Financial Intelligence Unit

New Zealand Police

Quarterly Typology Report
Third Quarter (Q3) 2015/2016

(1 January – 31 March)

PREDICATE OFFENCE

(Issued June 2016)

INTRODUCTION

This report is the third Quarterly Typology Report (QTR) of 2015/2016 produced by the Financial Intelligence Unit (FIU), part of the New Zealand Police Financial Crime Group. As the QTR dissemination goes beyond law enforcement, the basics of money laundering, typologies and indicators will continue to be included to provide context to those new to the topic. **A list of typologies is contained in Annex 1.** This publication is comprised of open source media reporting observed within the last quarter. **Readers are strongly advised to note the caveat below.**

- **The open source nature of the material that this document is based on means that the veracity of the reports within this document may vary**
- **Views expressed within this document may not necessarily be those of the New Zealand Police or of any of its employees**
- **Reports within this document have been précised; additional information can be obtained via the hyperlinks if available**
- **The information contained within this document should NOT be taken out of context**

BACKGROUND

The Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act became law in October 2009. It is the result of a review of AML/CFT legislation and aims to assist in detecting and deterring money laundering, contributing to public confidence in the financial system and achieving compliance with the Financial Action Task Force (FATF) recommendations. The Financial Intelligence Unit produces the QTR as part of its obligations under section 142(b)(i)[1] and section 143(b)[2] of the AML/CFT Act 2009.

PURPOSE

The purpose of the QTR is to provide an accurate picture of current, emerging and longer term factors impacting on the AML/CFT environment. The QTR is intended to do the following:

- Examine money laundering and terrorist financing methods used in New Zealand and overseas
- Provide indicators of money laundering and terrorist financing techniques
- Highlight emerging trends and topics and share information in relation to AML/CFT and financial crime in general
- Provide typology case studies
- Update suspicious transaction reporting and Asset Recovery Unit activity

SCOPE

The QTR is a law enforcement document. However, it does not include sensitive reporting or restricted information and is published on the FIU website. The QTR is produced using a variety of sources and qualitative/quantitative data.

[1] Section 142(b) Financial intelligence functions of Commissioner: The financial functions of the Commissioner are to - produce guidance material, including: (i) typologies of money laundering and financing of terrorism transactions

[2] Section 143(b) Powers relating to financial intelligence functions of Commissioner: The Commissioner may - (b) share suspicious transaction reports, cash reports, suspicious property reports, and other financial information and intelligence with domestic and international authorities for the purposes of this Act and regulations

DEFINITION OF MONEY LAUNDERING

Under New Zealand legislation the money laundering offence is defined in section 243 of the Crimes Act 1961 and section 12b of the Misuse of Drugs Act 1975. The key elements of a money laundering offence are:

- Dealing with, or assisting in dealing with, any property for the purpose of concealing it
- Knowing or believing that such property is the proceeds of a serious offence, or being reckless as to whether it is the proceeds of a serious offence

DEFINITION OF TERRORIST FINANCING

Terrorist financing is criminalised in New Zealand under the Terrorism Suppression Act 2002. Under this legislation it is an offence to:

- Collect funds intended to be used for a terrorist act or intended for an entity known to carry out terrorist acts
- Knowingly deal with any property owned or controlled by a designated terrorist entity
- Make financial services available to a designated terrorist entity

Financial Intelligence Unit updates

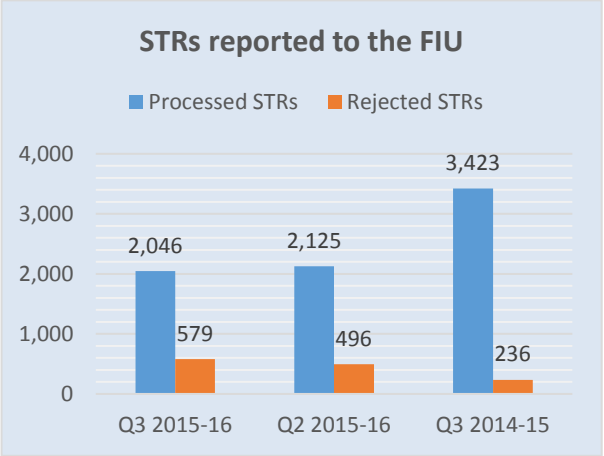
Information on the FIU is provided separately in permanent **Annex 2**.

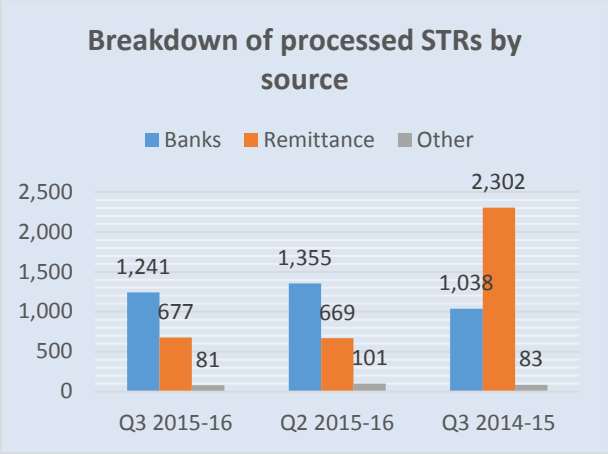
FIU QUARTERLY STATISTICS

Suspicious transaction reports (STRs)

The number of reported STRs processed by the FIU in Q3 2015-16 was 2,046. This total is 79 reports fewer than in Q2, but considerably lower than during the same Q3 last financial year.

The number of rejected STRs continued to increase in Q3 2015-16 to 579 from 496 in previous quarter. Comparing to the same Q3 last financial year, the FIU rejected about 60 per cent more reports.

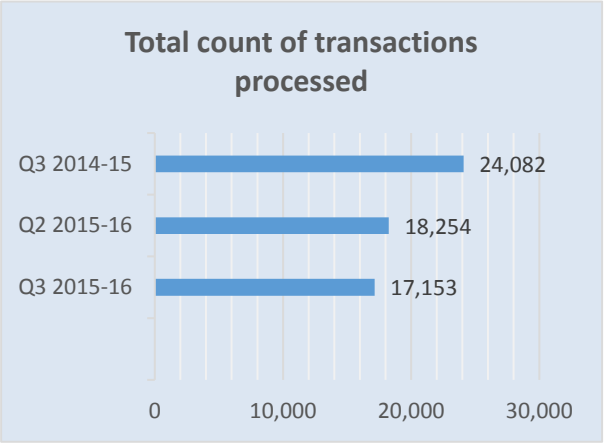




The majority of STRs are submitted by banks and remittance service providers. The breakdown of the processed reports for Q3 2015-16 is similar to Q2.

However, comparing Q3 number of processed STRs received from money remitters with the same Q3 last financial year, there has been a 71 per cent drop. This is due to continued improvement of transaction reporting processes by reporting entities which have led to fewer, but higher quality STRs as the AML/CFT regime has matured.

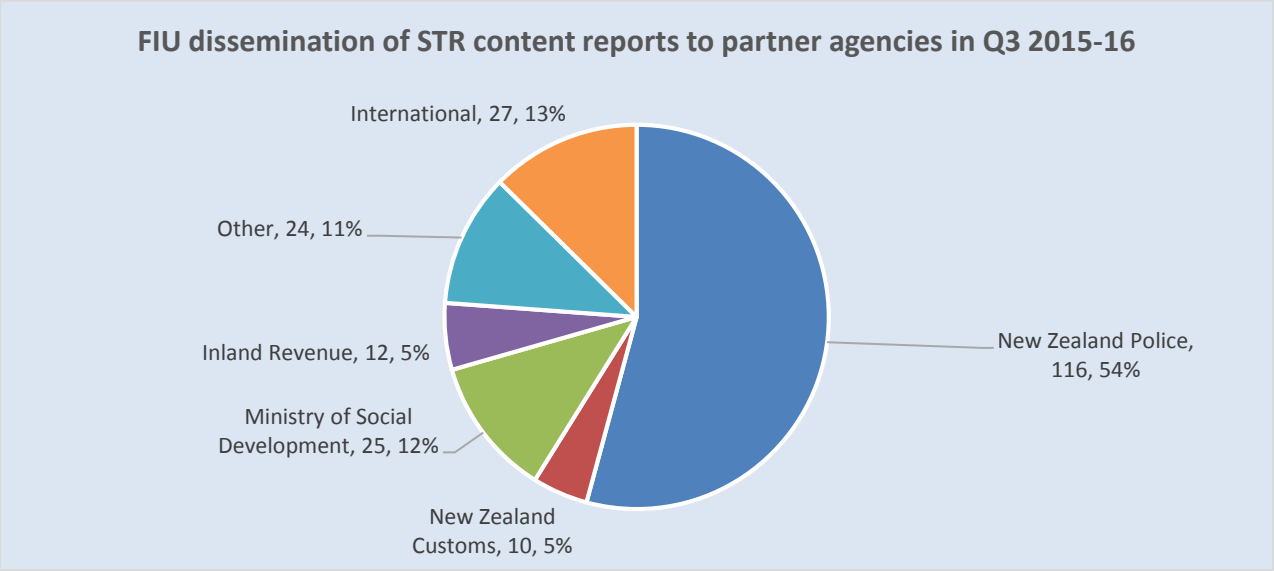
In Q3 2015-16 the number of transactions in accepted STRs has increased by 5,828 reports from Q2, and is 29 per cent more than in the same Q3 last financial year.

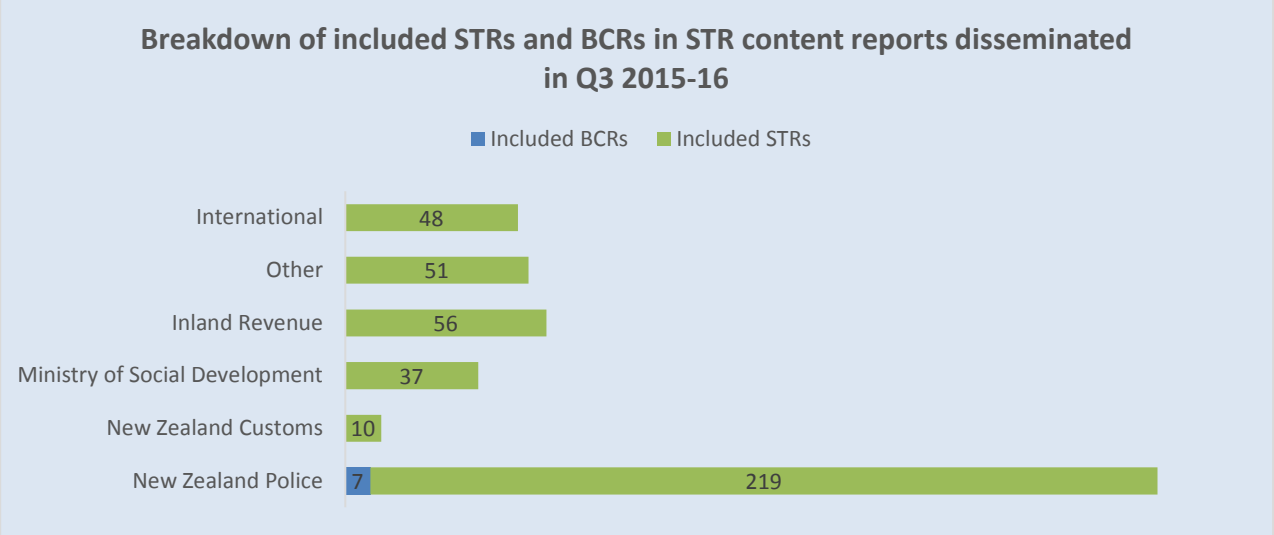


STR content reports

The FIU collects and collates information provided by external parties and reporting entities, especially banks and other financial institutions. After the required analysis, intelligence products such as STR content reports, STR spreadsheets and intelligence reports are sent to other investigative and intelligence units within Police, sector supervisors, domestic partner agencies and to relevant international agencies.

An STR content report is a basic intelligence product that comprises of the reporting entities grounds for suspicion, the reported transactions and biodata. Often the FIU will add additional value to the STR content report by including information held in Police intelligence systems. These STR content reports primarily contain data from the reported relevant STRs, and also border cash reports (BCRs) and suspicious property reports.

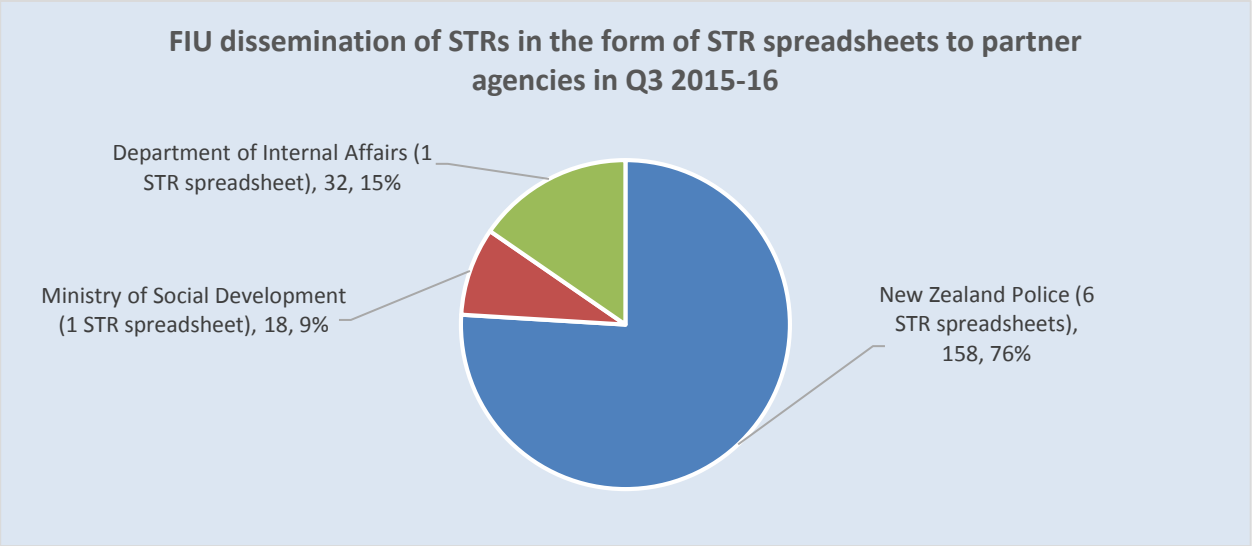




In Q3 2015-16, the FIU disseminated a total of 214 STR content reports, 54 per cent of which were sent to various New Zealand Police units. The other recipients included domestic and international law enforcement agencies. There were a total of 421 STRs and 7 BCRs included in these STR content reports for this quarter.

STR spreadsheets

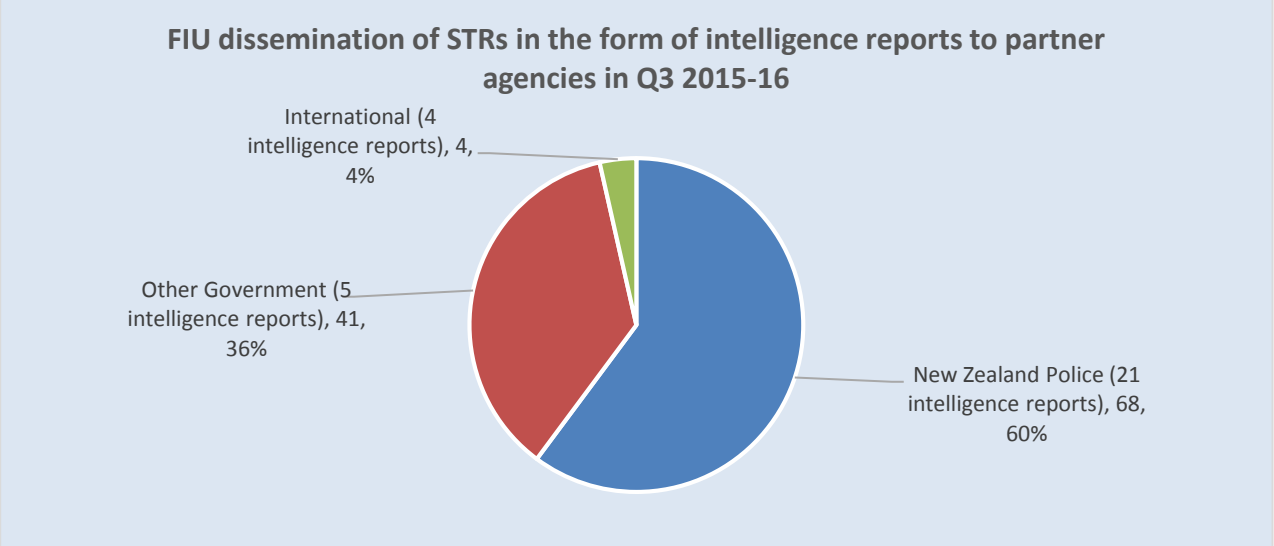
An STR spreadsheet is a collection document for the detection, investigation, and prosecution of offences by different prosecuting authorities within the New Zealand government. Once the collection phase is completed, the STRs are exported to a spreadsheet in their raw form. With the exception of the Police spreadsheets they do not have any added value from Police intelligence systems.



The FIU distributed 8 STR spreadsheets in Q3 2015-16 to three partner agencies, which included raw data of a total of 208 STRs.

Intelligence reports

Intelligence reports are produced by the FIU intelligence analysts and they involve a wide collection of data including information from the reported STRs. These reports contain data analysis of the STRs, drawn inferences and recommendations made to the intended recipient.



During Q3 2015-16 the FIU has produced 30 intelligence reports which contained analysis of a total of 113 STRs.

FIU UPDATES

FIU Conference 2016

Preparation for the annual FIU Conference being held at Te Papa, Wellington on 14 and 15 September 2016 is progressing well. The theme this year is "Private Sector Engagement/Partnership".

FIU have confirmed the majority of the speakers which includes an international component. The presentations will link to the theme in respect of how this disrupts or affects money laundering, terrorist financing, bribery, corruption and other predicate offences. There will be two case studies presented and an opportunity for breakout sessions for the various sectors.

Registration papers will be available from early July. Please contact the FIU at FCG.Seminar@police.govt.nz if any questions arise about the conference.

Prescribed Transaction Reporting and goAML Upgrade

As part of the recent AML/CFT Amendment Act 2015, New Zealand reporting entities will be required to submit Prescribed Transactions Reports (PTRs) for international wire transfers of NZD1,000 or more and domestic physical cash transactions of NZD10,000 or more from 1 July 2017.

The IT project, as a result of this new legislation, will officially commence 1 July 2016. It will involve an upgrade of the goAML system (to Enterprise Edition), where the vendor is UNODC (United Nations Office on Drugs and Crime). The UNODC is expected to have staff in New Zealand during the first quarter of 2017 to help Police ICT with the design and implementation of goAML EE, in readiness for the increased volumes of reports beginning mid-2017.

Asset Recovery Units

The New Zealand Police Asset Recovery Units were established in December 2009 to coincide with the implementation of the Criminal Proceeds (Recovery) Act 2009 (CPRA). The CPRA established a regime for the forfeiture of property that has been directly or indirectly acquired or derived from significant criminal behaviour. It is intended to reduce the possibilities for individuals or groups to profit from criminal behaviour, to reduce the opportunities they have to expand their criminal enterprises, and act as a deterrent for criminal activity. There are four Asset Recovery Units (ARUs), based in Auckland, Hamilton, Wellington and Christchurch.

CRIMINAL PROCEEDS (RECOVERY) ACT 2009 (CPRA)

As at 31 March 2016, New Zealand Police held Restraining Orders at over an estimated **NZD270 million** worth of assets. Since CPRA came into effect, an estimated **NZD85 million** worth of assets have been subject to Forfeiture Orders. For the quarterly period ending March 2016, **NZD7.30 million** worth of assets were restrained, and **NZD2.93 million** were forfeited. The majority of restrained assets related to cases where **methamphetamine dealing** was the predicate offence.

NZD M	This QTR	Last QTR	Last Year
Value of Forfeitures[1]	**2.93**	**4.54**	**3.44**
Value of Restraints[2]	**7.30**	**46.44**	**2.22**
Fraud	-	1.05	-
Money Laundering	-	0.33	-
Tax Evasion	-	41.23	-
Drugs and other offending	7.30	3.83	2.22

[1]Value of Forfeitures is based on the date of the Forfeiture Order.

[2]Value of Restraints is based on the date of the Restraining Order, and in very rare cases, this might include assets that are no longer in restraint. For each CPRA case, a main predicate offence will be identified.

Note that these values are drawn from a dynamic database, where information about cases can be continuously updated.

OBSERVATIONS – CENTRAL ASSET RECOVERY UNIT

Introduction

CPRA is now seven years old and all Asset Recovery Units in New Zealand are seeing increased referrals with notable increases from government agencies outside of Police. For example, the ARUs have been able to forfeit illegal funds and assets from people involved in offending such as education fraud, fisheries exploitation, MSD fraud, people smuggling, and organised criminal entities involved in drug offending.

Co-mingling

A common theme is 'co-mingling' of funds, where illicit earnings are integrated with legal income, particularly from cash-intensive businesses that are used to disguise the source of such funds. This typology has been evident in several investigations, including one involving the commercial cultivation and sale of cannabis, people smuggling, and farming.

Stored-value cards

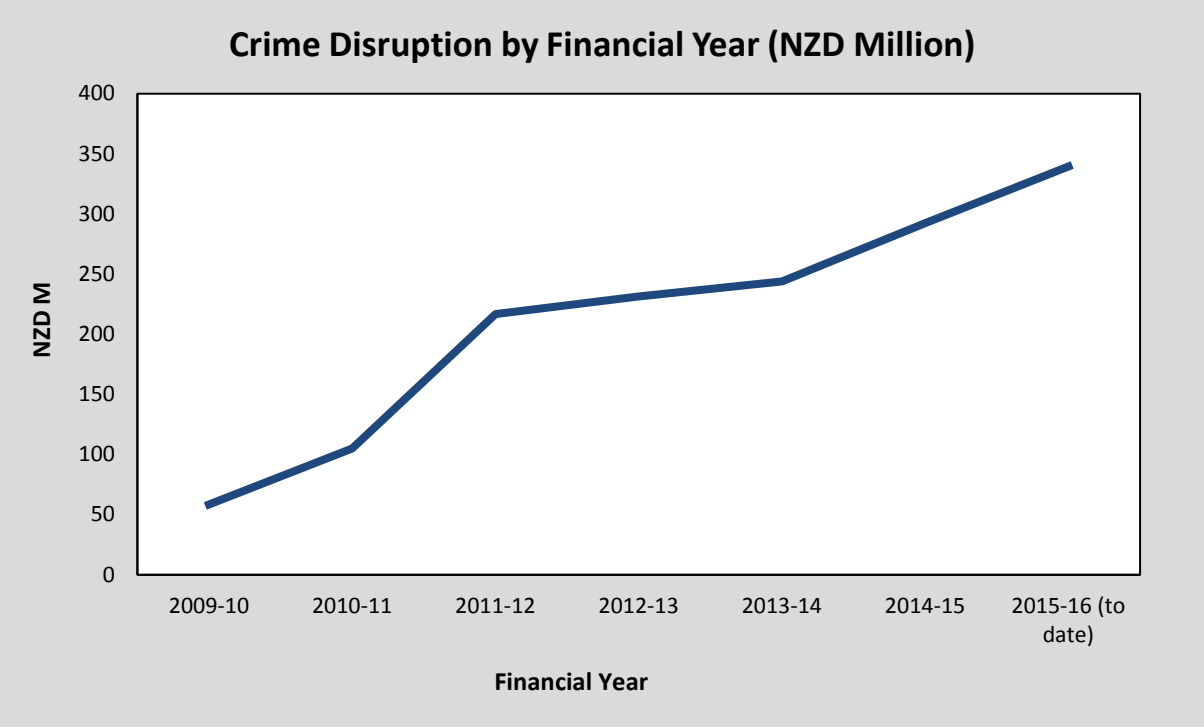
We are now seeing the frequent use of value cards (e.g., travel cards, 'Prezzy cards'), which are easily purchased with cash, easily transferrable, simple to use, and can be 'topped up'. The variety of cards on the market is a challenge, and staff are becoming more vigilant and aware of how these cards can be easily used for illegitimate purposes.

Other trends

False identities and laundering funds through those identities is a familiar, but popular, typology. Also, with the AML/CFT legislation, we have seen greater compliance within the financial sector, resulting in criminals finding it more difficult to introduce illicit funds. As criminals become more conversant with the legislation, we are noticing some interesting trends occurring in order to launder illicit funds gained from criminal enterprises. It is evident that 'cash is still king'. Criminals often try to hide their assets in "third party" names or nominees. Lastly, we are seeing an emergence of high-value, portable commodities, in particular bullion and jewellery.

CRIME DISRUPTION

According to the Proceeds of Crime Disruption Index (POCDI), every NZD1 worth of assets restrained contributes to an estimated NZD3.30 in crime disruption, and NZD3.50 for every NZD1 worth of assets forfeited. The below graph shows the estimated amount of crime disruption achieved since the CPRA was enacted, by financial year.



PREDICATE OFFENCE

DEFINING PREDICATE OFFENCE

A “predicate offence” is an offence whose proceeds may become the subject of any of the money laundering offences established under the United Nations Convention. Many countries already have laws on money laundering but there are many variations in the definition of predicate offences. Some countries limit the predicate offences to drug trafficking, or to drug trafficking *and* a few other crimes. Other countries have an exhaustive list of predicate offences for money laundering which may include the following:

> *fraud, forgery, bribery, corruption, child pornography, prostitution, extortion, murder, theft, robbery, drug offending, tax avoidance and evasion, possessing counterfeit money, betting and pool setting.*

Generally speaking, the term "predicate offence" is used in reference to offences underlying money laundering and/or terrorist financing activity.

Under New Zealand legislation, the money laundering offence can be any offence, it is defined in section 243 of the Crimes Act 1961:

> *“money laundering offence means an offence (or any offence described as a crime) that is punishable under New Zealand law, including any act, wherever committed, that would be an offence in New Zealand if committed in New Zealand.”*

PREDICATE OFFENCE FOR MONEY LAUNDERING IN NEW ZEALAND

Money laundering may be conducted both domestically and internationally and may relate to proceeds of crime generated either domestically or overseas. In New Zealand, the most prevalent predicate offences for money laundering are drug offences, fraud and tax evasion.

The FIU estimates that NZD1.35 billion of domestic proceeds is laundered in New Zealand per annum. The harm caused by the money laundering and the predicate offending it facilitates is many times this figure which belies the scale of human suffering caused by financially motivated crime.

The estimate of domestic proceeds of crime relates principally to drug and fraud offending, but excludes the value of tax evasion or transnational money laundering.

The table on page 11 is a summary of the significant predicate offences and threats (domestic and international) with vulnerabilities, money laundering phase where the predicate offence likely to take place and money laundering and/or terrorist financing typologies.

Threat		Phase	Description
Drug offending	Self-laundering; laundering by close associates ("smurfing" etc.); laundering by professional services; possible access to international money laundering networks	Predicate offending	Cash-based
		Placement	Cash deposits, cash purchase of assets, 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, assets
		Other	Potentially higher value overall and more offenders involved
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 business, likely to be professionally facilitated
		Integration	Real estate, assets
		Other	Potentially higher value per offender
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	Nominees, trusts, family members or third parties etc.
		Integration	Professionals
		Other	Laundering of proceeds from tax offences
			Businesses
			Gambling

The transnational movement of proceeds of crime through New Zealand and New Zealand legal structures is likely to be at least as significant in value terms. The below table describes methods to be associated with high risk transnational threats in previous New Zealand cases and reporting.

Jurisdiction	Specific threats	Description of likely methods
China	Drug offending connected to New Zealand	Remittance and alternative remittance; movement of funds through financial institutions, designated non-financial businesses and professions, businesses and assets; trade-based money laundering through merchandise trade
	Corruption and other economic crime	Trade-based money laundering; remittance and alternative remittance; attempts to seek a safe haven in real estate or possibly market investments (either in person as fugitives or to store proceeds while maintaining control from offshore)
Australia	Organised criminal groups with trans-Tasman connections	Remittance and alternative remittance; movement of funds through financial institutions; designated non-financial businesses and professions, businesses and assets; trade-based money laundering through merchandise trade
	Tax evaders and other economic criminals	Trade-based money laundering using trade in services and legal structures
Eastern Europe	Organised crime and economic criminals with no link to New Zealand	Use of legal structures and alternative payment platforms
USA	Organised crime	Remittance and alternative remittance; movement of funds through financial institutions; designated non-financial businesses and professions, businesses and assets; trade-based money laundering through merchandise trade
	Economic criminals	Trade-based money laundering using trade in services and legal structures
	Terrorist financing	Groups raising capital from domestic sympathisers; remittance and alternative remittance
South Asia and Middle East	International controllers	Remittance and alternative remittance; trade-based money laundering
East and South-East Asia	Drug offenders with connection to New Zealand	Remittance and alternative remittance; movement of funds through financial institutions; designated non-financial businesses and professions, businesses and assets
	Economic criminals	Abuse of legal structures; movement of funds through financial institutions; designated non-financial businesses and professions, businesses and assets; attempts to seek a safe haven in real estate or possibly market investments (either in person as fugitives or to store proceeds while maintaining control from offshore)

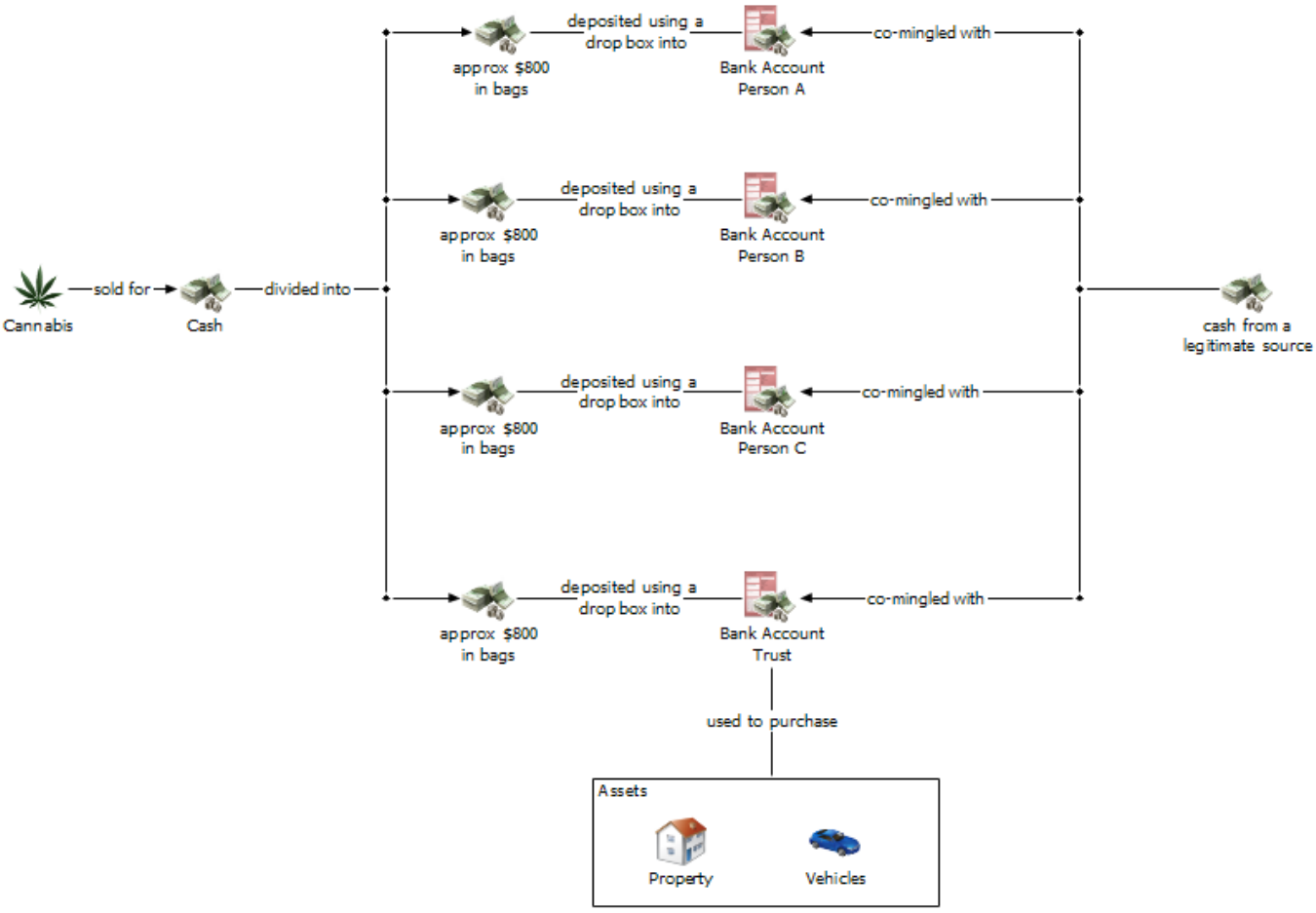
The table below outlines a qualitative assessment of the harm caused by laundering the proceeds from drug offending, fraud and tax offending.

Threat	Disruption of harm
Drug offending	Effect on law enforcement
	• Reinvestment of proceeds in further drug offending leading to expanded drug distribution enterprises and cascading growth of other drug harms, including: o proliferation of second tier offending as users commit crime to feed addiction o violent offending between drug offenders seeking to expand market share • Corruption of facilitators of drug offending and related money laundering • Proliferation of uneconomic businesses used to launder money • Drug offenders enjoy the financial benefits of their offending
	Effect on reputation
	• Reinvestment and opportunity to enjoy proceeds of drug offending may: o impact foreign relations with source countries, and other jurisdictions used to facilitate New Zealand drug market o impact on meeting international obligations to combat drug offending
Fraud	Effect on law enforcement
	• Predicate offending is undetected, leading to ongoing victimisation • Offenders are able to enjoy the proceeds of crime motivating further offending • Proceeds are placed beyond recovery • Corruption of facilitators, especially gatekeeper professionals
	Effect on reputation
	• Loss of trust in financial institutions • Growing perception of corruption
Tax offending	Effect on law enforcement
	• Predicate offending remains undetected • Unfair economic advantage to offending companies • Loss of revenue • Corruption of facilitators, especially gatekeeper professionals
	Effect on reputation
	• Loss of trust in the financial institutions • Loss of trust in the tax administration • Reputation of corrupt practices and evasion leads to further offending
Other	Effect on law enforcement
	• Offenders are able to enjoy the proceeds of crime motivating further offending • Proceeds are placed beyond recovery
	Effect on reputation
	• Offenders are able to enjoy the proceeds of crime motivating further offending • Proceeds are placed beyond recovery • Corruption of facilitators

NEW ZEALAND CASE STUDY 1 – OPERATION FOXY: DRUG OFFENDING

In 2012, the Wellington Covert Operations Group and the Central Asset Recovery Unit started investigating a family syndicate for the commercial distribution of cannabis. The syndicate grew and sourced cannabis from other growers to sell. The syndicate earned a significant profit, and over a seven year period syndicate members made over NZD1.6 million in cash deposits into numerous bank accounts operated by family members. The head of the syndicate, Person A, would spend several hours each morning banking cash, then the afternoon selling cannabis, and the evening preparing for the next days activities.

To attempt to hide the origin of funds, the head of the syndicate, Person A, smurfed cash into multiple accounts. Person A opened multiple bank accounts with several banks either in their name, the trust name, or a family member's name. Person A would then package cash earned from the sale of cannabis into drop box plastic bags. Generally the money was in NZD800 amounts. Person A would then visit multiple banks and bank the cash into various accounts via drop box. Person A did not interact with bank tellers, it was likely that this was an attempt to minimise the risk of detection. Person A then co-mingled the funds with legitimately sourced funds to purchase assets. Syndicate members purchased ten properties, many of which were owned by the trust the syndicate set up. Cash was also deposited into the trusts bank accounts.



NZD3.1 million in assets were restrained under the Criminal Proceeds Recovery Act 2009. These assets included properties, vehicles, and cash. Person A, was subsequently charged with selling cannabis, possession of cannabis for supply and money laundering.

NEW ZEALAND CASE STUDY 2 – POLICE OPERATION IN 2011: TAX EVASION

Person A was the Director and Shareholder of Company B. Person A made claims to Inland Revenue based on false invoices. Based on the same invoices they evaded taxation responsibilities estimated by Inland Revenue at approximately NZD250,000 and received approximately the same amount from Inland Revenue. Person A was charged with tax evasion offences having used nominees, trusts, family members and third parties to co-mingle funds. Person A then fled to Australia.

Person A was extradited from Australia and was returned to New Zealand. Person A was convicted on 18 charges of Evades Tax Payment and was sentenced to nine months home detention and 150 hours community work. Their assets, including two properties and cash, were also forfeited.

OVERSEAS CASE STUDY – AUSTRALIA: TAX EVASION[3]

Australian law enforcement agencies conducted an investigation into a complex 'round robin' tax evasion scheme. These schemes essentially aim to make funds movements appear as payments to other parties while, in reality, the funds ultimately return to the original beneficiary. Part of the investigation focused on two suspects (A and B) who were jailed for evading company and personal income tax of approximately AUD750,000 (approximately NZD787,000).

Suspect A was the sole director and shareholder of companies X and Y, and suspect B was the sole director and shareholder of company Z. Both suspects operated businesses which performed contract work through their respective companies in the building industry.

The method used to facilitate tax evasion was:

1. The suspects transferred funds from their companies' accounts to the bank accounts of companies in New Zealand. The New Zealand companies and the bank accounts were controlled by the Vanuatu-based accountant, who was a signatory to the bank accounts.

2. The payments were falsely described in the suspects' companies' records as expenses in the form of 'management and consultancy fees'. False invoices were created for the fictitious expenses. No evidence was available to show that any consulting work had been carried out. The invoice amounts matched the amounts paid to the bank accounts in New Zealand.

3. The false expense payments were claimed as deductible expenses in the tax returns of companies X, Y and Z, thereby fraudulently reducing the companies' taxable income and therefore the amount of tax they were assessed as liable to pay.

4. The accountant then transferred the funds under the guise of international 'loans' through a series of round robin international transactions, through accounts held in the name of companies owned and operated by the accountant.

[3] http://www.austrac.gov.au/case-studies/austrac-information-revealed-complex-%E2%80%98round-robin%E2%80%99-tax-evasion-scheme

5. The accountant transferred the funds into the personal bank accounts of the suspects in Australia. The funds were transferred via an overseas company controlled by the accountant, separate to the companies in New Zealand that received the funds originally.

6. In order to disguise the funds being transferred back into Australia as loans, false documents were created purporting to be international loan agreements with a foreign lender. Loans are not assessable income and are tax free in Australia.

7. The funds, disguised as international loans, were not disclosed in the suspects' personal tax returns. The suspects were thus assessed as liable for less tax than they should have been, thereby avoiding income tax obligations.

8. Effectively, the 'loans' paid to the suspects were funds from their respective companies but were disguised by the scheme, allowing them to evade company and personal tax.

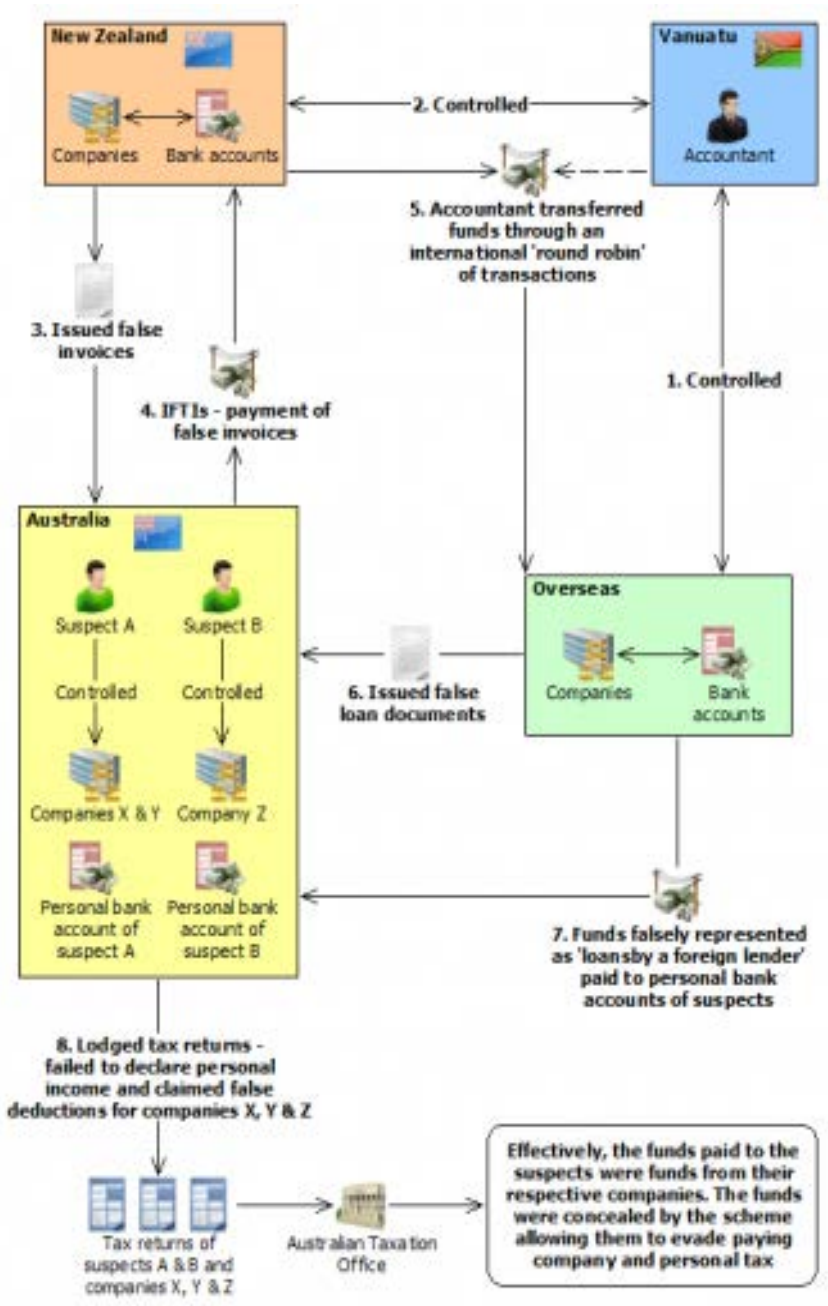
It was alleged that suspect A engaged in 15 round robin transactions over a one-year period and lodged false tax returns for himself and companies X and Y. The data showed that over a five-year period suspect A received incoming international funds transfers of approximately AUD540,000 (approximately NZD566,000) from New Zealand. These funds were sent by a company of which the accountant was a director.

It was alleged that suspect B engaged in 11 round robin transactions over a three-year period. He also lodged false tax returns for himself and company Z. Over a one-year period suspect B made four international funds transfers to bank accounts in New Zealand for amounts ranging from around AUD26,000 to AUD40,000 (approximately NZD27,000-42,000). The accountant was a signatory to the New Zealand bank accounts.

Suspects A and B evaded around AUD390,000 (NZD409,000) and AUD360,000 (NZD370,000) in company and personal tax respectively.

Suspect A pleaded guilty to one charge of obtaining a financial advantage by deception. Suspect B pleaded guilty to defrauding the Commonwealth, obtaining a financial advantage by deception, and dealing in proceeds of crime.

Both suspects were sentenced to three years imprisonment. The accountant was convicted of conspiring to defraud the Commonwealth and was sentenced to eight years and 11 months imprisonment.



Indicators:

- Account activity inconsistent with customer profile
- Customer receives international funds transfers declared as loans from a foreign lender
- Customers undertaking complicated transfers without a business rationale
- Different ordering customers sending international funds transfers to the same beneficiaries
- False invoices created for services not carried out
- International funds transfers to a high-risk jurisdiction
- Multiple high-value international funds transfers to and from Australia with no apparent logical reason

OVERSEAS CASE STUDY – INDONESIA: CORRUPTION[4]

Ms. X, a People's Representative Council (PRC) member, was charged for corruption and money laundering totalling USD625,000 related with abuse of authority in deciding the region to receive local infrastructure funds. According to INTRAC's analysis, the total value in Ms. X's bank account was USD5 million. The funds were suspected to be the result of criminal action. Most of the funds were used to purchase assets such as insurance policy, time deposits, houses, apartments and gold jewellery. Ms. X also used a credit facility and transferred the funds to a third party. Some of Ms. X's assets totalling USD1 million were seized. Ms. X was indicted to six years in prison and USD50,000 in fines.

[4] APG Yearly Typology Report 2015 http://www.apgml.org/includes/handlers/get-document.ashx?d=d2dcfb98-e648-4ab1-bfa9-0d0d4bc65fab

Annex 1

THE THREE INTERNATIONALLY ACCEPTED PHASES FOR THE MONEY LAUNDERING PROCESS:

Phase	Description	Example
Placement	Cash enters the financial system.	Proceeds of selling cannabis deposited into a bank account.
Layering	Money is involved in a number of transactions.	Money is transferred into other bank accounts that have been set up and international travel tickets are purchased.
Integration	Money is mixed with lawful funds or integrated back into the economy, with the appearance of legitimacy.	International travel tickets are cancelled, which results in a reimbursement cheque being issued to the suspect, minus cancellation fees. Money is used to buy goods, services, property or investments.

TYPOLOGIES - BASED ON THE ASIA PACIFIC GROUP ON MONEY LAUNDERING DEFINITIONS

- **WIRE TRANSFERS —** transferring proceeds of crime from one person to another via money remittance services.
- **PURCHASE OF VALUABLE COMMODITIES —** laundering proceeds of crime by purchasing valuable commodities, for example, precious metals or gems.
- **PURCHASE OF VALUABLE ASSETS —** laundering proceeds of crime by purchasing valuable assets, for example, property or vehicles.
- **SHELL COMPANIES —** registering companies which have no actual business activity. Internationally based directors/shareholders and offshore bank accounts are used to facilitate money laundering and/or terrorist financing by unverified beneficiaries. In addition, there is also the risk of exploitation of other corporate forms, particularly limited partnerships.
- **NOMINEES, TRUSTS, FAMILY MEMBERS OR THIRD PARTIES** — utilising other people to carry out transactions in order to conceal the true identity of persons controlling proceeds of crime.
- **TRADE-BASED MONEY LAUNDERING —** manipulating invoices, often in connection with international trade, by overstating the value of a shipment providing criminal entities with a paper justification to either launder proceeds of crime and/or send funds overseas to finance terrorism.
- **CANCEL CREDITS OR OVERPAYMENTS —** laundering proceeds of crime by overpaying, then requesting refund cheques for the balance.
- **ELECTRONIC TRANSFERS —** transferring proceeds of crime from one bank account to another via financial institutions.
- **CO-MINGLING —** combining proceeds of crime with legitimate business takings.
- **GATEKEEPERS/PROFESSIONAL SERVICES —** utilising "professionals" to establish seemingly legitimate business activities, for example, lawyers, accountants, brokers, company formation agents.
- **CASH DEPOSITS —** placement of cash into the financial system.
- **SMURFING —** utilising third parties or groups of people to carry out structuring.
- **CREDIT CARDS, CHEQUES, PROMISSORY NOTES —** instruments used to access funds held in a financial institution, often in another jurisdiction.

- **CASH COURIERS —** concealing the movement of currency from one jurisdiction to another using people, luggage, mail or any other mode of shipment, without declaration.
- **STRUCTURING —** separating large transactions into small transactions to avoid scrutiny and detection from financial institutions.
- **ABUSE OF NON-PROFIT ORGANISATIONS —** raising funds to finance terrorism using non-profit organisations (charities) to conceal the source and nature of funds, as well as to facilitate distribution.
- **INVESTMENT IN CAPITAL MARKETS —** laundering proceeds of crime by using any market in which securities are traded, for example, the stock and bond markets, as well as futures trading and currency speculation.
- **OTHER PAYMENT TECHNOLOGIES —** utilising emerging or new payment technologies to facilitate money laundering and/or terrorist financing.
- **UNDERGROUND BANKING/ALTERNATIVE REMITTANCE SERVICES** — transferring proceeds of crime from one person to another via informal banking mechanisms.
- **TRUSTED INSIDERS/CORRUPTION —** collusion, coercion or bribery of financial institution staff by customers, particularly high-profile individuals, for instance, government officials, business executives, celebrities or individuals known or suspected of being involved in serious crime.
- **CASH EXCHANGES —** exchanging low denomination notes for high (also known as refining) as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.
- **CURRENCY CONVERSION —** converting one currency into another as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.

Annex 2

FINANCIAL INTELLIGENCE UNIT

The Financial Intelligence Unit is part of the Financial Crime Group, which is made up of four Asset Recovery Units, a core administrative/analytical team and the Financial Intelligence Unit. The Financial Intelligence Unit has been operational since 1996 and part of its core functions is to receive, collate, analyse and disseminate information contained in Suspicious Transaction Reports, Suspicious Property Reports and Border Cash Reports. It also develops and produces a number of financial intelligence products, training packages and policy advice. The Financial Intelligence Unit also participates in the AML/CFT National Coordination Committee chaired by the Ministry of Justice. It is also a contributing member to international bodies such as the Egmont Group of international financial intelligence units and the Asia/Pacific Group on Money Laundering. The FIU can be contacted at: **fiu@police.govt.nz**

Annex 3

TYPOLOGY INDICATORS

GENERAL INDICATORS

These indicators are present in many of the typologies used in money laundering and terrorist financing.

- Transactions involving locations with poor AML/CFT regimes or high exposure to corruption
- Significant and/or frequent transactions in contrast to known or expected business activity
- Significant and/or frequent transactions in contrast to known employment status
- Ambiguous or inconsistent explanations as to the source and/or purpose of funds

- Where relevant, money presented in unusual condition, for example, damp, odorous or coated with substance
- Where relevant, nervous or uncooperative behaviour exhibited by employees and/or customers

WIRE TRANSFERS — transferring proceeds of crime from one person to another via money remittance services.

Possible indicators (specific)

- Significant and/or frequent cash payments for transfers
- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers to high-risk countries or known tax havens
- Transfers to numerous offshore jurisdictions with no business rationale
- Multiple transfers sent to same person overseas by different people
- Same home address provided by multiple remitters
- Departure from New Zealand shortly after transferring funds
- Reluctant to provide retailer with identification details

PURCHASE OF VALUABLE COMMODITIES — laundering proceeds of crime by purchasing valuable commodities, for example, precious metals or gems.

Possible indicators (specific)

- Customers requiring safe custody arrangements with financial institution
- Significant and/or frequent cash purchases of valuable commodities
- Regular buying and selling of valuable commodities that does not make economic sense

PURCHASE OF VALUABLE ASSETS — laundering proceeds of crime by purchasing valuable assets, for example, property or vehicles.

Possible indicators (specific)

- Purchase/sale of real estate above/below market value irrespective of economic disadvantage
- Cash purchases of valuable assets with cash and/or cash deposits for valuable assets
- Low value property purchased with improvements paid for in cash before reselling
- Rapid repayment of loans/mortgages with cash or funds from an unlikely source

SHELL COMPANIES — registering New Zealand companies with internationally based directors and/or shareholders in order to open bank accounts to facilitate money laundering and/or terrorist financing by unverified beneficiaries.

Possible indicators (specific)

- Large numbers of companies registered with the same office address
- Address supplied is a "virtual office"
- Accounts/facilities opened/operated by company formation agents
- Lack of information regarding overseas directors/beneficiaries
- Complex ownership structures
- Structures where there is no apparent legitimate economic or other rational

Additional Indicators:

- The same natural person is the director of a large number of single director companies
- The same person (natural or corporate) is the shareholder of a large number of single-shareholder companies
- Use of one of a small number of New Zealand 'agents' who undertake transactions with the companies register

NOMINEES, TRUSTS, FAMILY MEMBERS OR THIRD PARTIES — utilising other people to carry out transactions in order to conceal the true identity of persons controlling proceeds of crime.

Possible indicators (specific)

- Customers using family members or third parties, including the use of children's accounts
- Transactions where third parties seem to be retaining a portion of funds, for example, "mules"
- Accounts operated by someone other than the account holder
- Many transactions conducted at various financial institutions and/or branches, in one day
- Significant and/or frequent transactions made over a short period of time

TRADE-BASED MONEY LAUNDERING — manipulating invoices, often in connection with international trade, by overstating the value of a shipment providing criminal entities with a paper justification to either launder proceeds of crime and/or send funds overseas to finance terrorism.

Possible indicators (specific)

- Invoice value greater than value of goods
- Discrepancies in domestic and foreign import/export data
- Suspicious cargo movements
- Suspicious domestic import data
- Discrepancies in information regarding the origin, description and value of the goods
- Discrepancies with tax declarations on export declarations
- Sudden increase in online auction sales by particular vendors (online auction sites)
- Unusually frequent purchases between same buyers and vendors (online auction sites)

CANCEL CREDITS OR OVERPAYMENTS — laundering proceeds of crime by overpaying, then requesting refund cheques for the balance.

Possible indicators (specific)

- Casino gaming machines loaded with cash, credits cancelled and a refund cheque requested
- Casino chips purchased, followed by limited or no gambling, then a refund cheque requested
- Frequent cheque deposits issued by casinos
- Significant and/or frequent payments to utility companies, for example, electricity providers
- Frequent cheque deposits issued by utility companies, for example, electricity providers
- Significant and/or frequent payments for purchases from online auction sites
- Frequent personal cheque deposits issued by third parties

ELECTRONIC TRANSFERS — transferring proceeds of crime from one bank account to another via financial institutions.

Possible indicators (specific)

- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers involving accounts located in high-risk countries or known tax havens
- Transfers to offshore jurisdictions with no business rationale
- Multiple transfers sent to same person overseas by different people
- Departure from New Zealand shortly after transferring funds
- Transfers of funds between various accounts that show no economic sense (i.e. multiple transfers incurring bank fees where one single transfer would have been sufficient)

CO-MINGLING — combining proceeds of crime with legitimate business takings.

Possible indicators (specific)

- Significant and/or frequent cash deposits when business has EFTPOS facilities
- Large number of accounts held by a customer with the same financial institution
- Accounts operated by someone other than the account holder
- Merging businesses to create layers
- Complex ownership structures
- Regular use of third party accounts

GATEKEEPERS/PROFESSIONAL SERVICES — utilising "professionals" to establish seemingly legitimate business activities, for example, lawyers, accountants, brokers, company formation agents.

Possible indicators (specific)

- Accounts and/or facilities opened and/or operated by company formation agents
- Gatekeepers that appear to have full control
- Known or suspected corrupt professionals offering services to criminal entities
- Accounts operated by someone other than the account holder

CASH DEPOSITS — placement of cash into the financial system.

Possible indicators (specific)

- Large cash deposits followed immediately by withdrawals or electronic transfers

SMURFING — utilising third parties or groups of people to carry out structuring.

Possible indicators (specific)

- Third parties conducting numerous transactions on behalf of other people
- Many transactions conducted at various financial institutions and/or branches, in one day
- Accounts operated by someone other than the account holder

CREDIT CARDS, CHEQUES, PROMISSORY NOTES — instruments used to access funds held in a financial institution, often in another jurisdiction.

Possible indicators (specific)

- Frequent cheque deposits in contrast to known or expected business activity
- Multiple cash advances on credit card facilities
- Credit cards with large credit balances
- Transactions inconsistent with intended purpose of facility

CASH COURIERS — concealing the movement of currency from one jurisdiction to another using people, luggage, mail or any other mode of shipment, without declaration.

Possible indicators (specific)

- Transactions involving locations with poor AML/CFT regimes or high exposure to corruption
- Customers originating from locations with poor AML/CFT regimes/high exposure to corruption
- Significant and/or frequent cash deposits made over a short period of time
- Significant and/or frequent currency exchanges made over a short period of time

STRUCTURING — separating large transactions into small transactions to avoid scrutiny and detection from financial institutions.

Possible indicators (specific)

- Many transactions conducted at various financial institutions and/or branches, in one day
- Small/frequent cash deposits, withdrawals, electronic transfers made over a short time period
- Multiple low value domestic or international transfers

ABUSE OF NON-PROFIT ORGANISATIONS — raising funds to finance terrorism using non-profit organisations (charities) to conceal the source and nature of funds, as well as to facilitate distribution.

Possible indicators (specific)

- Known or suspected criminal entities establishing trust or bank accounts under charity names
- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers involving accounts located in high-risk countries or known tax havens
- Transfers to numerous offshore jurisdictions with no business rationale
- Entities that use third parties to distribute funds or have weak financial governance mechanisms

INVESTMENT IN CAPITAL MARKETS — laundering proceeds of crime by using any market in which securities are traded, for example, the stock and bond markets, as well as futures trading and currency speculation.

Possible indicators (specific)

- Securities accounts opened to trade in shares of only one listed company
- Transaction patterns resemble a form of market manipulation, for example, insider trading
- Unusual settlements, for example, cheques requested for no apparent reason, to third parties
- Funds deposited into stockbroker's account followed immediately by requests for repayment
- Limited or no securities transactions recorded before settlement requested

OTHER PAYMENT TECHNOLOGIES — utilising emerging or new payment technologies to facilitate money laundering and/or terrorist financing.

Possible indicators (specific)

- Excessive use of stored value cards
- Significant and/or frequent transactions using mobile telephone services

UNDERGROUND BANKING/ALTERNATIVE REMITTANCE SERVICES — transferring proceeds of crime from one person to another via informal banking mechanisms.

Possible indicators (specific)

- Significant and/or frequent cash payments for transfers
- Cash volumes and transfers in excess of average income of migrant account holders
- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers involving accounts located in high-risk countries or known tax havens
- Transfers to countries that are not destination countries or usual remittance corridors
- Large transfers from accounts to potential cash pooling accounts
- Significant and/or frequent transfers recorded informally using unconventional book-keeping
- Significant and/or frequent transfers requested by unknown or intermittent customers
- Numerous deposits to one account followed by numerous payments made to various people

TRUSTED INSIDERS/CORRUPTION — collusion, coercion or bribery of financial institution staff by customers, particularly high-profile individuals, for instance, government officials, business executives, celebrities or individuals known or suspected of being involved in serious crime.

Possible indicators (specific)

- Customers regularly targeting the same employees
- Employees relaxing standard AML/CFT procedures to facilitate transactions
- Employees exhibiting sudden wealth and/or assets in contrast to remuneration
- Employees avoiding taking annual leave
- Sudden improvement in employee's sales performance
- Employees adopting undue levels of secrecy with transactions
- Customers regularly targeting young and/or inexperienced employees

CASH EXCHANGES — exchanging low denomination notes for high (also known as refining) as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.

Possible indicators (specific)

- Significant and/or frequent cash exchanges from small to large denominations (refining)

CURRENCY CONVERSION — converting one currency into another as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.

Current impact on New Zealand assessed as:

Possible indicators (specific)

- Significant and/or frequent New Zealand or foreign currency exchanges
- Opening of foreign currency accounts with no apparent business or economic purpose