of New Zealand legal persons. These requirements significantly improve the opportunity for professionals to detect abuse of legal persons, both at the time of registration and as part of ongoing due diligence.

Table vii: Overview of legal persons vulnerability

Type of legal person	
Description	Vulnerability
Limited liability company	
The most common form of legal person (approx. 628,300), accounting for around 96% of all New Zealand legal persons. They are the most vulnerable to ML/TF being both readily available and easy to set up, with limited liability on the shareholder for any criminal activity to which the company may be linked. Determined laundering attempts may involve use of nominees to circumvent NZ resident director requirements	High
Unlimited liability company	
Vulnerable in much the same way as LLCs, being simple to set up and easy to access. However, much smaller in number (approx. 390 in total) which limits the overall impact should they be abused. The shareholders can be held ultimately liable for the company's actions which may act also as a deterrent to criminal abuse. Their low number also likely reduces their attractiveness to criminals aiming to create anonymity by mimicking normal business behaviour	Low/moderate
Co-operative company	
Co-operative companies offer opportunities for hiding beneficial ownership as shareholding information is maintained by the company itself and not held on public the register. However, this vulnerability is mitigated by the shared ownership structure which makes it difficult to gain control for criminal purposes. Their low number (approx. 130 in total) limits the overall potential harm should they be abused.	Moderate
Overseas company registered in New Zealand	
These entities are inherently international with offshore control, which creates a particular vulnerability as it provides offshore persons access to the New Zealand financial system. However, they are comparably low in number (approx. 2,130 in total) with the majority being Australian companies which gives a comparable level of compliance assurance and avenues for law enforcement enquiry. In addition, the requirements for overseas companies are much stricter than for other legal persons[35]	Moderate
Limited liability partnership	
LLPs were designed to enable overseas investments for projects. They protect the privacy of the limited partner with only the general partner details visible on the public register. This may create challenges to identifying beneficial ownership. However, the Companies Office has visibility of all partners, and there are also comparably few LLPs (approx. 2,700 in total), which limits the potential impact should LLPs be abused	Moderate

[35] The Companies Office Registries Integrity and Enforcement Team (RIET) regularly review overseas non-ASIC companies and verify that the entity is in fact conducting actual business activities in New Zealand.

Legal arrangements vulnerability

The main type of legal arrangement in New Zealand, and most relevant from an ML/TF perspective are trusts. The principal attraction of trusts to criminals is they can be used to hide beneficial ownership and create a front behind which criminals may mask their activity. Trust arrangements can also be an effective means of dispersing assets while retaining effective control.

Trusts are widely available in New Zealand and are usually established by lawyers, accountants and TCSPs, all of whom are required to comply with AML/CFT obligations including conducting due diligence on the parties to the trust and determining who the beneficial owner is. There is no central register of trusts in New Zealand and as a result it may be difficult to identify the existence of a trust or the identity of the trustee if the trust does not interact with the New Zealand financial system. Information on any particular trust is limited to what is available at the time it interacts with the financial system or can be obtained from trustees.

Table viii Overview of legal arrangements vulnerability

Type of legal arrangement	
Description	Vulnerability
Express trust	
Express trusts are the most common type of trusts in New Zealand, estimated to number between 300 and 500 thousand. They are commonly structured using nominees and professional trustees which hides beneficial ownership. Express trusts are commonly identified as asset holding vehicles in Police Asset Recovery investigations. Increased AML/CFT controls have improved opportunities for detection but significant vulnerability remains due to overall low levels of transparency	High
Charitable trust	
Charitable trusts may be particularly attractive to criminals generating cash from offending as the charitable activity provides an opportunity to commingle illicit cash. There are some notable examples of New Zealand criminal gangs using charitable trusts, however, the primary purpose appears to have been to improve the gang's image rather than for money laundering. The main mitigating factor is that using this arrangement for money laundering exposes the activity to regulatory oversight	Moderate/high
Foreign trust	
New Zealand's settlor-based tax regime has created a market for trustee services to establish New Zealand foreign trusts for overseas settlors as an asset protection vehicle while minimising tax obligations. This market offers opportunity for money launderers and tax evaders to hold assets in New Zealand trusts. New Zealand's capability to detect abuse and assist overseas partners has significantly improved, with a register of foreign trusts established and increased AML/CFT obligations on gatekeeper professionals	Moderate/high
Maori land trust	
These legal structures are unique to New Zealand and differ from other trusts in that they are established by an order from the Maori Land court rather than being formed by settlors. They are difficult to establish and Te Ture Whenua Maori Act 1993 establishes a regime to minimise the risk of abuse for criminal purposes. Also, the community involvement and oversight would likely complicate attempts to abuse these structures for ML/TF	Moderate

Managing client affairs

The broad range of professional services enables money launderers to manage all of their financial and business affairs in one place. Professionals can act on behalf of clients in respect of both financial and legal affairs and changes to arrangements made quickly and frequently.

Typically, a money launderer arranges for a professional to set up a company or trust and then also act, or arrange for a third party to act, in a proxy role, including acting as a trustee, nominee resident director, or nominee shareholder. Money launderers, especially transnational launderers, may also use professionals to set up and manage bank or trading accounts creating a layer between the financial institution and the ultimate customer. With the fiduciary role appearing legitimate, the money launderer is able to conduct a range of criminal activity or asset transfers at arm's length from both regulatory and law enforcement agencies.

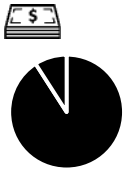
Services to overseas customers and purchasers

Generally, there is a high degree of international exposure for services offered by professionals. Many services are provided online and many services focus on offshore customers. New Zealand's risks involve the money laundering opportunity to:

- lend respectability or legitimacy to very large transactions;
- add value to illicit funds through the potential for capital gains;
- provide or facilitate services and techniques that money launderers would not ordinarily have access – such as the movement of cash and funds through trust accounts; and
- obscure layering and the integration of large amounts of money that frustrates detection and investigation.

Cash economy vulnerability

Figure vii: Cash economy vulnerability profile



Small compared to other jurisdictions

Anonymous and flexible

Cash businesses and other channels outside of AML/CFT control

Many forms of crime, particularly drug dealing and the sale of stolen property generate large amounts of cash. Likewise, cash remains a popular vehicle for transactions associated with these and other criminal offences because it:

- is anonymous;
- is flexible allowing peer-to-peer transactions;
- exists outside of formal financial institutions;
- does not require any recordkeeping; and
- forms no transactional ‘paper trail’.

However, cash present criminals with disadvantages, as cash:

- is inconvenient to transport when in bulk;
- is insecure; and
- increases the risk of detection – either by arousing suspicion by financial institutions or if discovered by authorities.

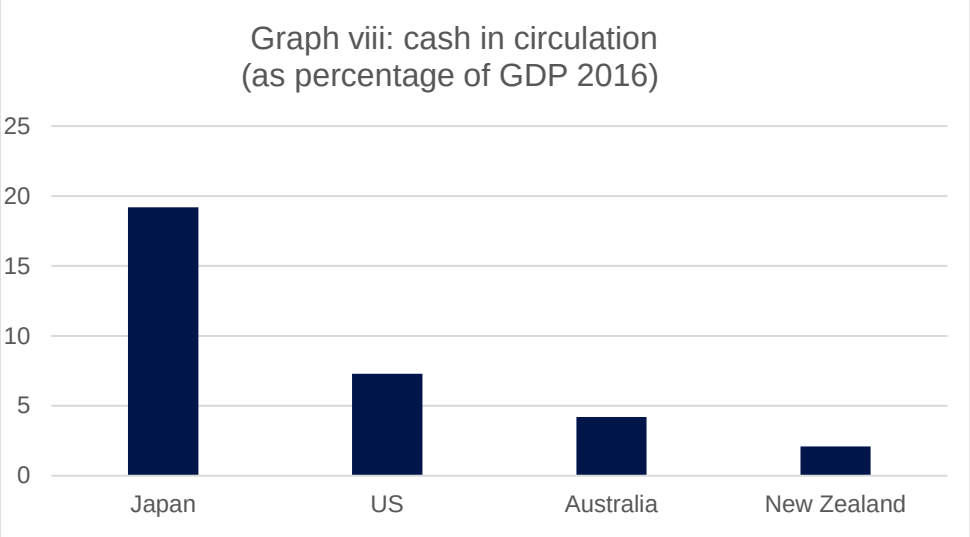
A number of low level criminals can lead a cash lifestyle. However, in order to make significant purchases or legitimise the appearance of their expenditure they need to place cash into the formal financial system to create a form of legitimacy. Broadly, placement must occur either through direct deposits, comingling with legitimate cash deposits or transportation offshore to locations where cash deposits raise less suspicion.

Once cash-generated proceeds have entered the financial system, the criminal origin may be obscured and criminals may have new opportunities to facilitate further offending. Placement can hinder investigations by providing criminals various options to conduct transactions that appear to be legitimate business transactions.

Opportunities to detect cash proceeds of crime are likely to be increasing given the large adoption of customer due diligence and suspicious activity reporting and border cash reporting requirements. Offending using cash is highly visible, and transactions involving cash are frequently identified in SAR reporting. Nonetheless, cash smuggling and placement through established methods (e.g. comingling with cash businesses, placement in cash intensive sectors such as casinos, and use of cash deposit “drop boxes”) can be difficult to identify and requires vigilance.

New Zealand cash economy

Cash is less popular in New Zealand compared to other jurisdictions. 2016 Payments NZ data shows that the value of banknotes in circulation in New Zealand amounts to 2.1% of GDP compared to 4.2% in Australia, 7.3% in the United States and 19.2% in Japan[36].



However, cash in circulation in New Zealand continues to increase faster than inflation in line with global trends. In particular, the NZD 100 banknote has also been growing in popularity in New Zealand. The total value of NZD 100 notes held by the public rose 184% between the years 2000 and 2015[37], compared to a 42% inflation of the Consumer Price Index over that time. This growth in the value of cash in circulation, in particular the value of high value notes increases the capacity of the shadow economy to facilitate illicit transactions and store proceeds of crime.

Improved controls has allowed increases in the detection of cash placement activities. Commencement of the AML/CFT Act and goAML (2013)[38], has further allowed the FIU to improve SAR reporting and identify structured cash deposits and long-term activities previously undetected. The introduction of large cash transaction reporting has further enhanced the FIU's capability to detect unusual patterns of cash transactions.

Vulnerability of sectors to cash laundering

The sector risk assessments analysed the channels most vulnerable to cash within the supervised sectors. This analysis informs where laundering of cash is available in the supervised sectors. The findings of the cash risk assessment are summarised overleaf.

[36] "Two Sides of the Coin: Cash Usage in New Zealand" PaymentsNZ, 20 May 2016 https://www.paymentsnz.co.nz/resources/news/two-sides-of-the-coin-cash-usage-in-new-zealand/
[37] Ibid.
[38] SAR reporting through the FIU's current core ICT system, goAML, commenced on 1 July 2013 when reporting pursuant to the AML/CFT Act commenced.

Table ix: Summary of findings of the cash risk assessment in the sector risk assessments

Sectors highly vulnerable to laundering of cash		
Sector	Cash services	Risk
Banks	Banks' cash intensive products include over-the-counter services such as depositing or withdrawal of cash, sales and purchases of foreign exchange, issuing or cashing travellers' cheques, and purchase of reloadable cash card products.	High risk of placement of cash; refining and foreign exchange
Building societies	Building societies, cooperatives and credit unions offer a similar range of cash intensive products and services to the core activities of retail banks.	High risk of placement of cash; and refining
Casinos	Casinos are a cash intensive business and there are many money laundering techniques that can be employed based on the diverse range of financial services offered. Classic methods for laundering cash included buying casino chips with cash proceeds and redeeming into a different form of value, and mixing winnings with cash proceeds into casino cheques	High risk of placement of cash; refining and foreign exchange
Money remittance	Most remittance services operate by accepting cash at an agent location which is then electronically transferred to the recipient location for the receiver to pick up in cash. Remittance businesses are also at risk of being used in cash transactions to break the audit trail of money laundering operations, particularly by overseas-based money launderers, for example by transferring to a New Zealand account so that a mule can withdraw cash and remit funds overseas.	High risk of placement of cash also at risk of layering; and foreign exchange
Sectors moderately vulnerable to cash laundering		
Sector	Cash services	Risk
Non-bank credit cards	Non-bank credit cards (stored value instruments) can also be used to transfer funds overseas via open loop global card networks, cash withdrawal options and the purchase of valuable assets. Cash passports may be reloaded with cash in structured amounts. Likewise cash withdrawals can be made worldwide in a variety of currencies. Other cash-based risks for non-bank credit cards: • ability to access cash at a range of ATMs worldwide • unusual cash advances and/or large cash payments • overpayments of balance	Moderate risk of placement and layering

Vulnerabilities in 'phase II' sectors

In addition, the sectors that have recently been brought into the regime in the second phase reforms are exposed to laundering of cash proceeds and have been associated with cash laundering in previous cases. The vulnerabilities to cash laundering will be described further in the relevant sector risk assessments.

Table x: Summary of findings of the cash risk assessment in phase ii sectors

Sector	Cash services	Vulnerability
High value goods dealers	High value goods dealers (including vehicle dealers) provide criminals numerous options for moderate value cash transactions, allowing cash to be converted to less conspicuous assets. Assets may then be either enjoyed by the money launderers (as integrated proceeds) or on sold as a layering transaction.	Placement and integration
Professional gatekeepers	Professionals may be used to conduct cash transactions, either as intermediaries for offenders or trust accounts may be used to place cash proceeds.	Intermediaries, placement
Real estate	The size of real estate transactions may make cash transactions in this sector conspicuous; however, anecdotal evidence suggests that purchases of property in cash do occur. Cash purchases of real estate may be used as either placement or integration in the same manner as less significant assets.	Placement and integration

Vulnerabilities in non-supervised sectors

As well as current and future AML/CFT supervised sectors, criminals take advantage of some non-financial businesses and financial service providers acting outside of regulation.

Alternative remittance

Alternative remittance, also known as underground banking and informal funds transfer systems, is a generic term for informal payment arrangements outside of the formal banking system. These systems may be derived from traditional financial networks that predate the formal banking system, and may be known as hawala, hundi or fei ch'ien depending on the geographic and cultural market. Such traditional services are cash intensive and offer criminals opportunities to place or move cash proceeds outside of the formal financial system.

The unifying principle of these services is that they facilitate transfer of funds or value without necessarily physically relocating it or with customers using the formal banking system. The diversity of geographic service, cultural norms and methods used can make regulatory control challenging and while these services are subject to the AML/CFT Act, some unregistered services may operate, or other supervised entities may provide underground services in addition to their supervised activity.

Alternative remittance services may provide a structure that inhibits detection of illicit activity by providing a service outside of the formal and regulated financial sector. Transactions may require no identification from either the originator or beneficiary of the funds other than a password sent

via phone, email, or text message. This anonymity allows criminals to place cash or move it offshore while avoiding customer due diligence.

Businesses

Cash businesses can provide an indirect route into the financial system for cash proceeds of organised criminal enterprises. Any business that could reasonably accept cash could be used to co-mingle cash proceeds. Bars and restaurants, beauty salons, barbers, and small-scale cottage industries have all been associated with this activity. Such businesses allow launderers to over-state cash takings to explain cash deposits to financial institutions. Alternatively, business expenses can be paid using cash proceeds, allowing corresponding legitimate earnings already in the financial system to be diverted as profit for the criminals.

The regularity with which ordinary businesses conduct transactions and the large number of businesses make them an attractive vehicle for money laundering. Criminals may also be attracted by the perception that a business front adds an air of respectability and is therefore unlikely to arouse suspicion. Integration of criminal proceeds into a legitimate business to transition from the criminal to the legitimate economy, or to prop up an uneconomical business, may also be the criminal motivation for offending.

Money laundering through a business can have subtle effects on the industry to which the business is associated. Infiltration of organised crime to facilitate money laundering can have a further corrupting effect on people involved, leading to facilitation of more offending. Furthermore, laundering criminal proceeds can give otherwise inefficient businesses a competitive advantage, or disadvantaging legitimate competitors. Left unchecked, widespread criminal infiltration of an industry may stifle innovation ultimately leading to poor service to customers, damage local economies and potentially make New Zealand business less competitive on the international stage.

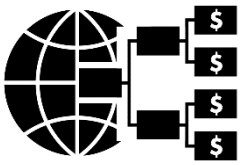
Cash businesses may also be attractive means of generating income for terrorism financing. As well as providing a normal opportunity to generate income, under-declaring cash takings may free funds for diversion to a terrorist cause. Alternatively, funds raised for terrorism, or to be used in proliferation, may be layered through the business, for example by creating a supposed reason for international payments. Although these risks have been recognised, this type of activity has not been observed in New Zealand.

Private high value good transactions

One of the most common and easiest methods of money laundering is through investment in high value commodities. Any high value commodity that holds significant value may be used in money laundering, particularly those that are transportable, maintain or increase value, and are transferable from person to person. A wide range of high value goods have been detected in New Zealand asset recovery cases, including art and antiques, jewellery and watches, precious metals and stones and vehicles.

Vulnerability to international threats

Figure ix: International vulnerability profile:



Global illicit capital flows threat

Open economy

Reputation and high integrity

New Zealand's attractiveness to international laundering and terrorism financing

Many of the same features that attract legitimate capital to New Zealand make New Zealand equally attractive to illicit capital flows. In particular, New Zealand's company and trust structures and the availability of associated professional services remain attractive to transnational and international money launderers. New Zealand's high level of integrity and transparency are likely to both deter and attract transnational illicit capital flows as while these factors may help to prevent illicit capital entering the economy; transnational criminals who are successful in moving proceeds through New Zealand benefit from an air of legitimacy from New Zealand's reputation. As the New Zealand economy continues to integrate into the regional and international economy, it is likely that the threat and risks posed by illicit capital flows will increase.

International abuse of shell companies

The association between New Zealand shell companies and international illicit transactions has been widely reported, most notably following the Thai interception of arms from North Korea on an aircraft leased by a New Zealand registered company in 2009. There have also been a number of less well publicised cases involving complex international money laundering in Eastern Europe. New Zealand shell companies have been involved internationally in cases relating to tax offending, money laundering, investment fraud and smuggling of illegal goods. New Zealand has since taken steps to mitigate these risks and deter transnational threats; for instance by introducing New Zealand residential requirements which ensure that at least one director will be in New Zealand or an enforcement jurisdiction, to provide information on the affairs of the company.

International abuse of trusts

A foreign trusts market has arisen in New Zealand as a by-product of New Zealand's principle-based approach to trust law. Unlike similar countries, New Zealand does not tax trusts with overseas settlors. This has created a market opportunity for New Zealand trusts to act as asset protection vehicles without incurring tax. Along with offering a legitimate vehicle, this market offers opportunity for money launderers and tax evaders to layer or hold assets in New Zealand trusts.

In addition, trusts provide money launderers and terrorism financiers a means to hide their beneficial ownership of assets and involvement in transactions. The introduction of mandatory reporting of beneficial ownership information to the IRD, accessible to the FIU and DIA for AML/CFT has mitigated issues caused by beneficial ownership.

Professional facilitation – availability of services, regulation and integrity

TCSPs, legal practices and accountancy firms provide many services, such as company and trust formation online and many actively market to offshore customers. In some instances the privacy

and secrecy of services is promoted, which would be attractive to transnational criminals. New Zealand professionals offer overseas clients all of the high-risk legal services identified by the FATF, including:

- use of trust accounts;
- purchase of real estate (this would also apply to other purchases of large assets and businesses);
- creation of trusts and companies;
- management of trusts and companies;
- setting up and managing charities; and
- managing client affairs[39].

It is worth noting that the high level of integrity of New Zealand's professionals may partially mitigate the risk of professional facilitation of transnational money laundering.

Bank secrecy

As discussed in the Financial Sector section, New Zealand is not a banking secrecy jurisdiction. New Zealand legislation does not provide for any greater privacy of financial affairs than other private information, while also providing mechanisms for law enforcement to access financial information.

Overseas investment attractiveness – businesses and markets

Investors of illicit capital are attracted by the same factors that attract legitimate investors. In addition, money launderers may attempt to move their proceeds through jurisdictions commonly used by investors in their own jurisdiction, or where investment returns may explain the origin of criminal proceeds.

New Zealand consistently scores well on the World Bank Doing Business[40] rankings for ease of doing business and business costs are comparatively low. The straightforward, business-friendly taxation system that supports capital development and international investment may also be attractive to transnational money launderers and terrorist financiers. New Zealand does not have currency controls and does not tax movement of capital. As with legitimate business, these factors reduce the cost of business for money launderers, and reduce the effort required to remain compliant with government requirements[41].

There are several major trading banks and numerous other banking institutions. Many large international banks gain representation in New Zealand through agents or sales offices that make the process of moving money into and out of New Zealand relatively easy[42]. Although geographically isolated, New Zealand's modern communications make movement of capital, including illicit capital, easy.

Limited financial markets

While the New Zealand economy is open and easily accessible, the options for layering and integration of proceeds of crime in the financial sector are more limited than in other jurisdictions. As discussed in the financial sector section, New Zealand's financial sector remains dominated by the banking sector, and the IMF notes that New Zealand investment remains heavily focused on real estate.

[39] "Money Laundering and Terrorism financing Vulnerabilities of Legal Professionals", FATF report, June 2013.
[40] "Doing Business" http://www.doingbusiness.org/rankings World Bank.
[41] "Why Invest Here?" New Zealand Trade and Enterprise https://www.nzte.govt.nz/en/invest/new-zealands-investment-advantage/
[42] Ibid.

Political and economic stability and reputation

Political and economic stability and a country's international reputation can act to both create and mitigate vulnerability to transnational money laundering. The orthodox approach would be to see New Zealand's high stability and low corruption as limiting opportunities for money laundering. By contrast, this as a factor that could attract illicit capital along with legitimate capital, both to make sure proceeds are safe (as in legitimate capital) and to give ill-gotten gains an air of respectability.

Shadow economy

New Zealand has a smaller shadow economy by international standards. For example, 2010 World Bank research placed New Zealand's shadow economy as the fifth smallest on the countries list of the Organisation for Economic Cooperation and Development (OECD)[43]. New Zealand's lack of a large shadow economy limits transnational criminals' opportunities to break the paper trail in New Zealand by layering illicit proceeds through informal sectors.

Alternative remittance and banking

There is an alternative remittance sector acting at least partly out of sight of the AML/CFT regime. These types of operations present a particular vulnerability to domestic and offshore illicit capital flows.

Financial providers that only offer services off-shore are not subject to Securities Act 1978 requirements to provide a prospectus, or the Reserve Bank of New Zealand Act 1989 requirements relating to capitalisation and governance introduced in response to the Finance Companies collapse and the associated fraud in 2011. Alternative banking platform providers can use a virtual office provided by an accountant, lawyer or TCSP as a place of business in New Zealand to register on the Financial Service Providers Register (FSPR) providing a veneer of regulation in New Zealand.

Trade

New Zealand's trade-focused economy creates inherent opportunities for money launderers to hide money laundering transactions amongst legitimate trade transactions. New Zealand also has well-established trade links with many of the jurisdictions that have been associated to major New Zealand cases of transnational crime.

The long-term trend in New Zealand trade is the shift from traditional markets, such as Australia and the United Kingdom, to trade with new and emerging markets, including in Asia. This shift is also happening in the context of growing international connectivity which reduces New Zealand's isolation from the wider world. Along with economic growth, this increase in trade and economic integration is likely to increase New Zealand's vulnerability to significant organised crime and money laundering risks.

International payments

The abuse of international payments can be combined with, or be inherent in, money laundering and terrorism financing methods such as trade-based money laundering, use of professional services, use of intermediaries, and use of trusts and companies.

Mainstream banks and remittance providers are highly available options for domestic money launderers and terrorist financiers, and unlike alternative remittance, no special networks are required to access these services. As a result, international payments offer a number of opportunities to launder funds or conduct terrorism financing transactions, including:

[43] Schneider, Buehn and Montenegro.

- movement of funds offshore for investment as part of either layering or integration;
- placement of cash proceeds, especially in the case of money remitters;
- use of money mules to create layers and obscure the money trail, for example, transnational payments to a money mule's account followed by cash withdrawal and remittance of cash break the money trail; and
- payments between companies for goods or services may facilitate payments between criminals in different jurisdictions and/or create layers in money laundering and terrorism financing schemes (see international trade section).

International payments also expose New Zealand to various transnational threats and crime types, such as corruption, overseas-based organised crime and international money laundering networks.

International payments was one of the factors considered in the Sector Risk Assessments, and those findings along with an assessment of the frequency with which each sector is abused in transnational cases known to the FIU are outlined in the tables below.

Table xi: Summary of sector vulnerability to abuse of international payment: FMA supervised sectors

FMA supervised sectors			
Description	Value of international payments through sector	Indicators in transnational cases	Vulnerability
Share Brokers			
NZX Market participants have a large proportion of customers based outside New Zealand, predominantly in Australia, but with links to other jurisdictions, such as the United States, United Kingdom, Brunei, China and Singapore.	NZD 24 billion	Unknown	Possibly moderate to high

Table xii: Summary of sector vulnerability to abuse of international payment: DIA supervised sectors

DIA supervised sectors			
Description	Value of international payments through sector	Indicators in transnational cases	Vulnerability
Money remitters			
The majority of money remittance transactions are international. Remittance services available in New Zealand are offered to over 200 countries worldwide. This sector also combines cash intensive businesses with facilitation of international payments and a high frequency of such transactions outside of business relations, which makes them attractive to money launderers and terrorism financers.	Unknown value, likely to be high	High	High

Trust and company service providers (TCSPs)			
Approximately 70% of all TCSPs offer services to international customers while approximately 20% do not specify whether international services are offered. TCSPs often do not directly conduct transactions, but provide the company or trust structure that facilitate transactions. As such, the value of international payments through the sector is likely to be low, while the value of international payments facilitated by the sector is likely to be much higher and relate to a wide range of financial activity.	Unknown value facilitated, likely to be high	High	High
Legal profession			
Many law firms actively promote their services to offshore clients, including services that are high risk for abuse by money launderers and terrorist financiers. No information has been gathered on the value of transactions facilitated by these services.	Unknown	High	High
Accountancy			
As with law firms, many accountancy firms promote their services to offshore clients, including services that are high risk for abuse by money launderers and terrorist financiers. No information has been gathered on the value of transactions facilitated by these services.	Unknown	High	High
Real estate			
The real estate sector continues to be marketed to overseas investment. However, reliable statistics on international investment in real estate are not available.	Unknown	Moderate	Moderate
Precious metals and gems dealers			
No information is available on the international exposure of precious metal and gem dealers.	Unknown	Low	Unknown – possibly low
Casinos			
The casino sector has a diverse customer base, including many international customers. As such casinos also offer a range of services to customers to facilitate movement of funds internationally to facilitate gaming.	NZD 14.5 million in 2009 from total sector of NZD 465 million	High	Moderate

Like money remitters, casinos also combines cash intensive businesses with facilitation of international payments and a high frequency of such transactions outside of business relations, which makes them attractive to money launderers and terrorism financers.			
Factoring			
Respondents indicated less than 10% of their business would involve international transactions. One respondent did note that invoices purchased from international clients tended to be of greater value.	Unknown	Unknown	Moderate (risk of TBML)

Table xiii: Summary of sector vulnerability to abuse of international payment: RBNZ supervised sectors

RBNZ supervised sectors			
Description	Value of international payments through sector	Indicators in transnational cases	Vulnerability
Banks			
A significant proportion of transactions by value through banks on a daily basis are international and the majority of international payments move through banks. One factor that will increase the risk of international payments is transactions with higher risk countries. Now that international wire transfer reporting has commenced strategic analysis of payments to higher risk jurisdictions is possible.	Estimated NZD 4.5 billion in international retails transactions per day in 2011[44]	High	High
Life insurers			
A significant proportion of transactions in the life insurance sector are domestic payments. This decreases the likelihood of transnational money laundering occurring. Current indications suggest international transactions account for less than 1% of the volume and value of transactions in the life insurance sector, and that the majority of international payments are to lower risk jurisdictions.	Less than 1% of transactions	Low	Low

[44] RBNZ letter to Ministry of Justice 4 April 2012.

Risks and outlook

Emerging risks and ongoing issues

Correspondent relationships

Correspondent relationships are critical to the New Zealand financial system. However, these relationships create risks that need to be managed.

Correspondent relationships create a situation where the correspondent's relationship is with the respondent institution, not with the parties underlying the transactions. The layers created between the correspondent and the parties of the transactions create a non-face-to-face relationship where the third party respondent can only mitigate the correspondent's risk. Arrangements involving multiple layers of respondents may also place additional layers between correspondents and the parties to transactions.

While trusted relationships and confidence in each other's risk management processes may provide correspondents and respondents with enough assurance that risk is managed, the relationships should be regarded as high risk and the practice creates an area of risk from a national perspective.

The AML/CFT Act puts controls in place that require financial institutions to conduct due diligence on respondents with whom it enters in to a correspondent relationship. These arrangements are designed to ensure that a risk-based approach is taken and that correspondent relationships are only entered into where the New Zealand institution is confident that the relationship does not create undue money laundering risk and that the respondents are trusted to take equivalent action to mitigate risk.

Displacement

It is likely that increased AML/CFT controls within the regulated sectors will lead money launderers and potentially terrorist financiers to seek new opportunities to conduct transactions through less controlled sectors. This is likely to lead to offenders using transactions, investments or assets in entities or sectors that have low levels of compliance or controls.

At the entity level, offenders are likely to target institutions that are known to have fewer AML/CFT controls. The FIU has already detected some limited instances of institutions within the remittance sector gaining a reputation as being an easy place for criminals to conduct business.

At the macro level, money laundering is likely to tend towards use of sectors where know your customer and customer due diligence procedure requirements are less stringent, or visible, and potentially to sectors known or thought to be less likely to report suspicious transactions. In some instances, criminals are seeking to avoid AML/CFT controls by conducting illicit transactions through sectors that are outside of the AML/CFT regime, such as by commingling cash in businesses.

Criminals may also increasingly seek to use intermediaries to interact with sectors with high levels of AML/CFT controls. This is likely to include use of family members and other parties to conduct transactions.

New Zealand may also be affected by international displacement. It is possible that increased AML/CFT controls within New Zealand will lead offenders to increasingly seek to layer criminal proceeds overseas to avoid New Zealand controls. Conversely, it is possible that overseas criminals will increasingly seek to layer funds through New Zealand either to avoid overseas controls or to capitalise on New Zealand's reputation, which are further enhanced by the perception

of a more stringent AML/CFT regime. Sectors where AML/CFT controls remain low are particularly vulnerable to the latter scenario.

De-risking

The phenomenon of reporting entities "de-risking" clients or classes of clients, particularly money remittance businesses, has raised a high degree of international concern. In October 2014, the FATF issued a statement on de-risking highlighting that the practice of deciding not to conduct business with a whole class of customer rather than managing the risks posed by individual customers was not a proper implementation of the risk-based approach and that the outcome of such actions may actually be contrary to AML/CFT objectives.

In New Zealand, de-risking has followed the international pattern of financial institutions terminating business relationships with money remitters because the money laundering risks are too high. In a New Zealand context where many immigrant communities rely on remittance businesses to support family and community in home countries, the social implications of de-risking are significant.

Perversely, the de-risking practice may increase national money laundering risk by forcing remittance businesses underground and displacing money remittance customers to higher risk alternative remittance operators. This outcome may increase the size of higher risk channels and the value of money remittance occurring in non-regulated sectors creating opportunities for money launderers and terrorist financiers.

Technological change

The rapid advance in technology, including payment and communication technology is likely to continue to create challenges for law enforcement in AML/CFT activity. New opportunities for money laundering are likely to be presented as technology evolves. In particular, technological advance carries four principal threats to AML/CFT law enforcement objectives:

- generation of proceeds of crime through cyber and cyber enabled crime
- development of technology that increases anonymity
- increased speed of transactions
- facilitation of international transactions

There is a risk that legislation will not keep pace with technological advances, for example allowing products or sectors to emerge that are outside of scope of the AML/CFT regime. However, New Zealand has taken a broad approach to legislative drafting and included provisions relating to measures to be taken in regards to high-risk technological advances, which should mitigate the legislative risks. The FIU recommends that agencies continue to monitor technological advances to anticipate any specific technological threats.

It is somewhat more likely that law enforcement and reporting entity AML/CFT programmes will be unable to keep pace with all technological advances. In particular, it is likely that products will emerge where vulnerabilities are not anticipated, or that require new investigative techniques or resource investment that cannot be put in place before exploitation can occur. Increased connection to the international system facilitated by evolving technology may also require new working relationships with overseas partners that take longer to develop than technology. Payment technologies that use business structures that straddle multiple jurisdictions may also create jurisdictional obstacles for law enforcement agencies that will need to be managed through effective partnerships with overseas law enforcement agencies.

Risks from combinations of threats and vulnerabilities

Combining the assessments of vulnerabilities within money laundering channels and the threat assessment, several risks emerge.

The flow on effect of these money laundering outcomes is likely to result in harm to the community from facilitated predicate offending significantly higher than the value of money laundering transactions.

The scale of money laundering in New Zealand does not appear significant enough to cause distortions that would be a direct risk to the stability of the financial system. However, it is possible that if New Zealand suffered significant loss of reputation from any of the risks identified here, the loss of confidence from international business partners would have an economic impact.

Compounding risk – particularly in relation to professional services	
Risk of layering vulnerabilities	It is likely that if offenders layer vulnerabilities, risk will compound. Several channels may interact creating higher levels of risk, in particular, professionals who act as gatekeepers to legal structures, businesses, capital markets and the New Zealand financial sector.
Risk of emerging money laundering methods	The combination of vulnerabilities may also lead to new methods. For example, the exploitation of vulnerabilities relating to companies, professionals and banking regulations has created a risk that alternative banking platforms will be created for criminal use.
Risk of compounding threats	Threats may also compound, for example offshore money laundering networks interacting with domestic organised crime. This is likely to expose New Zealand to higher levels of both money laundering and terrorism financing risk that may create a higher impact on law enforcement and reputational objectives than anticipated.
Legal structures	Although successive mitigation measures have been put in place (via Phase II reforms), residual risk will remain in relation to exploitation of legal structures by high-level domestic and overseas threats. This will require law enforcement and reporting entities to use those mitigation measures to disrupt laundering abuse in particular in relation to: • New Zealand shell companies being abused by transnational and international money launderers, as well as domestic offenders; • trusts being abused, particularly in relation to laundering of domestic proceeds, which may have a severe impact on law enforcement objectives, as well as transnational abuse impacting international reputation, particularly in terms of money laundering relating to tax offences; and • New Zealand company structures being abused to establish alternative payment mechanisms, such as alternative banking platforms to facilitate criminal transactions.
Money laundering in sectors with low levels of AML/CFT regulation	
Risk of domestic and international criminals abusing real estate investment	There is a risk of money launderers integrating criminal proceeds in, and potentially layering proceeds through, real estate investment which may create a secondary risk to integrity in sectors involved. In addition, there is a risk of transnational money laundering using New Zealand real estate investment.

	Phase II reforms have aligned the real estate sector and conveyancers with AML/CFT obligations, and recent amendments to the Overseas Investment Act 2005 go some way to mitigating the risk; however, law enforcement and sectors involved will need to maintain vigilance.
Risk of domestic criminals co-mingling cash proceeds in businesses	Cash businesses are not subject to AML/CFT, although business transactions through the financial sector are subject to AML/CFT monitoring, including cash deposits or withdrawals by businesses. These interactions present the opportunity to mitigate the risk of cash placement; however, residual risk of comingling cash proceeds with legitimate business earnings remains requiring financial institution vigilance.
Transnational money laundering	
Risk that domestic and international criminals abuse international payments	The risks relating to exploitation of mainstream international payments appear to be lower than in 2010 thanks to the increased AML/CFT controls, although risks emanating from these channels are inherently significant. There is likely to be a significant impact on New Zealand's law enforcement objectives and these risks may influence New Zealand's reputation.
Risk that professional services, legal structures or businesses are used to facilitate abuse of international payments	There is a risk that criminals will seek to use professional services and use of legal structures or businesses are used to facilitate international payments to defeat the AML/CFT controls on international payments. Phase II reforms have been implemented in part to mitigate this risk.
Risk that areas of low understanding will be abused to facilitate transnational laundering	In addition, there is a high level of risk that areas where global visibility is low will be abused to facilitate illicit international transactions, in particular, money laundering through international trade, the capital markets and alternative remittance. The abuse of these channels is also associated with particularly high-level threats including sophisticated predicate offenders.
Cash and assets	
Risk of criminals placing cash and dispersing assets	Traditional risks of placement of cash proceeds and dispersal of assets is inherently high because of the prevalence of cash-based money laundering threats, especially in relation to proceeds of drug offending and the resulting effect on law enforcement objectives. The risk of these methods is also likely to be higher in regards to lower value offending not considered in this report. It is possible that the cumulative effect of this low level offending has a very high impact on law enforcement objectives that is not currently visible.
Terrorism financing	
Risk that terrorism financing will occur in or through New Zealand	The information available indicates that New Zealand has a low overall level of terrorism financing risk. There is some low level, potentially growing, risk that domestic sympathisers or sympathisers within the region may seek to conduct terrorism financing transactions through the New Zealand financial sector or New Zealand structures. There is a risk that the low level of observable terrorism threat may lead to complacency. Recent events in New Zealand have emphasised the need to raise awareness of TF across sectors.

Glossary

AML/CFT	Anti-Money Laundering and Countering Financing of Terrorism
AML/CFT Act	Anti-Money Laundering and Countering Financing of Terrorism Act 2009
APG	Asia/Pacific Group on Money Laundering
ARU	Asset Recovery Unit(s), New Zealand Police
ATM	Automated Teller Machine
BCR	Border Cash Report
BERL	Business and Economic Research Limited
CDD	Customer Due Diligence
CPRA	Criminal Proceeds (Recovery) Act 2009
DIA	Department of Internal Affairs
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit, New Zealand Police
FMA	Financial Markets Authority
FMCA	Financial Markets Conduct Act 2013
FSPR	Financial Service Provider Register, New Zealand Companies Office
FTRA	Financial Transactions Reporting Act 1996
GDP	Gross Domestic Product
IMF	International Monetary Fund
IRD	Inland Revenue Department
MBIE	Ministry of Business, Innovation and Employment
ML/TF	Money Laundering / Terrorism Financing
NDIB	National Drug Intelligence Bureau
NPO	Non-Profit Organisations
NZX	New Zealand Stock Exchange
OECD	Organisation for Economic Cooperation and Development
OFCANZ	Organised Financial Crime Agency of New Zealand, New Zealand Police
RBNZ	Reserve Bank of New Zealand
REA	Real Estate Authority
REINZ	Real Estate Institute of New Zealand
RIET	Registries Integrity and Enforcement Team, New Zealand Companies Office
SPR	Suspicious Property Report
SRA	Sector Risk Assessment
SAR	Suspicious Activity Report
TBML	Trade-Based Money Laundering
TCSP	Trust and Company Service Provider
UNODC	United Nations Office on Drugs and Crime