Financial Intelligence Unit

New Zealand Police

Quarterly Typology Report
First Quarter (Q1)
2015/2016

(Issued October 2015)

INTRODUCTION

This report is the first Quarterly Typology Report of 2015/2016 produced by the Financial Intelligence Unit (FIU), part of the New Zealand Police Financial Crime Group. As the Quarterly Typology Report 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 Quarterly Typology Report as part of its obligations under s.142 (b) (i) and s.143 (b) of the AML/CFT Act 2009.[1]

PURPOSE

The purpose of the Quarterly Typology Report is to provide an accurate picture of current, emerging and longer term factors impacting on the AML/CFT environment. The Quarterly Typology Report 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 Quarterly Typology Report is a law enforcement document. However, it does not include sensitive reporting or restricted information and is published on the FIU website. The Quarterly Typology Report is produced using a variety of sources and qualitative/quantitative data.

DEFINITION OF MONEY LAUNDERING

Under New Zealand legislation the money laundering offence is defined in s.243 of the Crimes Act 1961 and s.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, and
- 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

1 S.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

S.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.

Financial Intelligence Unit and partner agencies - Updates

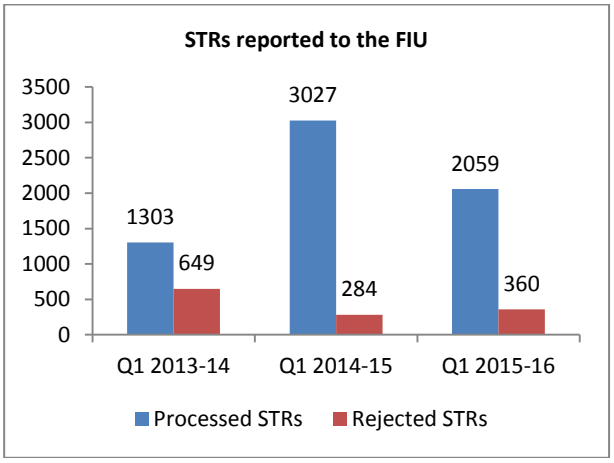
NOTE: Information on the Financial Intelligence Unit is provided as a permanent annex (refer Annex 2).

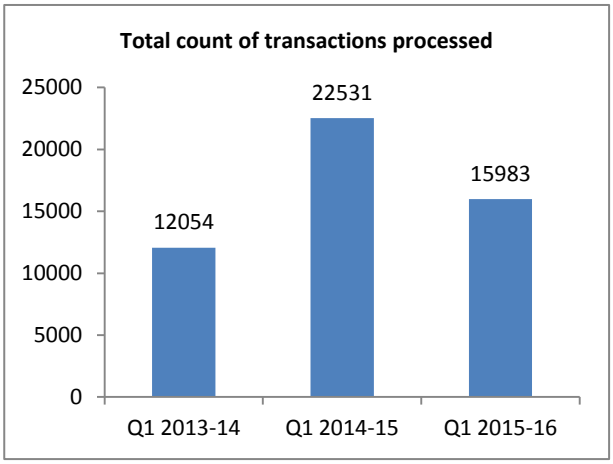
FIU STATISTICS

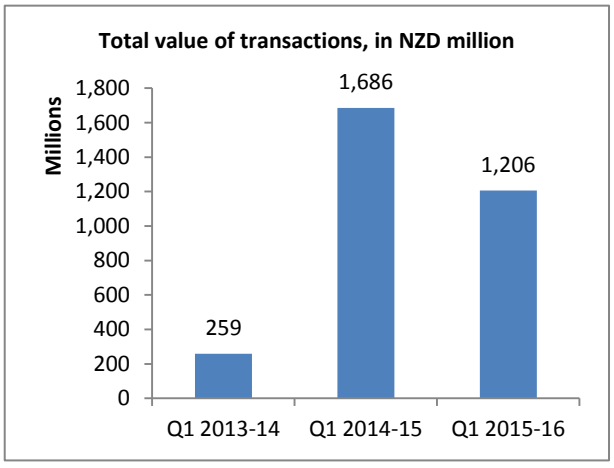
STRs

In first quarter of 2015-16 the number of STRs reported to the FIU decreased by one-third of the same time last year but it is still higher than in the first year of reporting pursuant to the AML/CFT Act. The FIU has processed 2059 STRs (compared to 3027 in 2014-15 and 1303 in 2013-14).

Currently the number of rejected STRs has increased to 360 from 284 in Q1 2014-15.







There is also a decline of the total count of transactions processed for this latest quarter corresponding to the decrease in the number of STRs. The FIU has processed a total of 15983 suspicious transactions (compared to 22531 in Q1 2014-15). In view of that, the total value of those transactions has too reduced to NZD 1.2 billion (compared to NZD 1.68 billion last year).

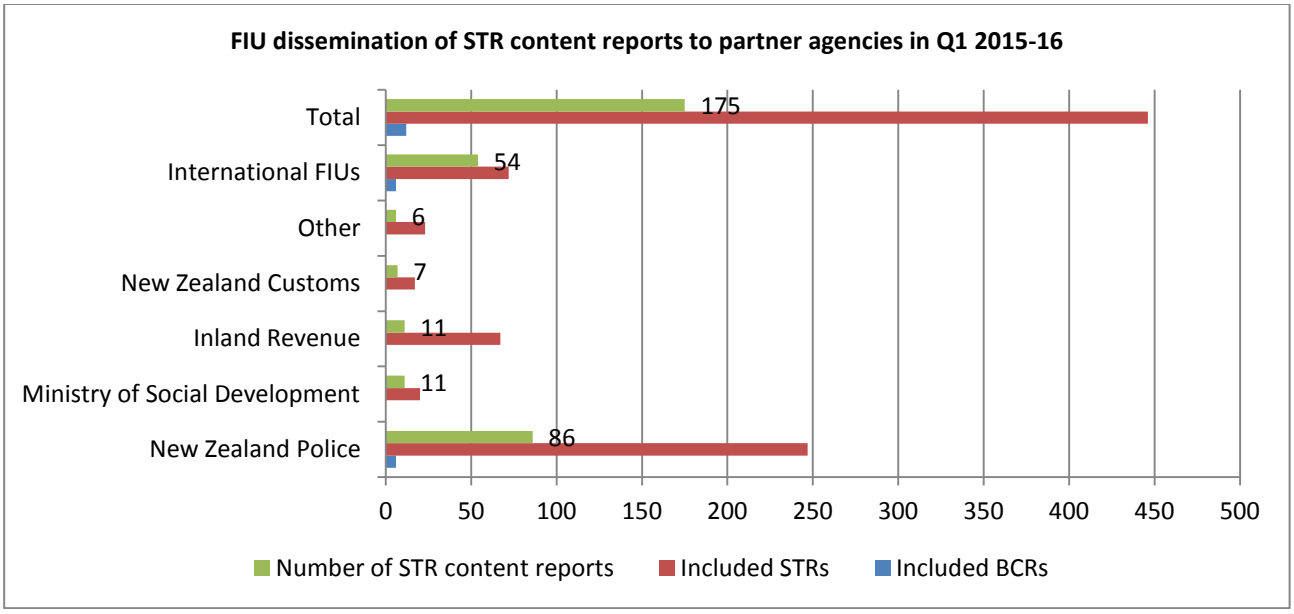
STR Content Reports

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.

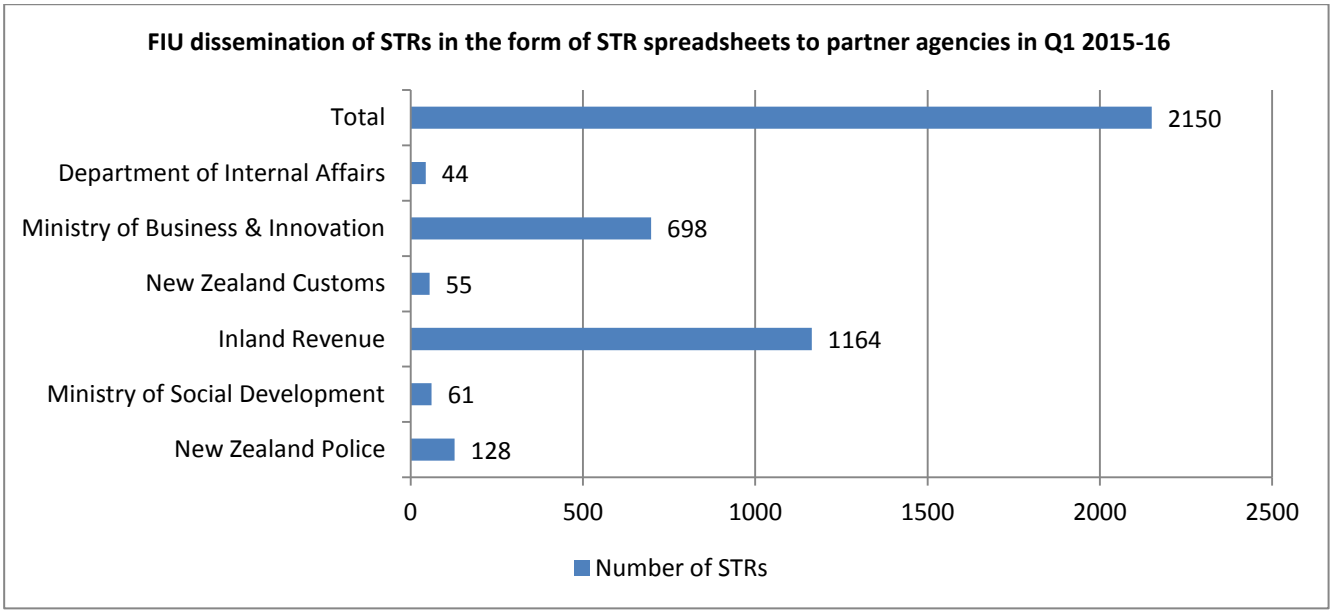
In Q1 2015-16 the FIU disseminated a total of 175 STR content reports, most of which have been sent to Police and international FIUs – 86 and 54 respectively. There were a total of 446 STRs and 12 BCRs included in these STR content reports for this quarter.



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.

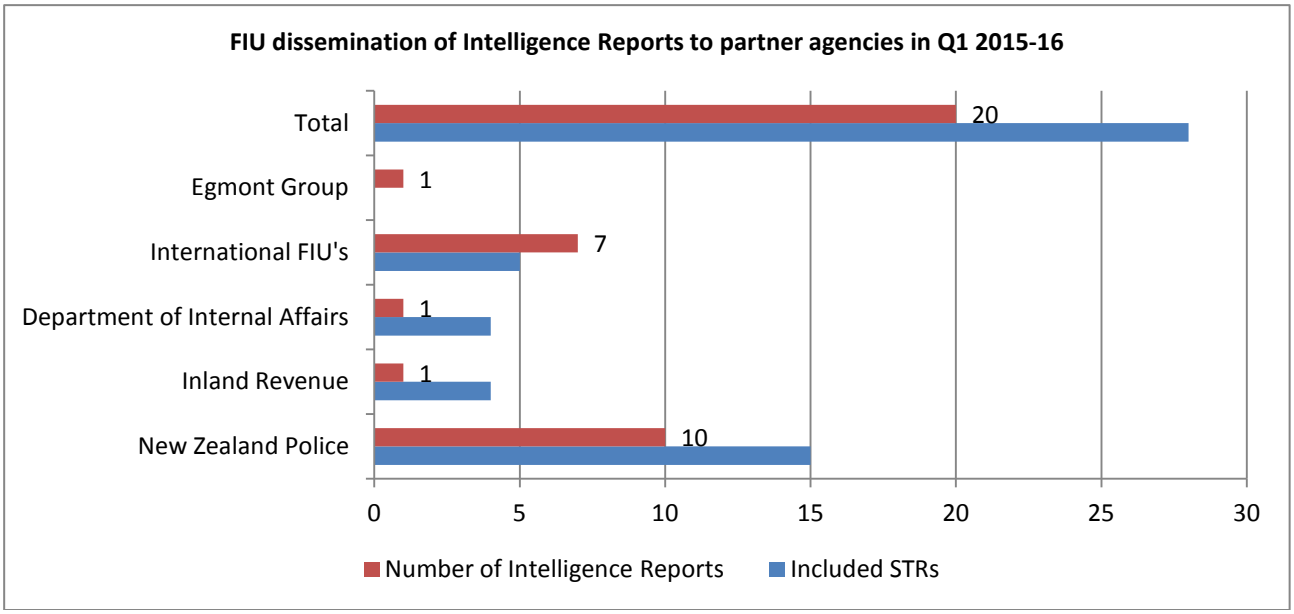
The FIU distributed 11 STR spreadsheets in Q1 2015-16 to six partner agencies, which included raw data of a total of 2150 STRs.



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 Q1 2015-16 the FIU has produced 20 intelligence reports which contained analysis of a total of 28 STRs. Half of these intelligence reports were sent to Police. Other recipients included Inland Revenue, DIA, Egmont Group and international FIUs.



FIU CONFERENCE 2016

The 2016 FIU-ACAMS conference will be held again next year at Te Papa, Wellington on 14-15 September. The FIU is currently scoping on the conference and will be sending out information through the goAML message board in the coming months. To make comments or suggestions, please contact the FIU at FCG.Seminar@police.govt.nz

GOAML 4.2 UPGRADE

The goAML upgrade will now happen between 3-16 December inclusive. This means that we will need to take the reporting website offline for about a week while the upgrade takes place. The FIU asks that during this the Reporting Entities hold all STRs and submit at the end of the down period. The FIU does not consider that Reporting Entities will breach the 3-day reporting rule. Any urgent STRs will be accepted verbally pursuant to the AML/CFT Act. We will be able to be more specific closer to the time.

We have posted a general web user guide for version 4.2 on our website, as well as a brief letter from Andrew Hill, Manager FIU. Note that the implementation date in the letter is no longer correct, as the upgrade was pushed back to December. Our information web site is here, and we will make updates as they come to hand.
http://www.police.govt.nz/advice/businesses-and-organisations/fiu/goaml

ORGANISED CRIME BILL

The Organised Crime and Anti-Corruption Legislation Bill has completed the Committee of the Whole House stage in Parliament. It was split into 15 various pieces of legislation which are awaiting third reading. The Bill includes amendments to the AML/CFT Act to introduce reporting for international transactions (with a threshold of NZD 1,000) and for large cash transactions (with a threshold of NZD 10,000). Officials expect that the Bill will pass before the end of 2015, with a commencement date for reporting of 1 July 2017.

2015 APG TYPOLOGIES MEETING

The 2015 APG Typologies and Capacity Building Workshop will be held from 16 to 20 November 2015, in Kathmandu, Nepal, and Senior Research Advisor will be attending this event. This typologies meeting will include workshops on new and emerging terrorist financing risks, with particular emphasis on terrorist financing related to ISIL. Its aim is to share regional experiences and considering opportunities to deepen international cooperation in assessing and responding to terrorist financing risks. The meeting will reflect current work being done by the FATF and UN, and APG members.

REGIONAL COUNTERTERRORISM FINANCING SUMMIT

In November Australia's and Indonesia's financial intelligence units, AUSTRAC and PPATK, will co-host the first counter-terrorism financing summit in our region in Sydney. This summit will boost collective efforts to track terrorism financing and proceeds of crime through a range of financial channels to counter the terror threat and combat transnational crime in the critical parts of the Australasia region. National Manager for Financial Crime Group will be attending the summit.

MUTUAL EVALUATION OF SINGAPORE

For three weeks in November, a FATF evaluation team will be conducting an onsite visit to Singapore as part of the country's evaluation process. The Manager of FIU will be joining this evaluation team as a law enforcement expert from New Zealand.

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, Christchurch.

ASSET RECOVERY UNITS: KEY STATISTICS - CORRECT AS AT 30 SEPTEMBER 2015

RESTRAINTS & FORFEITURES

At the end of Q1 2015-16:

- Forfeiture Orders for assets worth an estimated NZD 64.1 million were in place (see key terms below), and
- Restraining Orders were in place over assets worth an estimated NZD 252.1 million pending further investigation and court action (see key terms below).

In July 2015 Dr Michael McFadden from the Institute for Social Science Research undertook research in relation to the crime prevention value obtained through the work of the ARUs. The calculation that he developed estimates that on average crime to the value of NZD 3.3 can be prevented for every NZD 1 restrained and NZD 3.5 for every NZD 1 forfeited. Using this multiplier, crime to the value of NZD 1.1 billion has been prevented since the CPRA came into effect. The majority of this derives from cases associated with organised crime and serious drug offending.

During September –

- Assets valued at an estimated NZD 22.3 million were restrained; and
- Assets worth an estimated NZD 906K of assets were forfeited to the Crown.

This means that asset recovery actions have prevented crime to an estimated value of NZD 76.8 million in the last month.

N.B All data are provisional and are drawn from a dynamic operational database. They are subject to change as new information is continually recorded

ASSETS & CASES

The ARUs have investigated 2955 assets, worth NZD 451 million since the CPRA came into effect. These assets include –

- 1112 cash sums/bank accounts worth NZD 77 million,
- 578 vehicles worth an estimated NZD 19 million,
- 529 houses worth an estimated NZD 253 million, and
- 23 farms/orchards worth an estimated NZD 29 million.

CASES & OFFENDING

The ARUs have opened 953 cases, many with strong links to organised crime. 364 of these cases worth an estimated NZD 138 million are linked to methamphetamine offending. 333 cases worth an estimated NZD 91 million are linked to cannabis offending. 71 cases worth an estimated NZD 71 million are linked to other drug offending. Other cases are linked to theft, tax evasion, and money laundering. 81% of ARU cases are linked to drug offending.

Key terms

Investigated assets: These are…"assets that have been investigated since the Criminal Proceeds (Recovery) Act 2009 came into effect on December 1st 2009". Figures reported in this category include subsequently abandoned cases and should not be confused with **restrained** assets.

Restrained assets: These are…"assets that have been taken from the control of alleged offenders and placed in the hands of the Official Assignee whilst further investigations take place".

Forfeited assets: These are…"assets that, following their initial restraint, have been forfeited to the Crown". The NZD value of these orders does not represent the sum that will be returned to government accounts. Forfeiture Orders are subject to appeals and costs and third party interests must be paid out of the asset value.

Profit Forfeiture Order: This is an order made as a result of civil proceedings instituted by the Crown against a person in order to recover a debt due to it. The maximum recoverable amount, which is determined by calculating the value of any benefit received by criminal offending minus the value of any assets forfeited to the crime, is recovered by the Official Assignee on behalf of the Crown.

Capital Markets

Capital markets are an attractive option at layering and integration stages of money laundering. In addition, layering through capital markets may be inherent in offending or placement (for example, in predicate offences occurring in the markets such as insider trading, market manipulation and securities fraud).

New Zealand's capital markets are supervised by the Financial Market Authority (FMA) which was established in 2011. Its predecessor, the Securities Commission, had analysed money laundering risk in the New Zealand capital markets in their Sector Risk Assessment 2011 (SRA 2011),[2] and most of our following analysis is drawn from that report.

The opportunities presented to quickly carry out transactions, including transnational transactions, within the capital markets with relative anonymity may facilitate illicit transactions. For example, buying, selling and exchanging securities between countries may be more anonymous than transferring funds through telegraphic transfers. Effective movement of value between parties can also be achieved through manipulation of value on many trades effectively allowing transfers outside of traditional channels which are subject to high levels of scrutiny. In addition, because capital markets are perceived as respectable, unusual transactions through capital markets may attract less attention; or be perceived to attract less attention. Finally, as with other forms of wealth, investment in capital markets may be an attractive ultimate destination for proceeds of crime.

OPPORTUNITIES TO LAUNDER

The securities industry is one of the main industries through which persons and entities can access the international financial system. This access provides opportunities for criminals to abuse the financial system. It is increasingly recognised that capital markets offer many opportunities to launder illicit funds. Such opportunities for illegal activities include:

- Transnational transactions and exchanges are possible and may not arise suspicion or attract the same level of due diligence as other channels such as remittance service providers;
- Trade in low priced securities and private issues offer many opportunities for fraud and manipulation. These same opportunities may be exploited to launder money, for example, placing proceeds of crime in a company that is about to become public would offer an opportunity to sell the shares in the company establishing an apparently legitimate source of the funds;
- Some securities may be bought or sold at inflated or deflated rates, effectively transferring value from one party to any other (for example, if party A sells options at a price below the rational market rate to party B, an effective transfer of funds would have taken place if party B then sells the options in the open market);
- Similarly, exchange of one security for another allows for subtle effective transfer of value;
- New technology-based services in the markets provide opportunities to avoid CDD/KYC. For example, internet based trading platforms offer increased opportunity to trade without any face-to-face contact with clients anywhere in the world. Such platforms may be relatively easy to set up and may create a "black-box" in which it becomes impossible for financial institutions to understand individual transactions;
- Similarly, structures and accounts, such as trust, nominee, omnibus accounts, hedge funds etc, may be used to mask the individual beneficial owners and make KYC by financial institutions difficult.

OVERALL VULNERABILITY AND RISK ASSESSMENT

Capital markets are an attractive option for both domestic and international launderers, especially those laundering proceeds of crime with non-cash origin. In particular, businesses in these sectors provide opportunities for non-face-to-face transactions and transactions through intermediaries, significantly increasing access to substantial domestic and transnational channels. However, thanks in large part to the relatively small size of the New Zealand markets, which limits the availability for illicit transactions, the inherent vulnerability of the markets appears to be moderate.

[2] Securities Commission New Zealand Anti-Money Laundering and Countering the Financing of Terrorism Sector Risk Assessment March 2011 http://fma.govt.nz/assets/Reports/110301-aml-cft-sector-risk-assessment.pdf

In general, capital markets are easily accessible. There are many opportunities to enter markets online or to use intermediaries with limited face to face the gatekeepers. Although New Zealand does not have some identified high risk products, such as bearer negotiated shares, New Zealand's markets offer a wide array of products available for laundering which can often be accessed non-face-to-face. Where predicate offending such as market manipulation, abuse and fraud occur in the market, the placement of proceeds in the market is likely to be an inseparable element of the offending.

Many securities markets are inherently transnational, and international exchange of securities is not uncommon. The Securities Commission SRA 2011 found that both brokers and financial advisors had a high level of international exposure. In both cases, it was noted that Australia was the main overseas market, although customers in the USA, UK, Brunei, China and Singapore were also noted.[3] The smaller futures and options sector was noted as being an inherently international market and is particularly exposed to transnational capital flows.

DETECTION, STR REPORTING BY THE SECTOR AND PROSECUTION

Financial activity within the New Zealand capital markets is subject to AML/CFT controls including supervision by the FMA, Customer Due Diligence / Know Your Client (CDD/KYC) and STR reporting to the FIU. The FATF noted that, internationally, capital markets' vulnerability is increased as brokers/dealers may be overly reliant on CDD/KYC by third parties.[4]

For the 2014-15 financial year the FMA reported 24% of their investigations were related to insider trading, market manipulation and disclosure obligations. Only 2% of the FMA's reported investigations could potentially be related to money laundering, they are still ongoing.

There are very a few Police cases where use of shares and other capital markets have been involved. For example, in 2001 during Operation Illusion a gang associate was found to have accumulated NZD 2 million worth of assets, some of which were stored in the form of shares, demonstrating the potential use of the markets to launder. In another case, Police are currently investigating a foreign offender and have restrained a number of shares owned by the individual.

The low level of STR reporting and the lack of prosecutions for money laundering in New Zealand capital markets may suggest that these forms of illegal activities go undetected. It is possible that the chance of detection of money laundering (and terror financing) within the capital markets may potentially increase if CDD and KYC processes are improved.

OVERSEAS CASE STUDIES – CANADA[5]

Case 1. Securities traded over the counter

A subject of an investigation purchased over one million shares in a company traded over the counter in an off-market transaction for less than a third of the market price. An investment company sold the shares through an integrated firm (i.e. a major financial institution) on the part of the investigative subject. FINTRAC (the Financial Transactions and Reports Analysis Centre of Canada) suspected that the terms of the sale of these shares were predetermined by the investigative subject and the purchasing party, in order to transfer the criminal proceeds. The shares were sold the next day at market price, which enabled the share purchaser to receive a 300% return on their investment in one day, and provided a seemingly legitimate explanation for the source of the criminal proceeds.

Case 2. Early redemption of securities

In a drug protection case, suspected members of an organised crime group deposited cash into a front money account at a casino. The individuals then withdrew the funds and were issued cheques, which were deposited into the bank accounts of the suspects and used to purchase certain investment products called GICs (guaranteed investment certificates). These GICs were sold shortly afterward and the individuals did not appear to be concerned about the penalties that would result from their sale prior to maturity.

[3] Ibid page 23

[4] FATF Report: Money Laundering and Terrorist Financing in the Securities Sector, October 2009, page 31 http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20in%20the%20Securities%20Sector.pdf

[5] Money laundering trends and typologies in the Canadian securities sector, April 2013, pages 9-10 http://www.fintrac-canafe.gc.ca/publications/typologies/2013-04-eng.asp

OVERSEAS CASE STUDY – COOK ISLANDS[6]

Manipulation of hedge funds

In January 2013, the CIFIU (*Cook Islands Financial Intelligence Unit)* received a request from a foreign FIU regarding funds relating to an investigation in its country. The investigation related to a hedge fund trader, and two firms involved in a scheme that manipulated several U.S. microcap stocks and generated more than USD 63 million in illicit proceeds through stock sales, commissions and sales credits.

It was alleged that the individuals conducted the scheme through their broker-dealer with the assistance of their close associate, a trader who lives in another jurisdiction. They bought microcap public companies through reverse mergers and manipulated upwards the stock prices of these thinly-traded stocks before selling their shares at inflated prices to eight offshore hedge funds controlled by them. Their manipulation of the stock prices allowed them to materially overstate by at least USD 440 million the hedge funds' performance and net asset values (NAVs) in a fraudulent practice known as "portfolio pumping."

A total of USD 6,068,875 was laundered to an offshore trust account in the Cook Islands when it was frozen by the CIFIU. In July 2013, the total amount was repatriated back to the relevant authorities in the requesting country.

THE EGMONT GROUP CASE STUDY[7]

Undervalued share trading

A bank noticed that a business account that had been dormant for some years suddenly became active with large-scale fund transfers. The bank account was originally registered to a company registered in an offshore jurisdiction. After USD 150,000 was credited into the account, the firm used the funds to buy shares of a recently privatised Eastern-European company - 'ABC Corp'.

Three months later Brian, the representative who originally opened the account, deposited a total amount of USD 250,000 in cash into the company account. Immediately after depositing the money, he wanted to transfer USD 100,000 into a personal account at another bank. He claimed that the money came from his personal funds. When the bank asked him about the origin of these personal funds, he submitted commercial documentation showing that he had sold shares of ABC Corp - worth USD 150,000 - for USD 250,000 to another Eastern-European company 'DEF Corp'. The difference of USD 100,000 Brian explained as risk compensation, in the event the initial USD 150,000 worth of shares invested in company ABC had been devalued. This would have been fairly high return on capital, when one takes into account that a return of USD 100,000 over just three months would have equalled an annual interest rate of over 200 per cent.

The bank disclosed the transactions to the national FIU. By checking the records of its own intelligence and financial databases and liaising with other Egmont members, the FIU developed information that indicated Brian was the real owner of the offshore company. Also, it discovered that Brian was a member of the board of directors of company ABC. This suggested that the shares in company ABC might well have been knowingly sold at a low value to the offshore company before being sold onwards for a higher price to a third party. In effect, Brian siphoned off USD 100,000 profit by using his own offshore company as a 'hidden' stage in the share transfer.

The FIU notified the corresponding law enforcement authorities that Brian was suspected of money laundering and fraud. As a result of the police investigation, Brian was arrested and prosecuted, with the court also confiscating the USD 100,000 involved.

[6] APG Yearly Typologies Report 2014, page 31 http://www.apgml.org/includes/handlers/get-document.ashx?d=d82955e9-74cb-4eb5-b552-65470c113b2d

[7] 100 cases from the Egmont Group, page 5 http://www.egmontgroup.org/library/download/21

NEW ZEALAND RED FLAGS

The money laundering methods and techniques described below were identified after New Zealand Police FIU analysed STRs received from the financial and securities sectors. In general, the methods discussed fall into the "layering" stage of money laundering, where the goal is to create a complex series of financial transactions to disguise the source and/or ownership of the funds. These matters remain under investigation.

Case 1.

The FIU has received several reports from New Zealand banks about a potential movement of layered funds by two foreign nationals who reside in New Zealand as Category 1 investors. Under this category, a foreign national can apply for New Zealand residence if they can invest a minimum of NZD 10 million in New Zealand for at least three years.

It has been reported that in 2012, on the same day but separately, both investors had opened accounts to set up portfolios of New Zealand Immigration acceptable investments for three year period in order to secure New Zealand residency. Shortly thereafter, investor 1 had funds of NZD 10.5 million arrive into his newly opened account, originating from several international transfers. Less than two years later after the initial investment, NZD 10 million were remitted to his own account held in his home country. Meanwhile, investor 2 had about half of the required amount of NZD 10 million arrive into his Immigration NZ bond portfolio account, which 18 months later were moved out to a New Zealand corporate bank account and then subsequently transferred out further to another New Zealand bank account the following day. When questioned, investor 2 was unwilling to provide details about the large account withdrawal, and soon after he closed his portfolio account.

The banks were unable to determine the purpose of the international transfers, there are serious questions and concerns that both individuals have breached New Zealand immigration rules and potentially laundered illicit funds through New Zealand.

Case 2.

Several New Zealand banks have reported some unusual share trading patterns. Certain individuals would deposit cash of tens of thousands of NZD into their newly opened accounts, and immediately start buying various high value stocks and selling them off in a few days, always for a loss. The banks became suspicious when they repeatedly tried to explain the customers that their sale trade would result in losses but the clients had expressed no concerns about the large loss and continued with the pattern.

One customer had small deposits of NZD 1000 coming into his account every couple of days. The source of the incoming funds was unknown as they were either cash or wire transfers. His trading pattern was not in line with common trading activity, for example, he would buy a few number of shares relating to one company and within a month sell the same number of shares on that same company at an excessive loss.

Although no evidence of market manipulation has been proved at this stage, the banks have red-flagged these transactions as a potential money laundering tactic.

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 Co-ordination 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. 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