

NEW ZEALAND

FINANCIAL INTELLIGENCE UNIT

NATIONAL MONEY LAUNDERING AND TERRORISM
FINANCING RISK ASSESSMENT

2018

FINANCIAL INTELLIGENCE UNIT
NEW ZEALAND POLICE
PO BOX 3017 WELLINGTON 6140
FIU@POLICE.GOV.NZ

CONTENTS

CONTENTS	1
EXECUTIVE SUMMARY	3
Introduction	3
AML/CFT Risk Assessment System	3
Description of money laundering and terrorism financing	3
The role of a National Risk Assessment	4
Terrorism financing threat, vulnerability and consequences	5
Money laundering threats in New Zealand	5
Summary of remaining vulnerabilities to money laundering in New Zealand	7
THREAT FROM PREDICATE OFFENCES	9
Scale of domestic laundering	9
Main predicate offence types	10
TRANSNATIONAL THREAT	12
Overview	12
International requests to the FIU	13
Methods associated with known threats	14
TERRORISM FINANCING THREAT	16
Financing of terrorism in New Zealand	16
Traditional terrorism financing methods and techniques	18
SECTOR RISK ASSESSMENTS	22
Systemic vulnerabilities	23
Summary of SRA findings	24
FINANCIAL SECTOR VULNERABILITY	26
Bank dominated sector	26
Bank secrecy	28
Modern payment technology	29
GATEKEEPER PROFESSIONALS VULNERABILITY	30
Regulatory vulnerabilities	31
Structural vulnerabilities	32
Service vulnerabilities	32

CASH ECONOMY VULNERABILITY	35
New Zealand cash economy	36
Vulnerability of sectors to cash laundering	36
Vulnerabilities in sectors that will be supervised in phase 2	38
Vulnerabilities in non-supervised sectors	38
VULNERABILITY TO INTERNATIONAL THREATS	40
New Zealand's attractiveness to international laundering and terrorism financing	40
International payments	43
RISKS AND OUTLOOK	47
GLOSSARY	52

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 the 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 businesses 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 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. In 2011, each of the AML/CFT supervisors assessed their respective sectors using information collected from entities within those sectors. Information from those assessments is included throughout this National Risk Assessment. In 2014, the Department of Internal Affairs (DIA) also published updated risk guidance notes. In 2017, the supervisors completed a new suite of Sector Risk Assessments drawing on the restricted version of 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.

Description of money laundering and terrorism 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 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 enjoying 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 earning, 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
- **Use:** Terrorist groups 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 second National Money Laundering and Terrorism Financing 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 concept¹.

This 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 DIA, the Financial Markets Authority (FMA) and the Reserve Bank of New Zealand (RBNZ)).

This National Risk Assessment uses a new model based on international guidance², where risk is a function of threats, vulnerabilities and consequences. Discrete assessments of New Zealand's principal threats and vulnerabilities within money laundering channels are set out in individual sections, while consequences, or the potential impact on law enforcement work and international reputation are considered throughout.

¹ 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\(fatf_releasedate\)](http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc(fatf_releasedate))

² FATF guidance "National Money Laundering and Terrorism Financing Risk Assessment", February 2013

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 low-corruption and high integrity, while being enviable, is also a vulnerability. Given the level of international scrutiny on terrorism financing, overseas terrorism financiers 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 and professional services very seriously.

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.

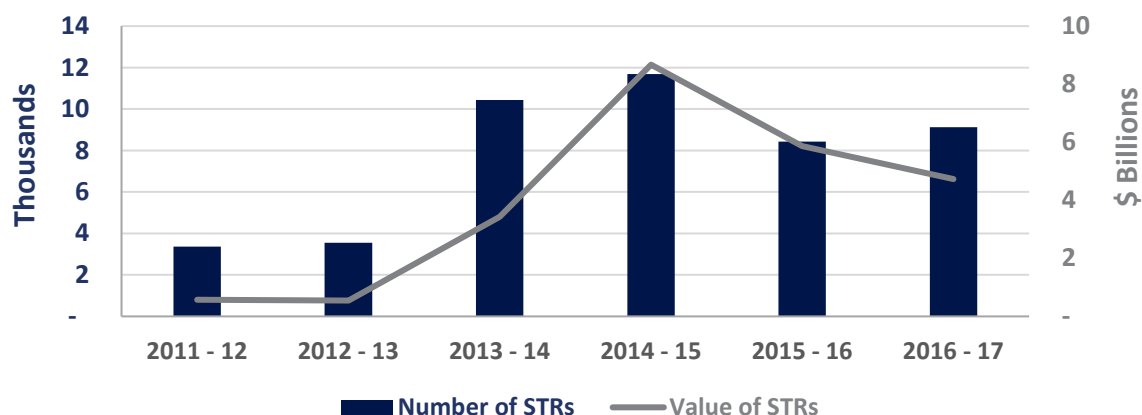
Domestic money laundering threat	The major groups of crimes known to generate money laundering domestically are drug, fraud and tax offending. The FIU estimates that NZD 1.35 billion is generated annually for laundering, primarily from drug and fraud offending. This figure excludes transnational laundering 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 • dedicated money laundering networks, which may also seek to move funds through the 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 a significant increase in reporting to the FIU, both in terms of the number of reports and the value of reported transactions.

Graph i: STR reporting for financial years 2011-12 to 2016-17



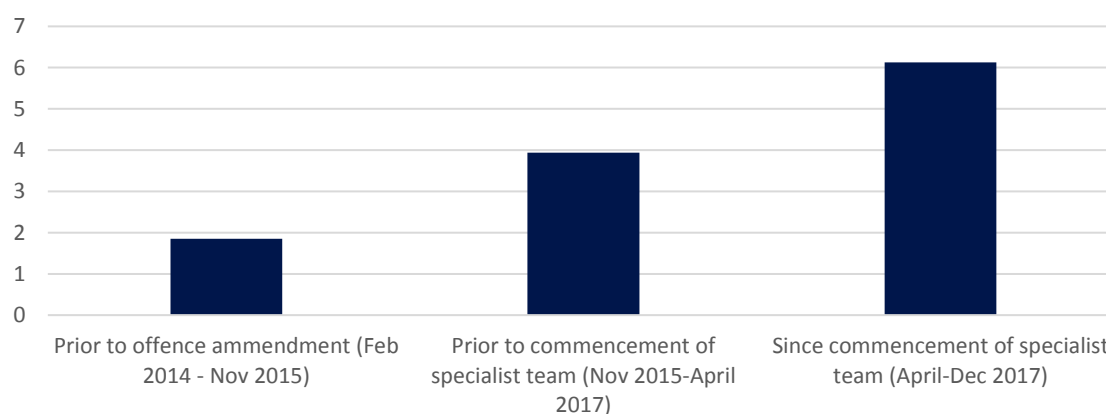
The Organised Crime and Anti-Corruption Legislation Bill received Royal Assent in November 2015. The Bill led to 15 amendment acts, most of which are already in effect. There were three AML/CFT-related amendments:

- 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 predicated 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 launched its first dedicated Money Laundering Investigations Team. This eight person team of detectives and specialist employees works 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.

Graph ii: Money laundering charges per month



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 such as measures relating to 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 RBNZ for banks, life insurers and non-bank deposit takers,
- The FMA 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 DIA for casinos, non-deposit taking lenders, money remitters, 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 New Zealand Racing Board as well as obliging cash transaction reporting for businesses dealing in high value goods (e.g. auctioneers, bullion dealers). These obligations come into force by a staggered implementation during 2018 and 2019. DIA is also the supervisor for the Phase 2 reporting entities. Phase 2 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,
- 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.

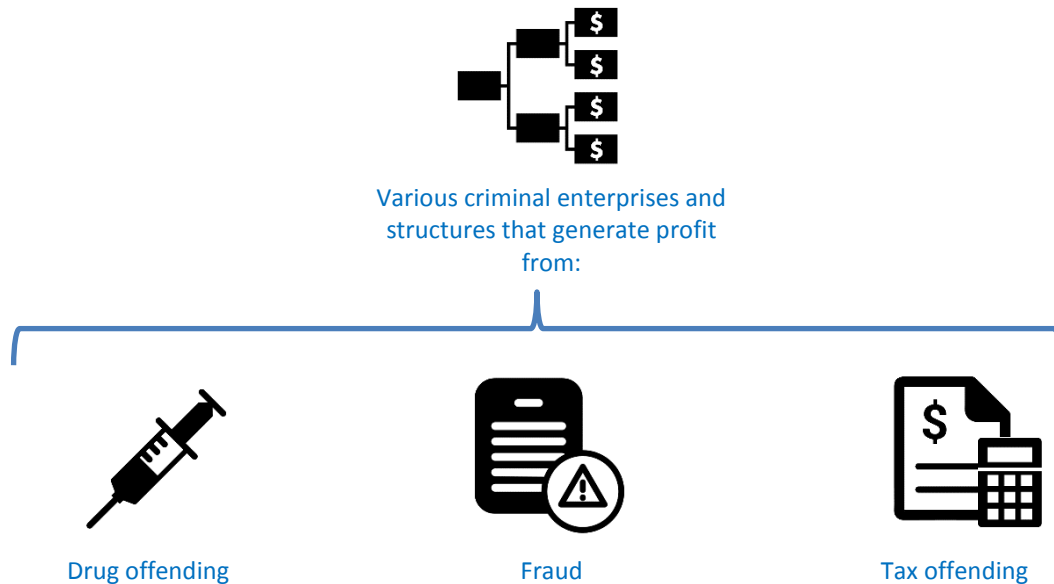
The highest priority observed vulnerabilities for New Zealand are:

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	Alternative methods of moving value and funds are highly vulnerable to displacement of illicit activity away from the financially regulated sector. 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 via new technology is closely related to the vulnerability to alternative methods of moving value and funds. New Zealand's exposure to high profile new payment technologies, including digital currencies, 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 provision of online alternative banking platforms nominally domiciled in New Zealand.
Gatekeeper professional services including formation of companies, trusts and charities	Currently there are low levels of AML/CFT controls of, and reporting by, New Zealand professional services providers. This 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. However, expansion of the AML/CFT regime to include professional services is expected to improve this situation as it is phased in from 1 July 2018.
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 from 1 November 2019 onwards.
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.

Until the Crimes Act was amended in 2015, a predicate offence was set as being any serious offence (those offences carrying a penalty of five or more years imprisonment). This was amended in 2015 to be any offence.

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.

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.³ 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

³ John Walker "The Extent of Money Laundering in and through Australia in 2004", RMIT University and AUSTRAC, 2005

million). 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.

The actual transactional value of money laundering is likely to be several times the NZD1.35 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

The above estimates and cases analysed as part of this risk assessment have identified three main domestic predicate offence types in New Zealand; drug offending, fraud and tax offending. The analysis drew heavily on cases from New Zealand Police Asset Recovery Units (ARUs) 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 principal 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, generated through a predominantly cash business model with payments in cash 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.

Fraud can potentially generate higher value transactions of illicit funds per offender from a wide variety of predicate offending.

Tax offending



The abuse of tax and superannuation systems 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.

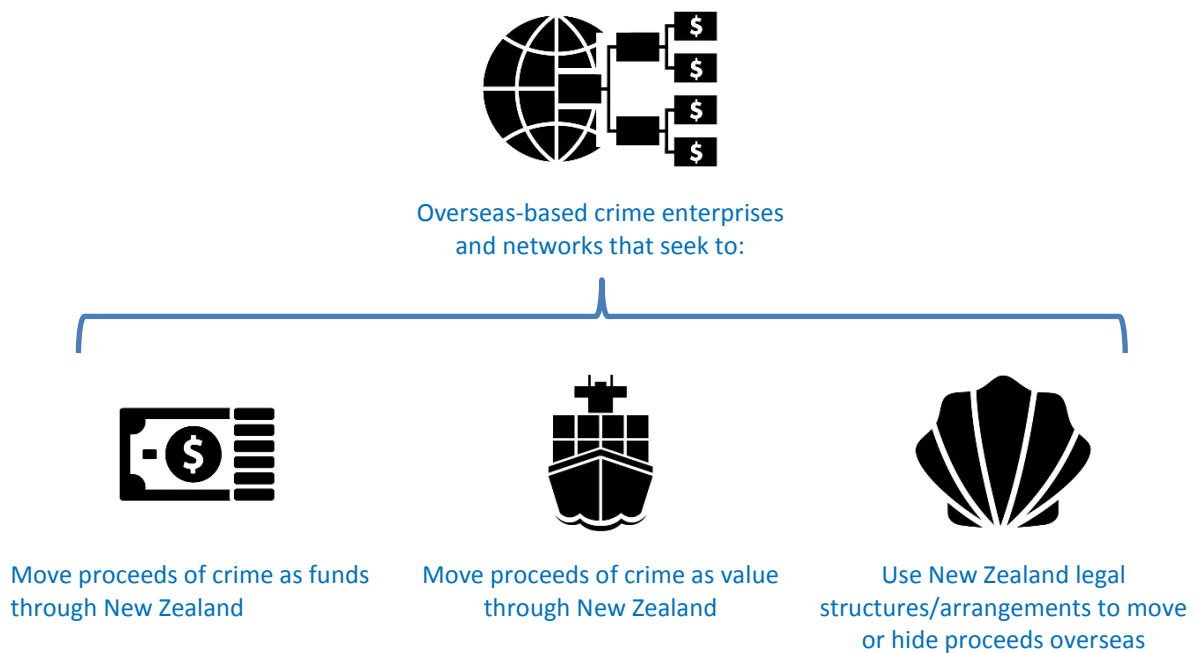
The table below details the profile of money laundering by each of the major predicate offence types identified through the cases analysed in this assessment.

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 dealers in high value commodities 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 in the vehicle used to commit predicate offence (i.e. in business, company or market)
		Layering	Use of companies and businesses, likely to be professionally facilitated; Movement of funds offshore through complex networks set up by professional money laundering facilitators
		Integration	Into real estate, high value commodities
Tax offending	Self-laundering; Laundering by professional service providers	Predicate offending	Non-cash based
		Placement	Likely to occur 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 complex networks set up by professional money laundering facilitators. Also via gambling and co-mingling with apparently legitimate business earnings
		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 on international exposure considers New Zealand's vulnerability to these threats as well as to external terrorism financier and to 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 type 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 can drive 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 terrorism financing. This transnational threat environment exposes countries with lower domestic threats, such as New Zealand, to new crime types, such as corruption, and sophisticated money 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 by the requesting jurisdictions. 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 various alternative banking platforms⁴, 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 with New Zealand. 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, businesses, alternative remittance⁵ and casinos.

⁴ 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.

⁵ 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.

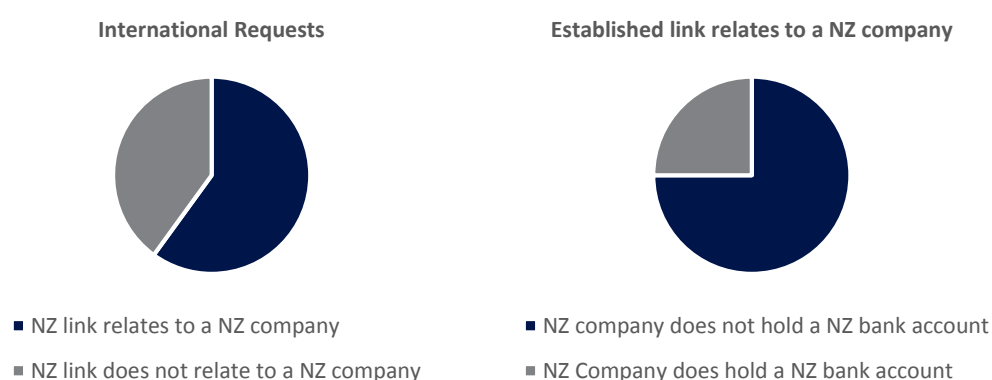
Methods associated with known threats

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

Requests from overseas partners for information to the FIU indicate that there is a risk that the financial system is abused 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 more sophisticated 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 United Kingdom and the United States. 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 significant money laundering threat.

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)

TERRORISM FINANCING THREAT

Figure iii: Terrorism financing threat profile:



Limited threat of domestic terrorism



Few terrorism financing reports



Threats in the international environment

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, terrorist 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 terrorist 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. Given the absence of evidence of significant domestic support for terrorism, it is likely that the domestic terrorism financing risk is lower than partner countries. However, like any country, New Zealand remains exposed to the financing of terrorism overseas.

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. 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

Two types of offshore groups pose a 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.

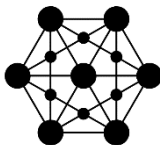
Although New Zealand's limited experience may make specific actions to target the terrorism financing threat difficult, AML/CFT controls to counter transnational laundering, combined with other activities to counter the threat of radicalisation, are likely to mitigate the deficiencies of specific counter measures for terrorism financing, provided counter measures are flexible enough to counter both threats.

Table iii: types of terrorism financing threat

Groups able to inspire support through ideology

	• The threat of radicalised individuals inspired by terrorist ideology 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 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 that 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.
---	--

Well-resourced groups with established networks

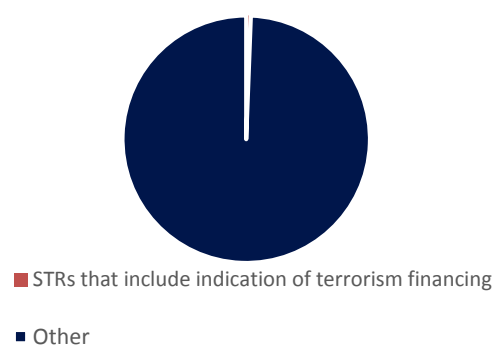
	• Abuse of New Zealand's vulnerabilities to transnational laundering by terrorism financing networks may involve movement of large sums of funding for terrorism. State-sponsored groups or groups operating with state-like infrastructure are more likely to have access to such networks. As with high-value international money laundering, this may occur through the abuse of New Zealand legal persons, alternative banking platforms, or New Zealand address services without transactions moving through New Zealand. • Given the relatively benign terrorism risk environment, the specific risk to New Zealand is more likely to be that terrorist networks operating offshore would exploit such New Zealand structures with only unwitting or reckless involvement of facilitators in New Zealand.
---	--

Suspicious transaction reporting on terrorism financing

For the period from the commencement of the AML/CFT Act on 30 June 2013 to 30 June 2017 the FIU received a total of 156 STRs that have an indication of a possible relation to terrorism financing, which is 0.392% of all processed STRs. These reports are illustrated in the graph to the right.⁶

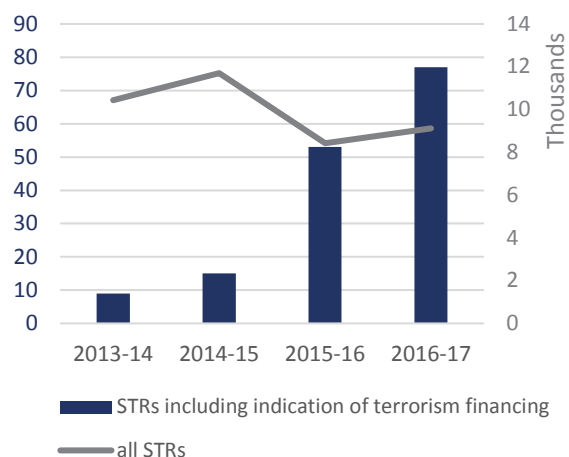
The total number for each financial year includes suspicious transaction reports that were assessed by reporting entities as relating to possible terrorism financing, as well as those suspicious transaction reports assessed by the FIU as relating to possible terrorism financing.

Graph iv: STRs potentially relating to terrorism financing



⁶ STRs that include indication of terrorism financing shown here at 1500% actual figure to be visible

Graph v: STRs indicating terrorism financing



The STR statistics suggest that there has been a slight increase in STRs related to possible terrorism financing. The increase in STRs that are suspected of relating to terrorism 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.

This increase in reports including indications of terrorism financing follows the global trend for increasing reporting. The underlying increased awareness should not in itself be read as a change of the terrorism financing threat.

Income generation

FATF and members of its global network have undertaken focused research on terrorist financing methods and risks⁷ 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.

Legitimate earnings

Relatively small amounts of funds may be involved in terrorism financing, which terrorist sympathisers may simply divert from legitimate income. In particular, 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 organisations⁸.

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 networks⁹.

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.

⁷ FATF "Emerging Terrorist Financing Risks", FATF October 2015

⁸ Ibid.

⁹ 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%932006-12-2015.pdf

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, as discussed below the Charities Service works closely with the sector so that charities exposed to such risks are able to mitigate them.

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 terrorism¹⁰. Foreign terrorist fighters and other terrorists have also used loan fraud to fund terrorist activity¹¹. 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. 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.

Kidnapping for ransom is particularly relevant to New Zealand as a kidnapping can occur in one jurisdiction and the ransom payment be made in another. There have also been examples of funds raised by relatives (on behalf of the victim), through the sale of assets and loans, and through the use of trusts to store funds for a ransom payment.

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.

However, 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.

¹⁰ FATF "Emerging Terrorist Financing Risks"

¹¹ Ibid.

Movement of funds

Funds transfers through banks

Funds transfers through banks continue to be the most common way to move money internationally for any purpose, including terrorism financing. The banking sector remains vulnerable, 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 organisations¹².

Australia has reported cases that have involved structured deposits of cash into bank accounts, followed by international funds transfers out of Australia¹³. 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 associated debit card 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 and, 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 license¹⁴. For example, the FATF report on Da'esh¹⁵ 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

Cash continues to be a widespread aspect of terrorist operations, and physical transportation of cash, especially foreign currency such as EUR and USD, across an international border is still very common¹⁶. 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 into an overseas bank account with low AML/CFT controls, then withdrawn from an ATM in a third jurisdiction and diverted to terrorism without a record trail.

Although the New Zealand cash economy is smaller than many similar-sized countries, cross-border cash movements valued over NZD 800 million equivalent 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

¹² Ibid.

¹³ Ibid.

¹⁴ FATF "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", FATF February 2015

¹⁵ Ibid.

¹⁶ FATF "Emerging Terrorist Financing Risks"

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 have been transported to high-risk jurisdictions.

Financial activity through high-risk jurisdictions

Terrorist financiers 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 terrorist sympathisers in exchange houses in Middle Eastern regional hubs have diverted the profits derived from money laundering to fund terrorist causes¹⁷. 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 scheme 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 both terrorism financiers and money launderers, as was seen in 2014, when 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 that 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" activities which are operating in close proximity to an active terrorist threat¹⁸. 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 conducted 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.

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.

¹⁷ 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>

¹⁸ 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

SECTOR RISK ASSESSMENTS

In 2011 each of the AML/CFT Act Sector Supervisors; the RBNZ, DIA and the Securities Commission (now the FMA); 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. In 2017, the supervisors updated their assessments drawing in part on the restricted version of this assessment. 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 upon which to base future risk assessments. The interaction between the various assessments allows a top down and bottom up understanding of the money laundering and terrorism financing risks facing New Zealand. The relationship between the assessments completed by the separate sectors and the FIU is shown in the diagram 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 on customer due diligence conducted by a third party;
- anonymity (of beneficiaries, beneficial owners etc.);
- attitude that customer due diligence is complete if the customer holds an account;
- gifting of units;
- dealing with high risk jurisdictions;
- offending (i.e. fraud and corruption) within sector;
- omnibus accounts;
- trusts;
- lack of price transparency;
- rogue or complicit employees;
- failure to identify people who control funds;
- 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;
- sympathy to a terrorist group's cause;
- 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 iv: Findings of sector risk assessments in 2011, 2014 and 2017

RBNZ supervised sectors		
Sector	2011 rating	2017
Registered banks (overall inherent rating)	HIGH	HIGH
• Retail		HIGH
• Business/Commercial		HIGH
• Wholesale/Institutional		MEDIUM
Non-bank deposit takers	MEDIUM	MEDIUM
Finance companies	MEDIUM	LOW
Building societies	MEDIUM	MEDIUM
Credit unions	LOW	MEDIUM
Life insurers	LOW TO MEDIUM	LOW

FMA supervised sectors		
Sector	2011 rating	2017 rating
Derivatives issuer	MEDIUM TO HIGH	HIGH
Brokers and Custodians	MEDIUM	MEDIUM TO HIGH
Equity crowd funding platforms	n/a	MEDIUM TO LOW
Financial advisors	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	n/a	MEDIUM TO LOW
Licensed supervisors	n/a	LOW
Issuers of securities	LOW	LOW

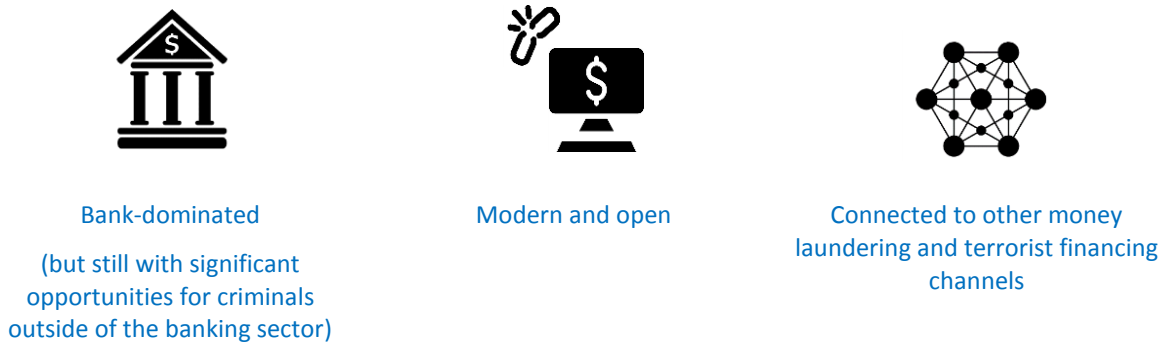
DIA supervised sectors in phase 1 ¹⁹		
Sector	2011 rating	2014 rating
Money remittance	HIGH	HIGH
Trust and company service providers	HIGH	HIGH
Casinos	MEDIUM TO HIGH	HIGH
Currency exchange	MEDIUM	MEDIUM
Safe deposit boxes	LOW TO MEDIUM	LOW
Cash transport	LOW TO MEDIUM	LOW
Non-bank credit cards	LOW	LOW
Factoring	LOW	LOW
Debt collection	LOW	LOW
Payroll remittance	LOW	LOW
Non-bank non-deposit taking lenders	LOW	LOW
Financial leasing	LOW	LOW
Tax pooling	n/a	MEDIUM
Stored value instruments	n/a	LOW

DIA supervised sectors in phase 2		
Sector	AML/CFT commencement	2017 rating
Lawyers	1 July 2018	MEDIUM-HIGH
Conveyancers	1 July 2018	LOW
Accountants	1 October 2018	MEDIUM-HIGH
Real estate agents	1 January 2019	MEDIUM-HIGH
High value dealers	1 August 2019	MEDIUM-HIGH
Racing board	1 August 2019	MEDIUM-HIGH

¹⁹ An updated SRA is due to be published in 2018

FINANCIAL SECTOR VULNERABILITY

Figure v: Financial sector vulnerability profile:



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.²⁰ While this significantly reduces the national money laundering and terrorism financing risk, it potentially increases the criminal incentive to abuse the financial sector.

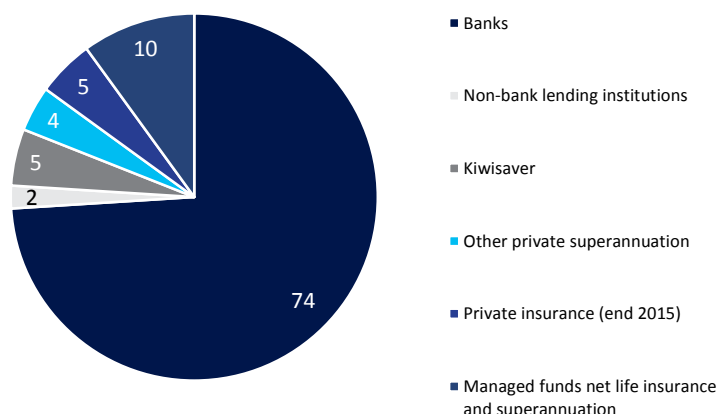
Bank-dominated sector

New Zealand's financial system is dominated by the banking sector, which accounts for about 75 percent of total financial assets.²¹ Compared to other countries, this is a high proportion of financial assets for which New Zealand banks must account. Annual reporting to the Sector Supervisors indicates that the value of transactions through the banking sector totals 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).

²⁰ 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

²¹ "New Zealand Financial System Stability Assessment" ("FSAP Report") International Monetary Fund 10 April 2017

Graph vi: Financial Systems in New Zealand
(in percentage of total financial assets, September 2016)



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 2016.²² As such, a significant portion of inherent money laundering and terrorism financing risk in the financial sector is concentrated on a small number of institutions. These banks' assets are focused on lending to the domestic private sector, and particularly to the residential real estate market and farms. As real estate has been identified as 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.

New Zealand banks also offer a full suite of other retail services, many of which are vulnerable to money laundering.²³ These services may be used to make large illicit transactions running a full spectrum; from large, supposedly business-related transactions, to numerous small-scale cash placements.

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.

In recent years the understanding of risk posed to derivative issuers and brokers/custodians has increased, in particular these sectors' vulnerability to fraud and tax offending at all stages and drugs offending at layering and integration. 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 funds²⁴ which are assessed by the FMA as lower risk²⁵. As shown in the graph below, the value of assets in managed funds is significantly higher than any other non-bank financial sector.

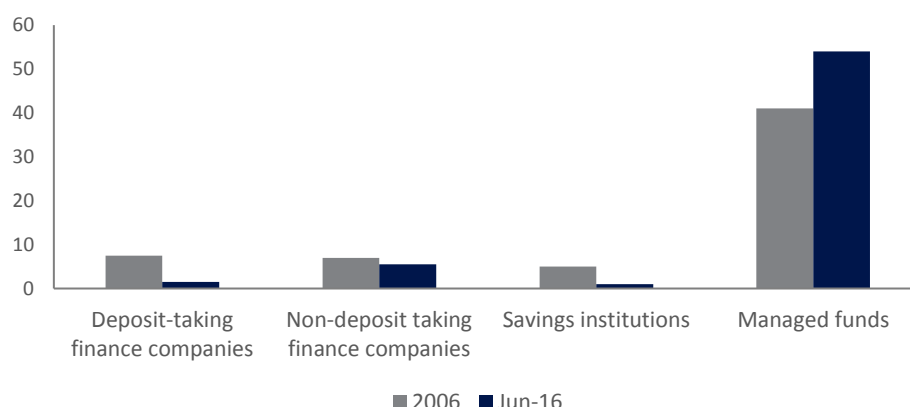
²² Ibid.

²³ "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

²⁴ FSAP Report

²⁵ "Anti-money Laundering and Countering Financing of Terrorism – Sector Risk Assessment 2017" Financial Market Authority 2017

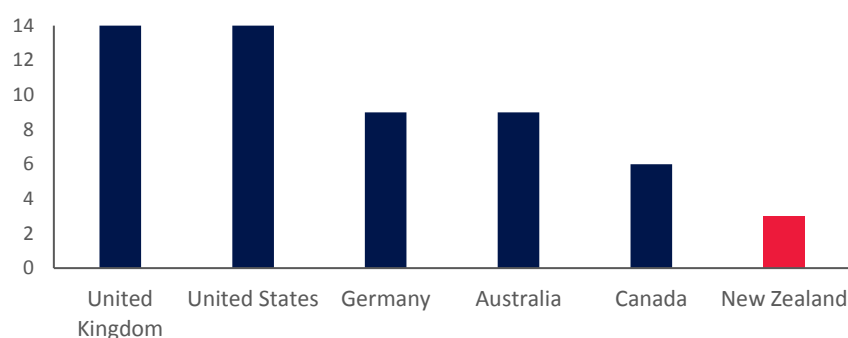
Graph vii: Assets of Non-bank and Other Financial Institutions
(in percent of GDP)



Growth in lower-risk KiwiSaver schemes, partial privatisation of state-owned enterprises, and low global and domestic interest rates have driven increases in stock market capitalisation. Between 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 Australia²⁶.

New Zealand's insurance sector is 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. Life insurance, which is the only supervised insurance sub-sector, has also been assessed by the RBNZ as being low-risk²⁷.

Graph vii: Private Insurance Premiums in Selected Countries
(in percent of GDP, 2014)



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 and bank and other financial accounts do not retain greater privacy rights than personal information held by other entities. The

²⁶ "Market Capitalisation of Listed Domestic Companies (%GDP)" World Bank Data
<https://data.worldbank.org/indicator/CM.MKT.LCAP.GD.ZS>

²⁷ FSAP Report

New Zealand Privacy Act 1993 specifically allows sharing of information, including financial information, for law enforcement purposes while the AML/CFT Act and the Criminal Proceeds (Recovery) Act 2009 (CPRA) 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 and are symptomatic, and a driver, of the move away from the cash economy. While this helps to reduce the macro-level exposure to cash laundering, 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 terrorist financiers may be attracted by the speed and convenience of new payment technology enabled transactions as such convenience 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 increases 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 technologies 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 financial institutions may be exposed to open-loop products, such as travel cards, issued by other institutions. Formal virtual currency exchanges have only a small presence in New Zealand, although a small number of new institutions are seeking to establish a regulated market. Individuals who operate outside of regulations, as informal exchanges using bank accounts, expose institutions to risk and provide criminals opportunities to obtain virtual currency for illicit purposes. Mobile phone services are limited to apps to facilitate payment through banking or remittance networks, and true mobile phone-based money transfer services have not emerged.

GATEKEEPER PROFESSIONALS VULNERABILITY

Figure vi: Gatekeeper professional vulnerability profile:



Lawyers, conveyancers, accountants and real estate agents provide a 'gatekeeper' role in providing professional services to clients. Such services 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 real estate;
- creating of trusts and companies;
- managing trusts and companies;
- managing client affairs; and
- transferring ownership of assets to third parties.

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 v: Overview of money laundering risk to gate keeper professional 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 complex, and cross-jurisdictional trusts or companies in another person's name 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. Standards enforced by the New Zealand Law Society prohibit lawyers acting in a way that unwittingly facilitates criminal offending. 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. This 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 Chartered Accountants Australia New Zealand and the New Zealand Association of Certified Public Accountants (NZACPA). These standards include that accountants must not act in a way that facilitates criminal offending.

In New Zealand, real estate agents are required to hold a current licence, regulated by the Real Estate Agents Authority through a Code of Conduct. They are subject to control through the Real Estate Agents Act 2008, and the FTRA.

Although these measures to promote professional integrity are in place, legislation currently enforce does not include a supervision regime to specifically mitigate the money laundering risk to lawyers, conveyancers, accountants and real estate agents. Low rates of suspicious transaction reporting by professional services indicate that the general measures are 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 transaction reports from lawyers, and 7 suspicious transaction reports from accountants (who are not captured as other types of AML/CFT reporting entities such as financial advisors). This vulnerability will be addressed by the introduction of the second phase of AML/CFT reforms over 2018-2019.

In addition, regulatory vulnerability in relation to companies and trusts creates further incentives for criminals to use professional services. Companies and trusts can be quickly and cheaply set up to obscure beneficial ownership. Criminals can also 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, which incentivises criminals to seek professional services 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. These services remain available online or through professional introductions, and in some cases are marketed to offshore clients. In many instances, the anonymity/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 is a common method employed by money launderers. Despite high levels of professional integrity and FTRA obligations, use of professionals' trust accounts is a common money laundering method employed in New Zealand. Trust accounts 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 schemes 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 a consistently high number, and value, of assets pertaining to real estate restrained and forfeited in New Zealand. The inherent vulnerability for conveyancing and real estate transactions is high, and is exacerbated by the large annual volume of valuable asset transfer.

The specialist knowledge needed to complete a real estate transaction means that New Zealand real estate transactions are generally facilitated by experienced lawyers or conveyancers. In particular, the requirement from the 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 (lawyers and accountants)

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 legal arrangements 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;
- 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 professionally facilitated cases examined in the NRA, while hiding beneficial ownership using methods such as trust structures was observed in all of the sample of real estate cases.

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 can be made quickly and frequently.

Typically, a money launderer arranges for a professional to set up a company or trust, then act in a proxy role. The money launderer may otherwise arrange a third party to act in this role, which can include acting as a trustee, nominee resident director, or nominee shareholder. Money launderers, and 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.

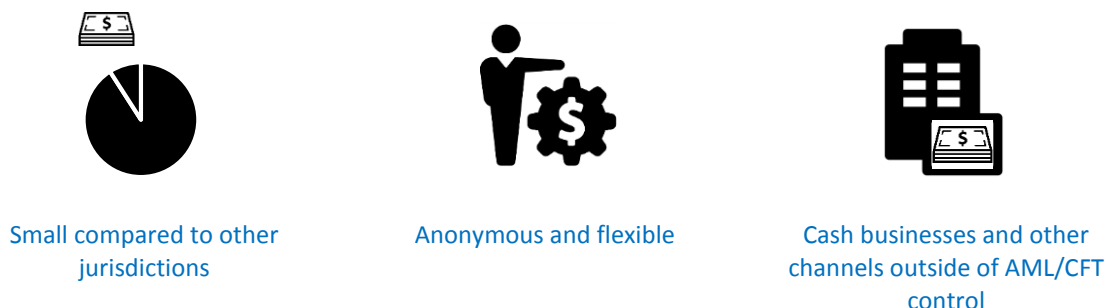
Services to overseas customers and purchasers

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:



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 presents 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.

Criminals need to place cash into the formal financial system to enjoy the profits from crime and 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.

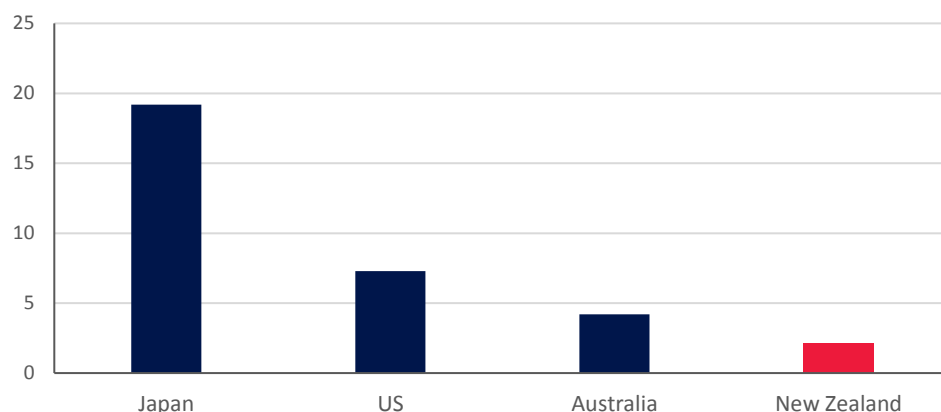
Once proceeds of crime that were generated in cash have entered the financial system, the criminal origin may be obscured and criminals may have new opportunities to facilitate further offending. Placement can hinder investigations by providing criminals various options to conduct transactions that appear 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 along with suspicious transaction, border cash and large cash transaction reporting requirements. Offending using cash is highly visible, and transactions involving cash are frequently identified in STR 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 require maintained 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 Japan²⁸.

Graph viii: cash in circulation
(as percentage of GDP 2016)



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 2015²⁹, 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 strengthening of controls has allowed increases in the detection of cash placement activities. Commencement of the AML/CFT Act and goAML³⁰, has further allowed the FIU to improve STR reporting and identify structured cash deposits and long-term activities previously undetected. The introduction of large cash transaction reporting will again lead to growth in 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 indicates where laundering of cash is available in the supervised sectors. The findings of the cash risk assessment are summarised overleaf.

²⁸ "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/>

²⁹ Ibid.

³⁰ STR 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 vi: 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	The majority of money remittance business is cash intensive 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 withdrawal 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 sectors that will be supervised in phase 2

In addition, the sectors currently outside of AML/CFT supervision that will be 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 vii: Summary of findings of the cash risk assessment in phase 2 sectors

Sector	Cash services	Money laundering stages
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 by acting 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 and without customers using the formal banking system. The diversity of geographic service, cultural norms and transfer methods used can make regulatory control challenging. While these services are subject to the AML/CFT Act, some unregistered services may operate across New Zealand 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 and/or law enforcement. 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.

The business industry may also provide access to other facilitators of crime. Transport companies, pharmacies, prostitution and bars may all be used to facilitate trafficking and sale of illicit drugs.

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 disadvantage legitimate competitors. Left unchecked, widespread criminal infiltration of an industry may stifle innovation ultimately leading to poor service to customers, damage to local economies and potentially making 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 used in proliferation, may be layered through the business creating a supposed reason for payments.

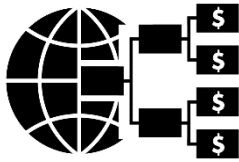
Private high value good transactions

One of the easiest and most common 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 commodities that are transportable, maintain or increase value, and are transferable from person to person. A wide range of high value goods have been identified in New Zealand asset recovery cases, including art and antiques, jewellery and watches, precious metals and stones, and vehicles.

Criminals who need to place a significant value of proceeds by purchasing high value goods are likely to resort to buying goods from some form of dealer whereas smaller values of cash may easily be used to purchase high value goods through private sales. The value of goods may be recapitalised through further uncontrolled trading. However, significant sales of high value goods may cause the launderer to be captured as a second hand dealer and subject them to regulatory control increasing the risk of detection.

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. 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 in international cases relating to tax offending, money laundering, investment fraud and smuggling of illegal goods.

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 by the FIU and DIA for AML/CFT enforcement, is set to mitigate issues caused by beneficial ownership.

Professional facilitation – availability of services, regulation and integrity

TCSPs, legal practices and accountancy firms provide many services, such as online company and trust formation, and many actively market to offshore customers. In some instances, the privacy and secrecy of services is promoted which is attractive to transnational criminals. New Zealand professionals offer overseas clients all of the high-risk legal services below, identified by the FATF:

- 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 affairs³¹.

The high level of integrity of New Zealand's professionals may partially mitigate the risk of professional facilitation of transnational money laundering. However, until Phase 2 reforms address lower levels of AML/CFT controls and understanding, the sector's inherent vulnerability to money launderers and terrorist financiers will be exacerbated.

Bank secrecy

As discussed in the Financial Sector Vulnerability 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. In addition, New Zealand has specific legislative mechanisms to provide 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 Business³² rankings due to ease of doing business and comparatively low business costs. The straightforward, business-friendly taxation system that supports capital development and international investment may also be attractive to transnational money launderers and terrorist financiers. Unlike many countries, New Zealand does not have currency controls and does not tax movement of capital³³. 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.

There are several major trading banks and numerous other banking institutions in New Zealand. 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 easy³⁴. Although geographically isolated, New Zealand's modern communications make movement of capital, including illicit capital, easy.

³¹ "Money Laundering and Terrorism financing Vulnerabilities of Legal Professionals", FATF report, June 2013

³² "Doing Business" <http://www.doingbusiness.org/rankings> World Bank

³³ "Why Invest Here?" New Zealand Trade and Enterprise <https://www.nzte.govt.nz/en/invest/new-zealands-investment-advantage/>

³⁴ Ibid.

Limited financial markets

While the New Zealand economy is open and easily accessible, the options for layering and integrating 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. New investment markets are emerging and investment markets such as the stock market are growing. Nonetheless, given the low level of diversification, the IMF notes that New Zealand investment remains heavily focused on real estate.

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, more recent research has seen this as a factor that will 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 small 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).³⁵ 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

Only a handful of alternative remittance operators openly operate in New Zealand and the availability of alternative remittance is therefore difficult to assess. Anecdotal experience indicates that there is an alternative remittance sector acting at least partly out of sight of the AML/CFT regime. These types of operations would present a particular vulnerability to offshore illicit capital flows; however, the extent of this vulnerability remains unknown.

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. 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.

The availability of alternative banking, and the ease with which platforms are set up, may allow criminals to establish platforms, facilitate offending and dismantle the structure before suspicious activity can be detected.

Trade

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

The long-term trend in New Zealand trade is a 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

³⁵ Schneider, Buehn and Montenegro

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:

- 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 withdrawals and remittance of cash thereby breaking 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 SRAs. These 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 viii: 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 ix: 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, making them attractive to money launderers and terrorism financiers.	NZD 150-200 million	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 instead provide a company or trust structure that is used to 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
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. Like money remitters, casinos also combine 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 financiers.	NZD 14.5 million in 2009/10 from total sector of NZD 465 million	High	Moderate
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 trade-based money laundering)

Table x: 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			
The majority of international payments are made via banks and these make up a significant proportion of the banks daily business activities. One factor that will increase the risk of international payments is transactions with higher risk countries. Once international wire transfer reporting commences, strategic analysis of payments to higher risk jurisdictions will be possible.	Estimated NZD 4.5 billion in international retail transactions per day in 2011 ³⁶	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

³⁶ RBNZ letter to Ministry of Justice 4 April 2012

In addition to the supervised sectors, several non-supervised sectors are highly exposed to international payments.

Table xi: Summary of international vulnerability of non-supervised sectors

Non-supervised sectors			
Description	Value of international payments through sector	Indicators in transnational cases	Vulnerability
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 is being increasingly 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

RISKS AND OUTLOOK

EMERGING RISKS AND ONGOING ISSUES AND RISKS

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. Correspondent relationships are must be only entered into where the New Zealand institution is confident that the relationship does not create undue money laundering risk and that the respondent are trusted to take equivalent action to mitigate risk.
Displacement	It is likely that increased AML/CFT controls within the regulated sectors will require 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. FIU compliance activity has already detected some limited instances of institutions 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 opportunities to avoid AML/CFT controls by conducting illicit transactions through sectors that are outside of the AML/CFT regime, such as by placing cash in cash businesses or by purchasing assets rather than deposits at financial institutions. 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. It is also likely to include increased attempts to use services in less controlled sectors as intermediaries or a layer to interact with regulated financial sectors. In particular, until phase 2 reforms come into force, increased AML/CFT controls in other sectors are likely to lead to increased demand for professional services to circumvent AML/CFT controls or place layers between criminals and institutions conducting AML/CFT controls. In extreme cases, criminals may establish criminal services expressly to facilitate illicit 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 highlighting that the practice of de-risking a whole class of customer, rather than managing the risks posed by individual customers, was not a proper implementation of the risk-based approach. The FATF further stated 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 as well as the value of money remittance occurring in non-regulated sectors, which creates 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.

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 be harm to the community from predicate offending that has a monetary cost 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. It is possible that if New Zealand suffered significant loss of reputation from any of the risks identified here, that the loss of confidence from international business partners would have an economic impact.

Compounding risk – particularly in relation to professional services	
Risk of compounding vulnerabilities	It is likely that if offenders exploit multiple vulnerabilities simultaneously, 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 high level of 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.
Legal structures	Although successive mitigation measures have been, and will be, put in place (including Phase 2 reforms), residual risk will remain in relation to the 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 particularly relating 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 of involved sectors. In addition, there is a growing risk of transnational money laundering using New Zealand real estate investment. Phase 2 reforms will align the real estate sector and conveyancers with AML/CFT obligations, which will go some way to mitigate 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 control (including high value dealers until Phase 2 is completed), 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.
Risk that illicit cash purchases of high value goods are not detected	Similarly, until Phase 2 cash reporting commences dealers in high value goods are not subject to AML/CFT controls, except in so far as they deal with the financial sector. As with cash business transactions, detection of unusual transactions at the point a dealer interacts with a financial institution already occurs. However, there is a high level of risk that insufficient controls are applied and illicit activity at the micro level will go undetected. The criminal opportunities presented by vulnerabilities in this sector create a high level of risk to law enforcement objectives that domestic criminals will place, layer and integrate through high value goods.

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 legal structures or businesses to facilitate international payments which defeats the AML/CFT controls on international payments. Phase 2 reforms are being 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 understanding 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 lower overall level of terrorism financing risk than many of our partners. 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.

GLOSSARY

AML/CFT	Anti-money laundering and countering of financing 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 service
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
REAA	Real Estate Agents 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
STR	Suspicious transaction report
TBML	Trade-based money laundering
TCSP	Trust and company service provider
UNODC	United Nations Office on Drugs and Crime