Financial Intelligence Unit
New Zealand Police

Quarterly Typology Report
First Quarter (Q1)
2013/2014

INTRODUCTION

This report is the second Quarterly Typology Report of 2013 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 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).

AML/CFT ACT 2009 COMMENCEMENT

The AML/CFT Act 2009 fully commenced on 30 June 2013. All reporting entities subject to the AML/CFT Act should now have their AML/CFT measures and processes in place including:

- appointment of an AML/CFT officer;
- completion of a risk assessment to understand the reporting entities' unique risks so that the risk based approach can be used;
- implementation of Customer Due Diligence (CDD) and Know Your Customer (KYC) processes; and
- reporting Suspicious Transaction Reports (STRs) through the FIU's new goAML system (refer to FIU guidance material[2] for more information).

Entities such as lawyers, accountants and other Designated Non-Financial Businesses and Processionals (DNFBPs) remain subject to the Financial Transaction Reporting Act 1996.

Supervisors Commence Monitoring

The full AML/CFT supervisory regime began with the commencement of the AML/CFT Act on 1 July. The three AML/CFT supervisors (the Reserve Bank, the DIA and FMA) have several functions under the AML legislation, of which the key ones are:

- monitoring and assessing the risk of money laundering across reporting entities;
- monitoring reporting entities for compliance with the legislation; and
- investigating reporting entities and enforcing compliance with the legislation.

Each of the supervisors has already been fulfilling the first function by assessing the risk of money laundering across its sector in their sector risk assessments. Since 1 July, supervisors have now also commenced the monitoring compliance function. This monitoring activity will lead into the third function as it will alert supervisors to the majority of potential breaches of AML/CFT requirements requiring investigation and enforcement.

The supervisors have developed a range of tools to monitor their reporting entities' compliance including onsite inspections, desk-based reviews and surveys or questionnaires.

FIU TRAINING

During September, the FIU has conducted half and full day training with staff from banks and money remitters. Session have had different objectives, but they were generally focused on:

- the purpose of STRs and why STR reporting important to the FIU;
- why STR reporting should be important to reporting entities; and
- explanation of issues the FIU is experiencing with STRs submitted through goAML's Web Form entry

Further sessions are planned throughout the rest of 2013.

FATF Identifies Jurisdictions with Strategic AML/CFT Deficiencies[3]

The Financial Action Task Force (FATF) released a public statement (October 2012) listing high-risk and non-cooperative jurisdictions. In particular, FATF continues to call on its members and other jurisdictions to apply counter-measures against Iran and the Democratic People's Republic of Korea (DPRK). These jurisdictions have strategic deficiencies around money laundering and terrorist financing and pose a risk to the international financial system. See the FIU's website http://www.police.govt.nz/about-us/publication/financial-action-task-force for further details.

APG Typology Report

The 2013 Asia Pacific Group on Money Laundering (APG) Typology report was released in July. As part of the APG's role to conduct research and analysis into money laundering and terrorist financing trends and methods, it produces a yearly typology report including case studies from around the region. For more information, see the "Spotlight on…" section below.

[2] Guidance on goAML can be found at http://www.police.govt.nz/advice/businesses-and-organisations/fiu/goaml guidance on STR reporting can be found at http://www.police.govt.nz/sites/default/files/publications/fiu-guidelines-reporting-suspicious-transactions.pdf

[3] http://www.fatf-gafi.org/media/fatf/documents/FATF%20Public%20Statement%2019%20October%202012.pdf.

Asset Recovery Unit Update

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.

ASSET RECOVERY UNITS: UPDATE - CORRECT AS AT 31 MAY 2013

There are four Asset Recovery Units (ARUs), based in Auckland, Hamilton, Wellington, Christchurch. Since the CPRA came into effect the ARUs have investigated assets worth an estimated $293 million. At the end of August 2013:

- forfeiture Orders for assets worth an estimated $30.5 were in place (see key terms below); and
- restraining Orders were in place over assets worth an estimated $134.8 million pending further investigation and court action (see key terms below).

NEW ZEALAND: MOTEL DRUG MANUFACTURING RING DISMANTLED

July 2013 saw the final blow landed against an organised crime group manufacturing methamphetamine out of a motel in Auckland. Operation Jacaranda targeted a syndicate headed by Zhong Jie Tang who allowed his leased motel to be used for the manufacture and supply of methamphetamine. The methamphetamine was 'cooked' in the kitchen above the restaurant after closing time in what has been described as one of the "largest clan labs found" in New Zealand[4]. The drugs were then distributed by a syndicate that included a company director who lived in a $2.4 million property in Remuera. Profit Forfeiture Orders have now been made and assets forfeited to the Crown with a total estimated value of almost $1.5 million (see key terms).

NEW ZEALAND: MSD TARGETS BENEFIT FRAUDSTER

In July 2013 a Forfeiture Order was imposed on a Bay of Plenty woman after falsely claiming benefits. The woman, who was alleged to have made false representations to the Ministry of Social Development over a five year period, was in a relationship at the time of her offending and, thus, was not entitled to receive the sole parent benefit she claimed. The woman was order to return more than $70,000 to the government under the CPRA.

NEW ZEALAND: STUDENT CHEATING WEBSITE INVESTIGATED

An internet company is being investigated by New Zealand Police after claims that it was selling papers to tertiary students attending universities and polytechnics across New Zealand. Allegations were made that the website was providing assignments for up to $500 each. Criminal charges may be brought under the Crimes Act 1961 or the Education Act 1989. Assets worth an estimated $3.7 million have been restrained from the company directors while further investigations take place.

INTERNATIONAL: MONEY LAUNDERING IN MANHATTAN

Authorities in the US have moved to seize millions of dollars of Manhattan real estate[5]. The assets are the property of a Cyprus based real estate corporation alleged to have benefited from an elaborate tax fraud scheme designed to steal US$230 million from the Russian state. This corporation, along with eight of its subsidiaries, is alleged to have laundered the money through the purchase of luxury condominiums and commercial spaces in New York.

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.

[4] http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10738821
[5] http://www.rferl.org/content/us-seeks-seizure-of-manhattan-real-estate-magnitsky-fraud-scheme-prevezon/25102020.html

Money Laundering Typology: Wire Transfers

The wire transfers typology refers to launderers transferring proceeds of crime from one person to another via money remittance services.

Wire transfers were assessed as the highest risk typology to New Zealand in the National Risk Assessment. Abuse of wire transfers presents an opportunity to domestic criminals to:

- attempt to place proceeds of crime out of sight and reach of New Zealand law enforcement;
- use other jurisdictions to layer funds before returning laundered criminal proceeds to use in New Zealand; and
- expatriate proceeds of crime overseas to criminals involved in New Zealand offending.

Abuse of wire transfers also exposes the New Zealand financial system to international money laundering threats and exposes New Zealand individuals to victimisation by transnational criminals. The financial system may be abused by overseas launders of proceeds of crimes such as corruption; tax evasion; drugs and people trafficking and fraud. Transnational criminals may chose to wire funds to New Zealand to:

- invest criminal proceeds in a safe haven beyond the visibility and/or reach of the authorities where the predicate offence was committed; and/or
- use New Zealand institutions in the layering stage of money laundering; for example, by transferring funds to New Zealand, or making New Zealand investments, and quickly remitting the funds off shore again.

Individuals may also fall victim to exploitation of wire transfers by either being victimised in scams or becoming unwitting money mules as is highlighted in one of the New Zealand case studies below.

POSSIBLE INDICATORS

- Significant and/or frequent cash payments for transfers
- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption[6]
- 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

[6] Refer to the FIU website for the FATF list of high risk jurisdictions: http://www.police.govt.nz/about-us/publication/financial-action-task-force

Terrorism Financing: wire transfers

TERRORISM FINANCING AND WIRE TRANSFERS

Given the low risk of domestic terrorism, off-shore remittance of money is a particular area of terrorism financing risk for New Zealand.

Terrorist financing may exploit the same vulnerabilities in the remittance system as money laundering. Therefore, the controls established to detect money laundering are applicable to detect and prevent terrorist financing.

However, understanding key differences between money laundering and terrorism financing is important. By definition money-laundering occurs after crime while terrorist financing occurs pre-crime to facilitate the crime (although in practice money-laundering may be used to fund further offending and terrorist financing may derive from earlier offending). Unlike money launderers, terrorist organisations can raise funds through legitimate sources as well as criminal activity. Terrorist activity can often be conducted for relatively low costs, particularly in the third world, and as a result, terrorist financing may involve small amounts of money.

Overseas experience has highlighted the particular use of identity crime, unwitting 'smurfs', abuse of charitable organisations and obscured final destination in terrorism financing in wire transfers for terrorist financing. These factors mean that it may be difficult to detect terrorist financing by wire transfer at face value – for example, in overseas cases terrorist financiers have obscured their activity by using false names while wiring charitable donations to a regional financial hub where the funds were diverted to fund terrorist groups in third countries using alternative remittance networks.

Therefore, it is important that entities use a risk-based approach and be aware of indicators (for more information refer to the FIU guidelines).

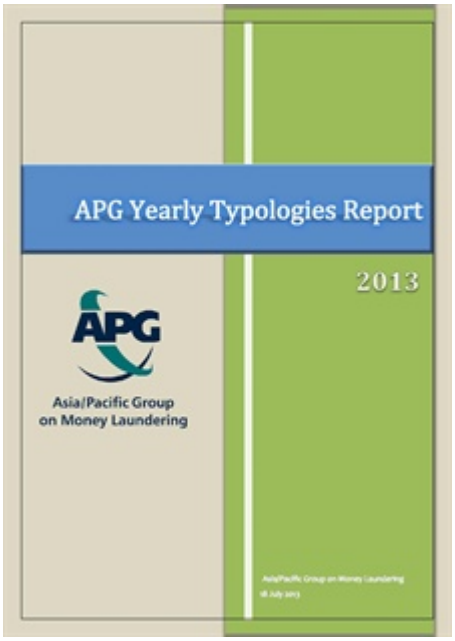
New Zealand designated terrorist list

Reporting entities should also take steps to ensure that they are able to detect wire transfers involving entities on the terrorist designation list on the Police website: http://www.police.govt.nz/about-us/publication/designated-terrorist-entities.

TERRORIST FINANCING INDICATORS:

- individuals using false names to undertake international funds transfers, particularly to high risk-jurisdictions. This may include an individual of one gender giving instructions that an international funds transfer be carried out in the name of an individual of the opposite gender.
- individuals, often from the same cultural background as overseas terrorist groups, using their personal bank accounts to transfer funds offshore to provide support for terrorism activities overseas,
- significant and/or frequent cash payments for transfers
- transfers to numerous offshore jurisdictions with no business rationale
- multiple transfers sent to same person overseas by different people
- same contact details appearing in multiple transfers, such as the same home address being provided by multiple remitters or the same phone number for multiple recipients
- reluctance to provide retailer with identification details or the use of false identification.

Spotlight on....the APG Typology Report



The Asia/Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organisation with 41 members from across Asia and the Pacific and a number of international and regional observers. One of the APG's functions is to conduct research and analysis into money laundering and terrorist financing trends and methods to better inform APG members of systemic and other associated risks and vulnerabilities.

In August the APG published the 2013 APG Yearly Typologies Report based on information on money laundering and financing of terrorism cases, trends and research provided by APG members and observers. The Report includes observations on money laundering and financing of terrorism techniques and methods from across the APG. These observations are intended to assist with identifying instances of suspicious financial activity in the real world.

Case studies and 'red flag' indicators included in this report will assist front-line financial institutions and non-financial businesses and professions (casinos, accountants, lawyers, real estate agents etc.) involved in implementing preventative measures including customer due diligence and suspicious transaction reporting.

The case studies featured in the report offer an insight to money laundering and terrorist financing across the Asia-Pacific regions along with work to detect and combat money laundering and terrorist financing. The FIU will publish selected APG case studies in QTRs. Reporting Entities should also familiarise themselves with the APG report to ensure that they are exposed to case studies that are relevant to their own particular business' circumstances and risks.

The full Report can be downloaded from the APG website at: http://apgml.org/news/details.aspx?pcPage=1&n=18

New Zealand Case Studies

The Love Struck Mule

A New Zealand woman became ensnared in two related scams that are unfortunately all too common. In the first scam, the woman was victimised in a romance scam after meeting a man living in Nigeria on an online dating site. After a period of online chatting, the scammer convinced the woman to make several wire transactions over a few days to Nigeria, supposedly to pay for airline tickets for the scammer to come to New Zealand.

When the scammer did not arrive in New Zealand the woman became suspicious and made a statement to Police that she was the victim of a scam. Contact from the scammer ended for several months leaving the woman several thousand dollars out of pocket as a result of the scam.

Months later, the scammer resumed contact the woman to initiate a second scam that would see the woman became an unwitting accomplice in money laundering. The scammer told the woman that a friend would transfer money from a New Zealand account to the woman's bank account. The woman was to withdrawal the money in cash and wire the money to several bank accounts in different South East Asian countries minus the money that the woman had "loaned" the scammer.

Unbeknown to the woman, the email address of the other New Zealand account holder had been hacked and fraudulent instructions had been send to the New Zealand bank. The woman's bank became suspicious when its account monitoring detected the money transfers being quickly followed by withdrawals and identified that she was being used as a mule. The woman's bank reported the matter to Police. The subsequent Police enquiry resulted in a formal warning for the woman for the Crimes Act Money Laundering offence.

STRs were received in relation to the transactions where the woman was used as a money mule. However, no STRs were received in relation to the initial wire transfers to Nigeria relating to the original scam despite the indicators (below). While there is no indication of money laundering in the initial scam transactions, reporting entities should be mindful that STRs must be submitted where there is suspicion that the transaction may be relevant to the investigation of any serious offence. In this case sections 240 *Obtaining by Deception or Causing Loss by Deception* and 249 (1) *Assessing a Computer System for Dishonest Purpose* of the Crimes Act 1961 would be relevant.

Typologies: wire transfers; cash deposits; electronic transfers; use of third parties

Money Laundering Indicators:

- Deposits quickly followed by cash withdrawal
- Multiple international wire transfers over a short time period
- Multiple transactions to structure transaction

Scam Indicators:

- Multiple wire transfers over a matter of days
- Wire transfers to high risk scam jurisdiction

New Zealand Shell Company Implicated in Suspected Attempted Sanctions Violation

A New Zealand registered company approached the client of an overseas-based law-firm seeking to buy a hotel in a third country. The law firm became suspicions about the transaction when it discovered that the owners of the New Zealand company did not have legal representation for the sale despite the size of the transaction which was in the tens of millions of dollars.

Know your customer and customer due diligence processes raised a number of additional concerns relating to individuals involved in the transactions. Firstly, the Iranian owners of the New Zealand company had passports issued by a State known to sell passports. In addition, the law firm could not find any indication that the owners had any real connection to New Zealand or the country where their passports were issued.

The transaction was to involve two New Zealand Companies. The company making the purchase and a second company that was to loan money to the first. However, the law firm could not establish the relationship between the two companies. In addition, the law firm could not establish what either company actually did or how the capital involved in the loan had been made.

The transaction for the New Zealand company to purchase of the hotel also raised the law firm's suspicions as the purchase was to be funded through an unusually complicated transaction structure which the law firm could not account for. The New Zealand company was proposing to raise funding by selling shares and through a loan from the second New Zealand company. Finally, a bank cheque drawing on Bank Melli (the Iranian national bank) was presented to pay for the purchase.

Based on these red flags, the law firm and the client became suspicious that the transaction was an attempt to circumvent sanctions against Iran. Based on the evaluation of the high risk of sanctions evasion, the client decided not to proceed with the transaction.

It seems likely that the Iranian nationals obtained passports from the offshore State and set up a New Zealand shell company and structured the complicated transaction to obscure the Iranian origin of funds that they were attempting to move from Iran.

Typologies: use of false identity; use of shell companies; real estate; use of shares

Indicators:

- Nationals of a State subject to sanctions using a company from a third country
- Individuals involved had newly issued passports from a country known to sell passports
- Unusually complex transaction
- Obscure origin of funds and business of companies involved in transaction.

Asia-Pacific Group Typologies[7]

The following case study has been taken from the 2013 APG Typologies Report. The APG is an autonomous intergovernmental organisation and the FATF style organisation for the Asia-Pacific region. As part of the APG's role to conduct research and analysis into money laundering and terrorist financing trends and methods, it produces a yearly typology report including case studies from around the region.

Fiji

A local business director remitted business funds into his multiple personal bank accounts in Country K. Business funds totalling FJ$378,783 (USD205,526) was remitted to multiple bank accounts maintained at different commercial banks in different localities of Country K over a period of 3 years.
Common suspicious indicators included:

- Director remitting multiple large remittances ranging from $5,000 to $15,000.
- Total of $378,783 outward remittances over a period of 3 years.
- Funds were remitted into multiple bank accounts in Country K.
- Bank accounts were maintained in different branches of the commercial banks in Country K.
- The director was using money remittance services to remit large cash transactions.

The suspicious transaction patterns of the individual raised a high flag on all the transactions of the business director. A proactive STR (PSTR) was raised internally by Fiji FIU (using an intelligence software: the Alert and Monitoring System & Data Mining System - AMS/DMS) for further background checks on the business director.

During the analysis it was established that the director held permanent residency status in Country K and made frequent payments to his Visa debit card through a foreign exchange company.

He breached the Central Bank's Exchange Control requirements by not providing proper tax clearance documents for the payments made to his Visa debit card. Furthermore it was established several of his business accounts were closed on the same day. After further analysis the FIU established a possible tax evasion offence and the case was referred to the local tax authority for further investigations.

[7] **APG Yearly Typology report 2013**
http://www.apgml.org/methods-and-trends/page.aspx?p=8d052c1c-b9b8-45e5-9380-29d5aa129f45

Domestic and International AML/CFT News

NEW ZEALAND:

Man sentenced for price hydraulicking and related money laundering

In January, a New Zealand man was sentenced to two years nine months imprisonment for dishonestly using a document and money laundering in relation to "price hydraulicking" to obtain 100% or greater mortgage funding. The fraud involved same day purchases and on-sale of particular properties at significantly different purchase prices; the purchase price on the greater value sale and purchase agreement being relied upon to obtain finance.

Once the two property transactions were completed, the settlement fund were paid to the vendor and the rest (the pecuniary gain) was distributed through third parties' (in this case exchange students living with the offender) accounts into a trust account or another account controlled by the offender.

Cash dogs

Drug detector dogs are now being trained to target the proceeds of crime by detecting large amounts of cash.

A recent trial involving two detector dogs from Police and Customs resulted in the seizure of over $350,000 in undeclared or concealed cash at Auckland International Airport, and while carrying out search warrants. The trial was so successful that Police are now training a further seven "cash dogs" and Customs another five, for operational use around the country.

The dual-trained dogs will be able to detect cash amounts of over $10,000, targeted at New Zealand, Australian and US currencies, as well as narcotics. Following training, the Customs dogs will be operational in Auckland, Wellington and Christchurch. The Police dogs will be based in Auckland, Bay of Plenty, Eastern, Wellington, Canterbury and Southern districts.

SWITZERTLAND

On 29 August, Swiss and US authorities jointly announced a new arrangement that will provide a voluntary programme for Swiss banks to gain protection from prosecution in return for cooperation with US efforts to curb tax evasion.

The programme includes a tiered framework for banks seeking non-prosecution that is designed to impose the greatest penalty on banks that have actively solicited customer leaving Swiss banks already under investigation by US authorities for facilitating tax evasion, with banks to pay up to 50% of the aggregate value of accounts opened after 28 February 2009. Banks that can demonstrate that they have not violated US law may obtain a 'non-target letter' and avoid penalty.

Banks will also be required to take measures to assist US authorities track down tax evasion, including a requirement to provide detailed anonymised account information to assist US authorities make formal requests for information under the US-Swiss tax treaty.

RUSSIA

In July, Russian police reported the discovery of a US$1.1billion money-laundering scheme involving more than 400 people.

The money-laundering operation used commercial banks and 100 Russian and foreign companies, including very short lived shell companies, to funnel money off-shore to be invested in real-estate in Cyprus and the Baltic states. Unusually, the criminals reportedly made a 2 percent profit on the money laundering operation.

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