

Financial Intelligence Unit
New Zealand Police

Quarterly Typology Report

First Quarter (Q1)

2014/2015

(Issued October 2014)

INTRODUCTION

This report is the first Quarterly Typology Report for 2014/2015 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 includes 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 will be disseminated to relevant New Zealand Police units, stakeholders (including the AML/CFT Supervisors, Ministry of Justice and New Zealand Customs Service) and interested private industry partners 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

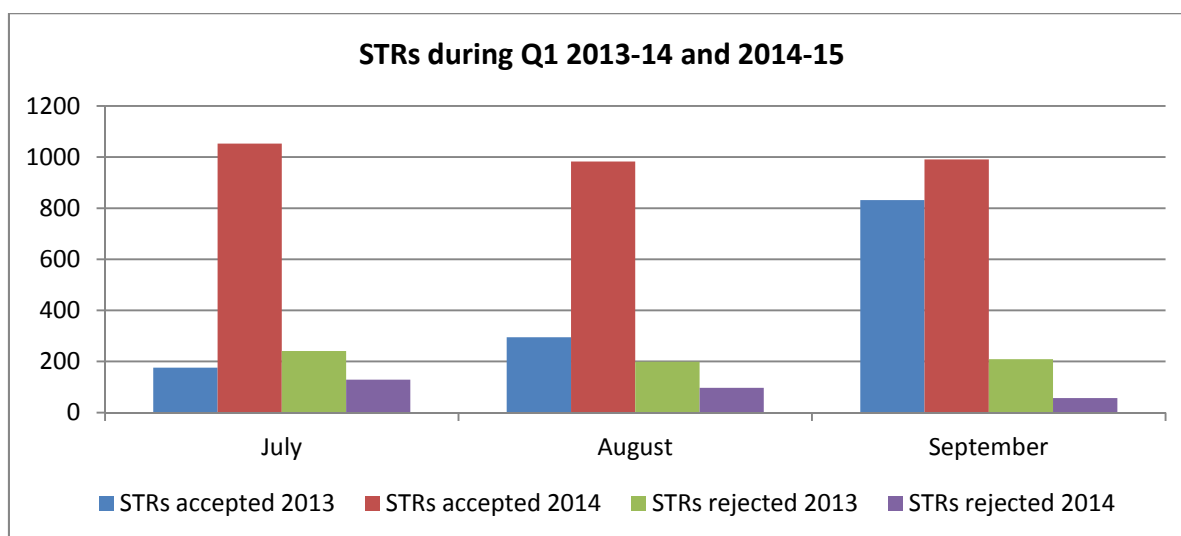
S.143 (b) Powers relating to financial intelligence functions of Commissioner: The Commissioner may - (b) share suspicious transaction reports, cash reports, suspicious property reports, and other financial information and intelligence with domestic and international authorities for the purposes of this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

STR reporting remained relatively steady throughout the first quarter of 2014-15 continuing a rate of around one thousand accepted reports per month. This rate of reporting is a significant increase on the first quarter of 2013-14 when the new reporting regime was introduced. The number of rejected STRs has also significantly reduced indicating an increase in the quality of reports.



APG ANNUAL MEETING

The 2014 Asia Pacific Meeting was held in Macau 14-18 July in Macau, China. New Zealand was represented by officials from the Ministry of Justice, the Department of Internal Affairs, the Ministry of Foreign Affairs and the FIU. The next annual meeting will be held in Auckland 13-17 July 2015, when around 400 delegates will be expected to attend. The APG Annual Meeting is the primary policy and decision-making vehicle for the APG and sets the course for the APG's work over the next year. More information on the APG and APG guidance material, including typologies studies, can be found at <http://www.apgml.org>

FIU-ACAMS SEMINAR

The next FIU-ACAMS Seminar is scheduled for 9-10 July 2015. Further details to be confirmed.

GOAML UPGRADE

The update of goAML, which was planned for 2014, has now been delayed until 2015. This is to prevent the update being undertaken concurrent to major updates of Police's systems.

AUSTRAC TERRORIST FINANCING REPORT

The Australian FIU, AUSTRAC, has published a public report based on its classified Terrorism Financing Risk Assessment. The report draws on real cases and intelligence to present a summary of Australian terrorism financing risks, vulnerabilities and the likely methods to be used in Australia. More information, and the report, can be found on the AUSTRAC website: <http://www.austrac.gov.au/terrorism-financing-in-australia-2014.html>

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: UPDATE - CORRECT AS AT 31 AUGUST 2014

Since the CPRA came into effect the ARUs have investigated assets worth an estimated \$387 million. At the end of August 2014:

- Forfeiture Orders for assets worth an estimated \$49.6 were in place (see key terms below).
- Restraining Orders were in place over assets worth an estimated \$160 million pending further investigation and court action (see key terms below).

NEW ZEALAND: GANG BOSS FORFEITS PROFITS OF METHAMPHETAMINE SUPPLY

In July 2014, the leader of the Wellington chapter of the Nomads motorcycle gang was ordered to forfeit five cars, one motorcycle, and two sums of cash that he had acquired through dealing in methamphetamine. Paul Rodgers, also known as Porky Rimene, was convicted in October 2011 of 11 charges including supplying methamphetamine, conspiracy to supply cannabis, and money laundering.² He was sentenced to fifteen years in prison. Forensic analysis of Rodgers' financial affairs showed that he had received at least \$800,000 from unknown sources between January 2009 and February 2011. The High Court ruled that this was likely to be a conservative estimate of what he made from drug dealing, dismissing Rodgers' claim that he had used large quantities of the drugs he bought to satisfy his own drug addiction rather than selling them on for profit. The assets forfeited include a 1965 Ford Galaxie, and 2004 General Motors Hummer, and a cash sum of \$88,305.³ The total value of the Forfeiture Order was an estimated \$219,970.

AUSTRALIA: USING ASSET FORFEITURE TO FIGHT TERRORISM

The Australian Federal Government has recently announced its intention to use the funds seized from organised crime to track down terrorism financing and money laundering schemes.⁴ AUS\$14 million (NZ\$15.6 million) will be used to expand the Criminal Assets Confiscation Taskforce, which believes that some organised crime groups are using illegal funds to support terrorist organisations. Intelligence suggests that up to 150 Australians overseas assisting are terrorist organisations and the Federal Government intends for this expansion to ensure that funds cannot reach them.

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 NZ\$ 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.

² <http://www.stuff.co.nz/national/crime/7633267/Gang-boss-Porky-jailed-for-drugs>

³ <http://www.stuff.co.nz/national/crime/7379643/Porkys-drugs-empire-outlined-by-associate>

⁴ <http://www.dailytelegraph.com.au/news/nsw/dirty-cash-from-organised-crime-will-be-used-to-track-down-terrorism-funding/story-fni0cx12-1227019862422>

Abuse of Trusts

New Zealand is known to have a very high ratio of trusts per capita reflecting a national predilection to arranging financial affairs using trusts. Research by the Law Commission found that in the year ending 31 March 2008, tax returns were filed for 237,500 trusts. The actual number of trusts at that time is likely to have been significantly higher as only trusts that earn income are required to file tax returns. In addition, New Zealand is likely to have several thousand foreign trusts (trusts where the settlor is resident overseas).

USE OF TRUSTS FOR LAUNDERING

While trusts may be an attractive means of ordering legitimate financial affairs, they are also attractive to money launderers and financiers of terrorism. Trusts can be used to facilitate laundering transactions at all stages of laundering. For example, placement may be achieved by depositing proceeds to a trust's bank accounts while proceeds may be integrated by purchase of property or assets in the trust's name. Trusts are also effective vehicles in the layering stage and may be used to create ostensive parties in a transaction, for example by shifting assets between a trust and other legal entities controlled by launders.

ATTRACTIVENESS

The principle attraction for launderers and terrorist financiers to trusts is their use to hide beneficial ownership or involvement of criminals in transactions. Trusts create a front behind which criminals may mask their activity. At the integration phase, trusts can be an effective means of dispersing assets while retaining effective control – and ultimate enjoyment of the fruits of criminal offending. During layering, trusts and other legal entities may be stacked, for example using trusts as shareholders of companies, to create complex legal structures. Such legal structures may obscure the involvement of the natural persons connected to the predicate offending. Trustees may be used as intermediaries in laundering transactions, which may allow especially complex and effective laundering where trustee service is provided by professional service providers. Trusts may also be used to mask criminal involvement in other laundering activity. For example, businesses used to co-mingle proceeds of crime may be distanced from offenders by using a trust controlled by the criminal as the shareholder of the business.

ATTRACTIVENESS TO TRANSNATIONAL LAUNDERERS

New Zealand's foreign trusts may also be used as a vehicle for international transaction by overseas launderers. Use of a New Zealand foreign trust may give the appearance of a transaction involving New Zealand. This may make the transaction appear benign by trading on New Zealand's reputation, or may simply obscure the money trail by adding the complexity of tracing money internationally. New Zealand's settlor-based tax regime also makes New Zealand foreign trusts an attractive vehicle for tax evasion as no tax is due in New Zealand where the settler is based overseas (most comparable jurisdictions tax based on the residence of the trustees).

CONTROLS

Because of the high level of risk associated with the opportunities to hide the identity of beneficial owners behind trusts, AML/CFT Act reporting entities must conduct enhanced customer due diligence when a trust:

- seeks to form a business relationship with the reporting entity [s22(1)(i)(a) refers]; or
- seeks to conduct an occasional transaction[s22(1)(i)(a) refers].

TCSPs were also included as AML/CFT reporting entities in the AML/CFT Act regulations. Other professionals involved in establishing and managing trusts, such as lawyers and accountants, are still subject to the Financial Transaction Reporting Act, but are planned to be included in the second tranche of the AML/CFT Act reform.

REPORTING TO THE FIU

504 STRs submitted between 1 January 2008 and 31 December 2014 were identified as relating to around 200 trusts. STRs included around 600 transactions amounting to over \$200million.

More detailed analysis was conducted on 33 STRs where sufficient information was received on the use of the trust. Transactions included in these STRs ranged in value from \$6,000 to \$2,000,000. The most common type of suspicious transaction in the sample was cash deposits to accounts held by the trust. Apparent layering activity was also common via electronic transfers between trusts' accounts, business accounts and personal accounts. For example, in two cases, frequent cash deposits were made to a personal account followed by a bulk transfer to a trust's accounts.

Five STRs related to large international transfers to New Zealand trusts from Russia, UAE, China and the US. All but one related to suspected proceeds of crime being transferred from an overseas company to the New Zealand trust's account in New Zealand. The other case related to funds transferred from offshore ostensibly to purchase real estate, but which were in fact partially transferred to a Bitcoin agent.

ARU EXPERIENCE

All four ARUs have seen extensive use of trusts in proceeds of crime cases. In the majority of these cases, the trusts were used to attempt to hide the beneficial ownership of assets. For example, bank accounts for trusts being used as a conduit for criminal proceeds to pay mortgages on property. In Operation Ark, described below, a trust was used as the nominee shareholder for several companies controlled by the offender. These companies in turn had nominee ownership of property which the offender retained enjoyment of.

New Zealand trusts have not been noted in terrorist funding cases. However, given the development of the foreign trust industry marketed to individuals overseas, there is a risk that New Zealand trusts may be used as a conduit for terrorist funds.

New Zealand Case Study

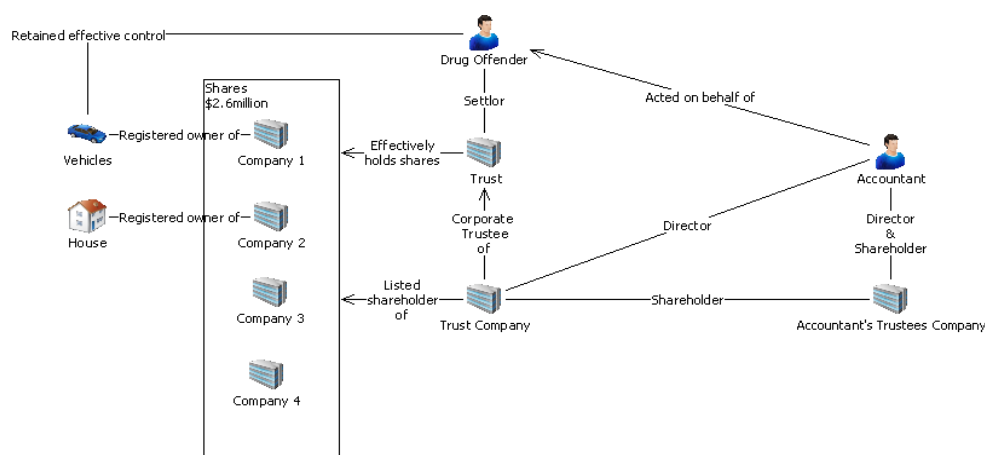
OPERATION ARK

In Operation Ark, other aspects of which were described in the Q2 2013/2014 Typology Report, drug offenders engaged an accountant to set up a complex structure of legal entities including a trust. This case demonstrates many of the principal ways trusts are used to launder proceeds, in particular:

- layering entities to hide the beneficial control of companies controlling assets,
- use of a professional service provider to access complex structures and act as an intermediary
- use of trust to hide criminal involvement in transactions.

The drug offender used the trust to buy shares in a fitness magazine business and a company with the proceeds of drug offending. Vehicles owned by the drug offender were then registered in the name of the company, ostensibly distancing the offender from ownership of the vehicles.

The offender also used his accountant as an intermediary and additional layer in the legal structure of his finances. Ultimately, as was the case in his layering of entities to hide ownership of the magazine and vehicles, the offender used the accountant and the trust to hide his own beneficial ownership of property. For example, the offender's house was put in the name of a company whose nominee shareholder was the accountant's trust company. The accountant's trust company was in turn holding the shares on behalf of the offender's trust.



Possible indicators:

- complex legal arrangements
- property owned by a company which is in turned owned by a professional intermediary
- ownership of property cannot be traced to a natural person

Overseas Case Study

CASE FROM THE FATF RBA GUIDANCE FOR TRUST AND COMPANIES SERVICE PROVIDERS (TCSPS)⁵

Use of professional intermediaries to facilitate money laundering

A criminal involved in smuggling into Great Britain set up a Trust in order to launder the proceeds of his crime, with the assistance of a collusive Independent Financial Adviser (IFA) and a Solicitor, who also appeared to be acting in the knowledge that the individual was a criminal. The Trust was discretionary and therefore power over the management of the fund was vested in the Trustees, namely the criminal, his wife and the IFA. This example illustrates the complexity of Trusts used to hide the origins of funds from any law enforcement scrutiny. One way in which funds were hidden was through the purchase of a garage. The criminal's daughter, who was a beneficiary of the trust, was given the property by her father and she in turn leased it to a company. The property was eventually sold to this company, the purchase funded by a loan provided by the Trust. The company subsequently made repayments of several thousand pounds a month, ostensibly to the Trust, but in practice to the criminal. Thus the criminal, who had originally owned the garage, probably maintained control despite his daughter's ownership. By controlling the Trust the criminal was able to funnel funds back to himself through loaning funds from the Trust and receive payment on that loan.

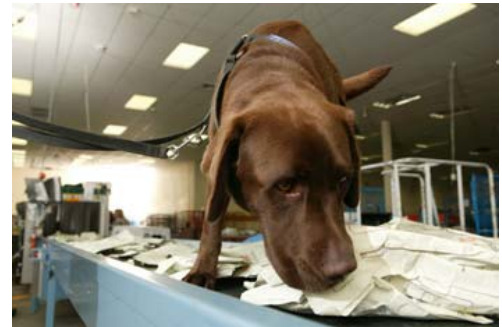
⁵ <http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20TCSPS.pdf>

Domestic and International AML/CFT News

NEW ZEALAND

Conviction Following First Drug Dog Interception

Customs' first interception using cash detector dogs has led to the conviction of a 59-year-old Auckland man. The man was about to board a flight to Hong Kong when the dog detected cash being carried by the man's wife. Subsequent searches of the man's, his wife's and their travelling companion's checked and carry-on baggage uncovered CNY 700,000 (NZD136,000). The money was apparently from legitimate income in China and was to be used to purchase property in Hong Kong. However, following the man's conviction for non-declaration of transport of the cash across the border, the money has been seized and the man fined an additional \$800.



UNITED STATES /NEW ZEALAND

New Zealand Alternative Banking Platform used in International Fraud

A Greek man was convicted in Boston in September of charges relating to an advance fee fraud targeting would-be developers. A New Zealand banking platform was created using a New Zealand company structure and a virtual office in Auckland. This banking platform was used to create accounts to re-assure victims that the "deposits" provided to the fraudsters were being used to secure loans for development projects. A website and online-banking facilities gave the impression that the deposits were safe and that the promised loan was being processed. However, in reality, the fraudsters had no intention of providing funding and the deposits were lost when the loans were ostensibly cancelled.

UNITED STATES

LA Fashion Industry Linked to Mexico Money Laundering

In September, seventy-five locations associated with the Los Angeles fashion industry were searched by American law enforcement agencies in relation to laundering proceeds of drug crime. At least USD 65 million has been seized and nine people arrested.



Prosecutors said other fashion businesses were being used to launder money from drug traffickers and other offenders in what is known as a "Black Market Peso Exchange" scheme. These searches, arrests and seizures relate to apparent use of fashion businesses to receive bulk cash proceeds and to then move funds back to cartels in Mexico using trade-based laundering.

Asset forfeiture targeting foreign corruption

The US Department of Justice has forfeited more than US\$480 million (NZ\$616 million) from the estate of General Abacha, who held the office of the president of the Federal Republic of Nigeria from 1992 until his death in 1996. Abacha, along with his son and other associates, is alleged to have misappropriated and extorted billions from the government of Nigeria, and to have laundered these funds through US financial institutions and through the purchase of bonds backed by the US.

This civil forfeiture action is the largest brought by the Department of Justice, and included funds from bank accounts in Jersey, France, the UK and Ireland. Claims to an additional US\$148 million (NZ\$190 million) in four investment portfolios in the UK are pending.

AUSTRALIA

Terrorist Funding and Terrorism Related Arrests

A 23 year old Melbourne man was arrested and charged in September on seven counts of funding terrorism. The charges relate to alleged provision of \$12,000 to support an American citizen fighting in Syria and alleged provision of funds to the Islamic State and Jabhat al-Nursa on multiple occasions between March and September. The man's arrest followed an eight month investigation initiated by information received from the FBI. Due to the complexity of the ongoing

⁶ <http://www.infozine.com/news/stories/op/storiesView/sid/59612/>

investigation, the court granted police an extension to finalise evidence and the committal hearing is now scheduled for 3 February 2015.

The terrorism funding arrest follows an apparently unrelated incidence in which an 18-year old Victoria man carrying an Islamic State flag was shot dead by counter-terrorism Police after he stabbed two officers. The terrorism funding case also follows arrests related to an alleged plot in Sydney to carry-out random terrorist attacks on individuals.

AUSTRALIA /INDIA

Australia – India Arrests Relating to Transnational Money Laundering

Australian and Indian law enforcement agencies conducted coordinated arrests in both countries following an investigation of alleged transnational money laundering in foreign exchange and remittance businesses. The businesses allegedly mixed proceeds of drug offending with legitimate transactions, including routing Australian proceeds of crime through Hong Kong-based businesses to other countries.

UNITED KINGDOM

Collaboration with the UAE to tackle overseas money laundering

Working in cooperation with UAE agencies, the UK government has recently recovered more than AED1.8 million (NZ\$628,366) from the sale of a Dubai Marina apartment owned by a British drug dealer, Redwan El Ghaidouni, who was convicted in 2011 for importing and possessing drugs.⁷

⁷ <http://www.thenational.ae/uae/uk-recovers-dh18m-from-sale-of-drug-dealers-dubai-apartment>

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 which 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