Financial Intelligence Unit
New Zealand Police

Quarterly Typology Report
Second Quarter (Q2)
2014/2015

Issued January 2015

INTRODUCTION

This report is the second Quarterly Typology Report of 2014/15 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:

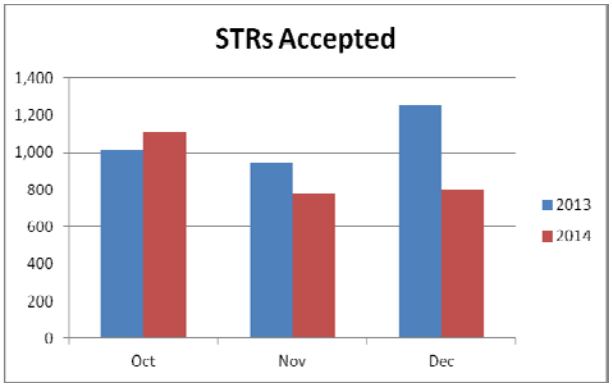
- Collect funds intended to be used for a terrorist act or intended for an entity known to carry out terrorist acts
- Knowingly deal with any property owned or controlled by a designated terrorist entity
- Make financial services available to a designated terrorist entity

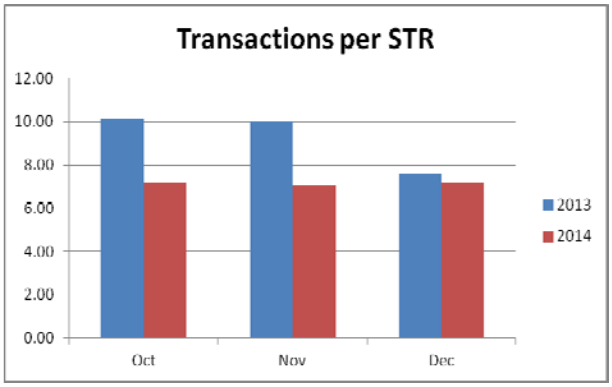
1 S.142 (b) Financial intelligence functions of Commissioner: The financial functions of the Commissioner are to - produce guidance material, including: (i) typologies of money laundering and financing of terrorism transactions
S.143 (b) Powers relating to financial intelligence functions of Commissioner: 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.

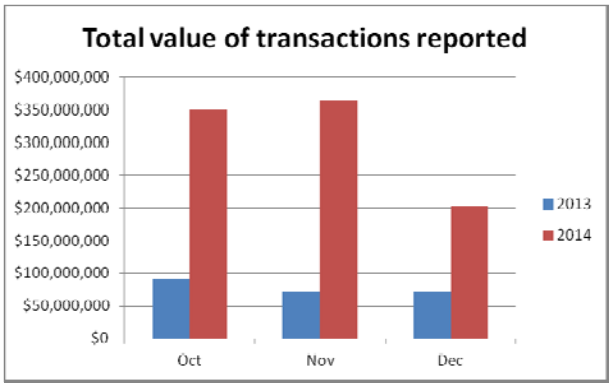
Financial Intelligence Unit and partner agencies updates

FIU STATISTICS

The number of STRs accepted by the FIU fell from November 2014 (to 774 in November and 798 in December compared to 1108 in October) and the numbers of STRs accepted in November and December 2014 were less than in the same months during 2013 (774 and 798 in 2014 compared to 943 and 1253 in 2013). The number of STRs per transaction was also less in October and November 2014 compared to the same months in 2013 (around 7 transactions per STR in 2014 compared to 10 in 2013). By contrast, the value of money in reported transactions was significantly higher in October, November and December 2014 compared to the same months in 2013 (averaging $300 million in 2014 compared to $77 million in 2013).







STR "GOLD" CONTRIBUTES TO MULTIPLE ARRESTS

An STR submitted in August 2014 led to FIU analysis that directly contributed to multiple arrests relating to a major cannabis cultivation operation.

The initial STR was submitted following bank suspicions raised by unusual cash deposits. Further analysis of the customer's account identified suspicious purchases consistent with drug cultivation.

The FIU identified links to historic offending by the depositor and linked the company that the customer was making purchases from to a previous Police investigation. The subsequent FIU report collaborated District police's suspicion that the subject of the STR was involved in a major cannabis cultivation operation. The report gave District police lines of enquiry that were described as "gold" in identifying and investigating the criminal operation. Subsequent STRs also contributed to the investigation.

Multiple parties were arrested when the investigation terminated and court proceedings are in progress.

FIU and STR information has initiated and/or contributed to several other significant investigations during the last quarter which will be reported on as information is made public.

MONEY LAUNDERING CRIME SCRIPTS RESEARCH PUBLISHED

Research by the New Zealand Police Research Fellow at Massey University was recently published in the European Review of Organised Crime on the steps to laundering using high value assets and cash intensive businesses. Both of these activities are common and high risk money laundering methods for many types of offender. Understanding the processes involved in these techniques may help reporting entities recognise hard to spot transactions used by these offenders. The article can be found at: http://sgocnet.org/site/wp-content/uploads/2014/06/Gilmour_3_35-56.pdf

APG TYPOLOGIES WORKSHOP

The 2014 APG Typologies Workshop was held jointly with the FATF in Bangkok on 24-26 November 2014 in Bangkok. The event was attended by approximately 250 delegates from 54 jurisdictions and eight international organisations. In addition to the plenary discussions there were three parallel typologies workshops:

- Transparency of beneficial ownership

- Third party money laundering
- Trade-based money laundering

Following the Typologies workshop, the APG held two technical seminars on 27-28 November on:

- Making Asset Recovery Work
- AML/CFT and New Technology: Understanding Cyber and Technology Enabled Crime

A member of the FIU represented New Zealand at the meetings and gave presentations on New Zealand's experiences to all workshops and seminars with the exception of the third party workshop. In addition, New Zealand, along with Canada, China and Chinese Taipei, provided sponsorship funding to assist some APG delegates and subject matter experts to attend and contribute to the event.

AUSTRAC TYPOLOGY REPORT

The 2014 Austrac Typology report is now available. Austrac describes the report as including: "20 real-life case studies showing how legitimate services offered by Australian businesses have been exploited for criminal purposes, including international drug smuggling operations, people smuggling and human trafficking syndicates and sophisticated overseas tax evasion schemes." The report can be found at: http://www.austrac.gov.au/typologies-and-case-studies-report-2014

ORGANISED CRIME BILL

The Organised Crime and Corruption Bill received its first reading in November 2014 and was referred to the Law and Order Select Committee. The Bill is an omnibus Bill and includes amendments to the AML/CFT Act to introduce reporting for international transactions (with a threshold of $1,000) and for large cash transactions (with a threshold of $10,000). The closing date for submissions is Thursday, 5 February 2015.

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 DECEMBER 2015

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

- Forfeiture Orders for assets worth an estimated $50.7 were in place (see key terms below).
- Restraining Orders were in place over assets worth an estimated $187 million pending further investigation and court action (see key terms below).

NEW ZEALAND: TRANSNATIONAL CO-OPERATION RESULTS IN RESTRAINT OF HIGH-END PROPERTIES

The Organised and Financial Crime Agency, New Zealand has restrained assets valued at an estimated NZ$8.5 million as part of Operation Roller. Operation Roller was established as part of a wider strategy to target the supply of methamphetamine in New Zealand, and focused on three individuals, all of whom were arrested when methamphetamine to the value of NZ$4.5 million was found in their possession[2]. The investigations were undertaken as part of wider co-operation between New Zealand Police and Chinese authorities, which has resulted in several successful operations targeting the transnational methamphetamine trade. The assets restrained in this operation include a high-end Audi R8, a Mercedes-Benz E500, 17 bank accounts and cash sums totalling $3.3 million, and 8 residential properties in Auckland, that are valued at an estimated $4.9 million.

NEW ZEALAND: TRANSNATIONAL CO-OPERATION RESULTS IN RESTRAINT OF HIGH-END PROPERTIES

Three houses and motor vehicles valued at an estimated $2.6 million have been restrained from an Auckland couple, Paul and Jane Rose, who have been charged with defrauding Mighty River Power. Rose had worked as an engineer at the Penrose power station and was responsible for identifying what services and equipment were needed for the plant[3]. It is alleged that during the period June 2005 to December 2012, Rose used his position to issue fraudulent invoices for goods that were not provided or services that were performed by other people or companies[4].

AUSTRALIA: USING ASSET FORFEITURE TO FIGHT OVERSEAS CORRUPTION[5]

The Australian Federal Police (AFP) is assisting the Chinese government with the extradition and seizure of the assets of officials who have fled to Australia with hundreds of millions of dollars gained from corrupt dealings. Beijing officials have identified that Australia is one of the most popular destinations for economic fugitives and have drawn up a priority list of targets from whom they intend to seize and forfeit assets. Corrupt officials will commonly send their families overseas, investing in what appear to be legitimate assets such as houses, shares, and bank accounts. When the time is right they then join their families.

In addition to joint operations between the AFP and Chinese authorities, the Australian government is strengthening its integrity measures to ensure that the Significant Investor Visa scheme, which offers residency in return for investment in the Australian economy, cannot be misused by corrupt officials fleeing from China.

UNITED STATES: CORRUPT OFFICIALS TARGETED BY THE KLEPTOCRACY ASSET RECOVERY INITIATIVE

The US Department of Justice is seeking the forfeiture of nine properties estimated to be worth US$1.5 million alleged to have been bought with a US$2 million bribe paid to Mario Zelaya, the former Executive Director of the Honduran Institute of Social Security[6]. Zelaya was the Executive Director of a Honduran government agency that provides social security services, such as retirement, maternity, and death benefits. He is alleged to have solicited and accepted US$2.08

[2] http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11358498
[3] http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11333790
[4] https://www.sfo.govt.nz/n464,25.html
[5] http://www.smh.com.au/world/australia-set-to-seize-assets-of-corrupt-chinese-officials-20141019-118kl3.html
[6] http://www.yumanewsnow.com/index.php/news/latest/9349-department-of-justice-seeks-recovery-of-approximately-1-528-000-in-bribes-paid-to-a-honduran-official

million from an IT company in exchange for prioritising and expediting payments to them and two of their Board of Directors. The funds were laundered into the US and used to buy properties in the New Orleans area.

The forfeiture action is being taken by the US Kleptocracy Asset Recovery Initiative, which aims to trace and recover the ill-gotten gains of public officials.

In a similar action taken by the US Kleptocracy Asset Recovery Initiative, the Second Vice President of Equatorial Guinea has agreed to hand over more than US$30 million of assets purchased with the proceeds of corruption. According to documents gathered during the course of an investigation undertaken with the assistance of the French authorities, Nguema Obiang used his position as a government minister to amass more than US$300 million through corruption and money laundering. He is alleged to have used intermediaries and corporate entities in the US to acquire numerous assets including a US$30 million mansion a Ferrari, and various items of Michael Jackson memorabilia.

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.

Abuse of Shell Companies

A shell company is a company that is used as a vehicle to conduct transactions but does not have significant operations or assets. Although there are some legitimate business uses for shell companies, shell companies are often abused in tax avoidance, fraud and large scale money laundering.

Using companies to conduct laundering transactions offers criminals several advantages. In particular companies:

- allow criminals to conceal the involvement of natural persons as the company conducts transactions while beneficial control of the company is hidden behind nominee directors and/or shareholders
- create the appearance of legitimate business transactions.

In particular, New Zealand company structures are attractive to launderers as:

- New Zealand's reputation as a well-regulated jurisdiction provides a veneer of legitimacy and credibility
- it is easier and cheaper to register companies in New Zealand than in other jurisdictions, meaning that New Zealand companies are essentially disposable, being easily and cheaply replaceable if offending is detected or the company is struck off
- historically, there was no need to have substantive links to New Zealand.

ATTRACTIVENESS TO TRANSNATIONAL LAUNDERS

Shell companies may be particularly attractive to launders engaged in large transnational transactions as use of a company may give the appearance of normal international business or investment, while obscuring the involvement of natural persons from law enforcement.

In particular, shell companies may be used to facilitate ostensive international investment transactions or trade based laundering.

Abuse of shell companies by transnational launderers is particularly concerning as New Zealand reporting entities may be targeted by offshore shell companies making CDD and KYC difficult, while New Zealand companies may be abused overseas exposing New Zealand's reputation to new money laundering threats.

POLICE EXPERIENCE OF SHELL COMPANIES

Although abuse of shell companies is primarily associated with transnational offending and overseas based threats, there has been some experience of this type of laundering by domestic offenders. Analysis of 57 high value Criminal Proceeds (Recovery) Act 2009 cases found that shell companies and similar arrangements were used in cases accounting for 30% of the total assets restrained in the sample. In particular, shell companies and similar structures were used in 29% of the fraud cases, which accounted for 71% of assets in fraud cases.

Two other examples where shell companies were used by domestic criminals are discussed in the case studies below, these are:

Operation Name	Value of Criminal Proceeds	Criminal activity
Op Major	NZ$135million	Drug trafficking
Op Starlifter	NZ$100 million	Tax evasion

However, the majority of the FIU intelligence regarding the abuse of New Zealand shell companies has come from overseas partners, or from investigation of shell companies involved in offending overseas. For the most part, this information relates to laundering of proceeds of crime generated overseas that flow through New Zealand companies' bank accounts commonly held in Eastern European countries such as Latvia, Lithuania and Estonia. Reports have also identified accounts held in Europe (Belgium and Germany) and island nations such as Cyprus and Mauritius.

High profile cases of overseas exploitation of New Zealand shell companies include:

Company Name	Amount of Criminal Proceeds	Criminal activity
SP Trading Ltd	US$18 million	Smuggling military weapons from North Korea to Iran. Account held in Estonia.
Tormex Ltd (see case study below)	US$680 million	Money laundering for various criminals including US$40 million of drug proceeds generated by the Sinaloa drug cartel in Mexico. Account held in Latvia.

Domestic intelligence shows that New Zealand bank accounts have also been used by overseas criminals exploiting New Zealand shell companies. Often these bank accounts are operated by a New Zealand Trust and Company Service Provider. For example, approximately 70 STRs have been received regarding transactions in New Zealand bank accounts held for suspected New Zealand registered shell companies held by overseas individuals.

PARTICULAR MODES OF ABUSE

Shell companies may be employed in a web of legal entities that also involve nominees and intermediaries to obscure involvement, control and beneficial ownership of criminals. Professional service providers who set up the company may act as nominee in an agent role or a third party individual, often with no connection to the criminal activity, may act as a nominee shareholder or agent. Unlike a front company, a shell company is likely to lack a dedicated office, so the registered office may be a “virtual office”, which may be provided professionals involved in formation of the shell company or an individual acting as a nominee. As these individuals are likely to be involved in registering and administrating multiple shell companies, that address is likely to be recycled and will appear in the registered information for a number of companies.

Possible indicators (specific)

- Company is registered with the same office address as a number of other companies
- Address supplied is a "virtual office" or to a residential 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
- 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 'agents' who undertake transactions with the companies register

New Zealand Case Studies

TORMEX LIMITED

The Tormex case which was publically reported overseas and in New Zealand demonstrates the layers of people and entities that may be used in shell company formation. In this case foreign bank accounts in the shell company's name were used to move criminal proceeds under the guise of trade transactions with the shell company.

Tormex Limited was a New Zealand shell company set up by a New Zealand Trust and Company Provider (TCSP), GT Group, based in Vanuatu. Tormex was registered on behalf of an unknown overseas client and nominees were used to hide the identity of the beneficial owners. The address listed on the companies register for Tormex was the same virtual office in Auckland listed for GT Group. The nominee director resided in Seychelles, and the nominee shareholder, Vicam (Auckland) Ltd, was a nominee shareholding company owned by, GT Group. Vicam was itself substantially a shell company and had also been used as the nominee shareholder for hundreds of other shell companies registered by GT Group. For instance, one of the other shell companies Vicam was used to facilitate was SP Trading Limited, which was used to charter an aircraft that was intercepted in December 2009 attempting to smuggle arms from North Korea.

The actual business of Tormex was not apparent and was not indicated by the company name. Unusual names that do not indicate the activity of the company is a common indicator of shell companies used to facilitate criminal activity.

The Organized Crime and Corruption Reporting Project,[7] a network of East European journalists, reported that, once Tormex was registered on the New Zealand companies register, a power of attorney document was used to transfer the directorship to a Russian national. A bank account was then opened at the Baltic International Bank in Latvia. Journalist enquiries with the man revealed he was unaware of either Tormex or its bank account. His identity had been used without his knowledge as he had sold his passport details.

An ex-officer of the Russian tax police told journalists "There are hundreds of law-firms in Moscow, which specialise in setting up ready-made shell companies for their clients, who want to remain in the shadows. Usually law firms use poor people, who sell them passport details. The sum for one passport may vary from US$100 to US$300,"

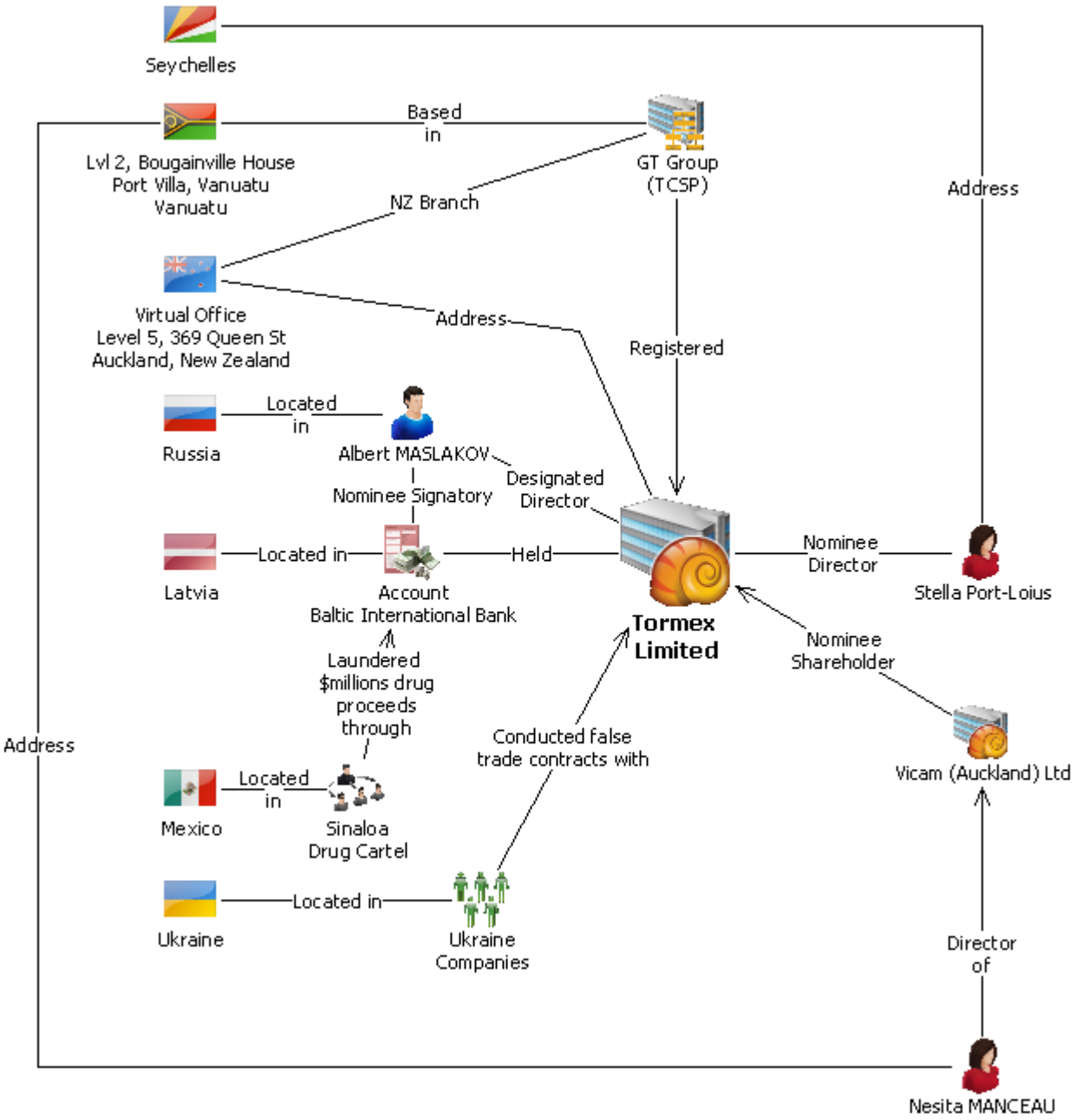
When the journalists examined bank statements for the Latvian account held by Tormex obtained by lawyers in a Moldova court case they discovered that during 2007 and 2008 US$680 million was transacted through the account. Analysis indicated the transactions were money laundering transactions carried out under the guise of trading contracts between Tormex Limited and several companies. Trade transactions were conducted with several Ukrainian companies including a state owned weapons trader. The contracts were then cancelled after the funds had been transferred and refunds were made to different third party offshore companies. The OCCRP journalists report that using transactions related to cancelled trade orders with legitimate companies is a common money laundering method amongst Russian organised crime.

Transactions were also made with three other New Zealand shell companies, Keronol Limited, Melide Limited and Dorio Limited, which had also been registered by GT Group using the same nominee director, nominee shareholder and virtual office address as Tormex.

The UK's Guardian newspaper reported that Tormex Limited, Keronol Limited, Melide Limited and Dorio Limited had been involved in laundering US$40 million for the Sinaloa Drug Cartel based in Mexico.[8] Part of the money laundering process involved the New Zealand shell companies transferring funds to an account held at Wachovia Bank in London linked to the Sinaloa Cartel.

[7] Organised Crime and Corruption Reporting Project (OCCRP) http://www.reportingproject.net/proxy/en/the-phantom-accounts

[8] www.guardian.co.uk/world/2011/apr/03/us-bank-mexico-drug-gangs?INTCMP=SRCH)



Possible indicators:

- Use of nominated shareholders and directors
- Use of virtual offices
- Unclear whether the company is actually operating and providing goods or services
- Large number of international transactions transiting through the account
- Same person and/or address used in registration of multiple companies
- Companies with unusually complex or unexplained ownership structures
- Unclear who the natural person with ultimate beneficial ownership is
- Company based in, or director/shareholder based in, jurisdiction associated with shell companies.

OPERATION MAJOR

Transnational drug dealing

Operation Major involved Asian organised crime using New Zealand registered companies to act as a cover for the facilitation of drug smuggling into New Zealand. Multiple companies and bank accounts were established for the sole purpose of being able to import legitimate goods which concealed illicit drugs within them (crystal methamphetamine and precursor chemicals). The companies purported to be in the business of international trading and supply of materials relating to polymer technologies. In May 2006, a New Zealand Customs drug seizure found 95kg of crystal methamphetamine concealed in the bottom of 95 paint tins. A few days later a second drug seizure found 150kg of pseudo ephedrine tablets in amongst a shipment of bags of block plaster. Both drug seizures had a combined potential

total street value of NZ$135 million. This was the largest and most significant illicit synthetic drug seizure in New Zealand's history. The shell companies involved were registered by accountants and the individuals involved in the drug importations.

OPERATION STARLIFTER

Transnational Tax Evasion

This operation involved an investigation into New Zealand registered shell companies that were being utilised to legitimise false expenses for companies in Australia, in order to reduce their income tax. The fraud involved an accountant based in Vanuatu who registered shell companies in countries including New Zealand, United Kingdom, Ireland, USA and Vanuatu. The accountant used the certificates of incorporation of these shell companies to set up 150 foreign currency accounts in New Zealand. Over a period of 10 years the accounts were used to evade an estimated $100 million of tax by Australian citizens. Approximately $30 million dollars was seized by NZP in bank accounts held for the shell companies.

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 that 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 the risk of exploitation of other corporate forms, particularly limited partnerships.
- **NOMINEES, TRUSTS, FAMILY MEMBERS OR THIRD PARTIES** — utilising other people to carry out transactions in order to conceal the true identity of persons controlling proceeds of crime.
- **TRADE-BASED MONEY LAUNDERING —** manipulating invoices, often in connection with international trade, by overstating the value of a shipment providing criminal entities with a paper justification to either launder proceeds of crime and/or send funds overseas to finance terrorism.
- **CANCEL CREDITS OR OVERPAYMENTS —** laundering proceeds of crime by overpaying, then requesting refund cheques for the balance.
- **ELECTRONIC TRANSFERS —** transferring proceeds of crime from one bank account to another via financial institutions.
- **CO-MINGLING —** combining proceeds of crime with legitimate business takings.
- **GATEKEEPERS/PROFESSIONAL SERVICES —** utilising "professionals" to establish seemingly legitimate business activities, for example, lawyers, accountants, brokers, company formation agents.
- **CASH DEPOSITS —** placement of cash into the financial system.
- **SMURFING —** utilising third parties or groups of people to carry out structuring.
- **CREDIT CARDS, CHEQUES, PROMISSORY NOTES —** instruments used to access funds held in a financial institution, often in another jurisdiction.
- **CASH COURIERS —** concealing the movement of currency from one jurisdiction to another using people, luggage, mail or any other mode of shipment, without declaration.
- **STRUCTURING —** separating large transactions into small transactions to avoid scrutiny and detection from financial institutions.
- **ABUSE OF NON-PROFIT ORGANISATIONS —** raising funds to finance terrorism using non-profit organisations (charities) to conceal the source and nature of funds, as well as to facilitate distribution.
- **INVESTMENT IN CAPITAL MARKETS —** laundering proceeds of crime by using any market in which securities are traded, for example, the stock and bond markets, as well as futures trading and currency speculation.
- **OTHER PAYMENT TECHNOLOGIES —** utilising emerging or new payment technologies to facilitate money laundering and/or terrorist financing.

- **UNDERGROUND BANKING/ALTERNATIVE REMITTANCE SERVICES** — transferring proceeds of crime from one person to another via informal banking mechanisms.
- **TRUSTED INSIDERS/CORRUPTION —** collusion, coercion or bribery of financial institution staff by customers, particularly high-profile individuals, for instance, government officials, business executives, celebrities or individuals known or suspected of being involved in serious crime.
- **CASH EXCHANGES —** exchanging low denomination notes for high (also known as refining) as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.
- **CURRENCY CONVERSION —** converting one currency into another as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.

Annex 2

Financial Intelligence Unit

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

Annex 3

Typology indicators

GENERAL INDICATORS

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

- Transactions involving locations with poor AML/CFT regimes or high exposure to corruption
- Significant and/or frequent transactions in contrast to known or expected business activity
- Significant and/or frequent transactions in contrast to known employment status
- Ambiguous or inconsistent explanations as to the source and/or purpose of funds
- Where relevant, money presented in unusual condition, for example, damp, odorous or coated with substance
- Where relevant, nervous or uncooperative behaviour exhibited by employees and/or customers

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

- Purchase/sale of real estate above/below market value irrespective of economic disadvantage

- Cash purchases of valuable assets with cash and/or cash deposits for valuable assets
- Low value property purchased with improvements paid for in cash before reselling
- Rapid repayment of loans/mortgages with cash or funds from an unlikely source

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

Possible indicators (specific)

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

Additional Indicators:

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers involving accounts located in high-risk countries or known tax havens
- Transfers to offshore jurisdictions with no business rationale
- Multiple transfers sent to same person overseas by different people
- Departure from New Zealand shortly after transferring funds

- Transfers of funds between various accounts that show no economic sense (i.e. multiple transfers incurring bank fees where one single transfer would have been sufficient)

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

CASH DEPOSITS — placement of cash into the financial system.

Possible indicators (specific)

- Large cash deposits followed immediately by withdrawals or electronic transfers

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

- Known or suspected criminal entities establishing trust or bank accounts under charity names
- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers involving accounts located in high-risk countries or known tax havens

- Transfers to numerous offshore jurisdictions with no business rationale
- Entities that use third parties to distribute funds or have weak financial governance mechanisms

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

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