Financial Intelligence Unit
New Zealand Police

Quarterly Typology Report
Second Quarter (Q2)
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).

FIU TRAINING

FIU training for reporting entities continued throughout the second quarter and will resume in February 2014. The FIU has already seen benefits from the training as the quality of STR reporting has improved leading to fewer rejected STRs and higher quality information received. The FIU has also gained valuable insight into reporting entitys' business practices and established new points of contract helping to further enhance relationships.

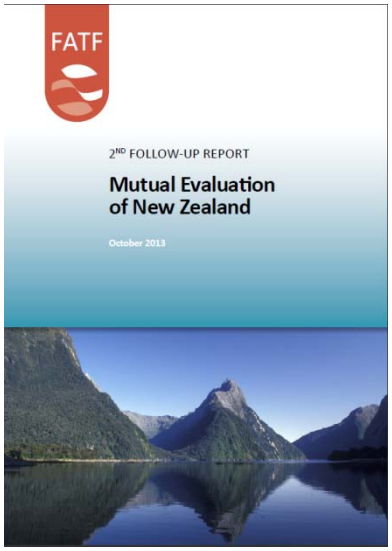
COMPANIES BILL

The Companies and Limited Partnerships Amendment Bill was reported back to the House of Representatives by the Commerce Select Committee in December 2013 and is scheduled for its second reading in July 2014. The Bill includes provisions to make it more difficult for money launderers to exploit New Zealand companies by requiring New Zealand companies to have a director resident in New Zealand or an enforcement country. More information can be found on the Parliament website: http://www.parliament.nz/en-nz/pb/legislation/bills/00DBHOH_BILL11152_1/companies-and-limited-partnerships-amendment-bill

NEW ZEALAND REMOVAL FROM FATF FOLLOW-UP REPORTING

In October, New Zealand was successful in its application to be removed from the FATF regular follow up report process. At its plenary meeting in Paris the FATF recognised the significant progress New Zealand has made since the 2009 mutual evaluation noting work on:

- Strengthening the AML/CFT legislative framework with the adoption of new preventive AML/CFT Legislation – the AML/CFT Act, 2009 - which came into full force and effect on 30 June 2013.
- Issuing a set of implementing preventive AML/CFT measures, a National Risk Assessment and comprehensive guidance material to assist reporting entities with the implementation of the Act.
- Introducing several changes to its supervisory framework, including establishing three statutory supervisors for reporting entities subject to the Act: The Reserve Bank of New Zealand; the Financial Markets Authority; and the Department of Internal Affairs.
- Strengthening its registration and licensing regime for financial service providers and the insurance sector.
- Introducing a new cross-border cash reporting regime.



The updated FATF assessment can be found here: http://www.fatf-gafi.org/countries/n-r/newzealand/documents/fur-new-zealand-2013.html

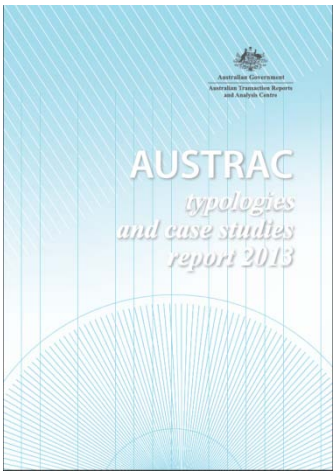
FATF Identifies Jurisdictions with Strategic AML/CFT Deficiencies[2]

The Financial Action Task Force (FATF) released a public statement (October 2012) listing high-risk and non-cooperative jurisdictions. In particular, the 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.

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

AUSTRAC TYPOLOGY REPORT

The Australian FIU, AUSTRAC, released its 2013 Typologies Report in December. This year's report contains 23 case studies involving abuse of account and deposit taking services, gambling and remittance along with description of trade-based money laundering, laundering using gold bullion, and laundering by politically exposed persons. The full report can be found at http://www.austrac.gov.au/typologies.html.



Asset Recovery Units

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

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

The application of joined-up, all-of-government approaches to criminal investigations, supported by civil recovery of the proceeds of crime, are becoming increasingly successful in New Zealand. The funds realised from the sale of forfeited assets are being used to target the drug trade and to help those affected by it get treatment. The first group of initiatives to be funded by the proceeds of crime were announced in the Department of the Prime Minister and Cabinet's *Methamphetamine Indicators and Progress Report*[3] in October 2013. They include enhanced front-line screening capabilities for Customs, support for people accepted into alcohol and drug treatment programmes, training for drug search dogs to locate cash, and programmes to reduce the impact of 'huffing' volatile substances.

Since the CPRA came into effect the ARUs have investigated assets worth an estimated $316 million.

At the end of December 2013:

- Forfeiture Orders for assets worth an estimated $35.6 were in place (see key terms below).
- Restraining Orders were in place over assets worth an estimated $148.6 million pending further investigation and court action (see key terms below).

NEW ZEALAND: ARU CONTRIBUTION TO OPERATION GHOST

The ARUs have been heavily involved in Operation Ghost, which terminated in December 2013 (see the news section below for more details). When the operation was terminated 132 assets worth an estimated $14 million were restrained pending further enquiries and Court action. These assets included cars, cash and bank accounts, jewellery, designer handbags, and collections of fine wine. Financial investigation by the ARUs are ongoing.

NEW ZEALAND: ASSETS FORFEIT FROM WAIHI METHAMPHETAMINE COOK

In February 2013 Scott Filer was sentenced to 17 years imprisonment for manufacturing methamphetamine in the Coromandel region[4]. Filer was convicted after manufacturing around 4kg of methamphetamine with a street value of $3-4 million. The investigation uncovered links to organised crime groups in Auckland but also to Asian based specialists who provided the precursors. In November 2013 a Profit Forfeiture Order was made for the sum of $1.6 million (see key terms). Assets including two residential properties, three cars, two cash/bank accounts, and one Kolbeco digger were forfeit to cover Filer's obligations.

INTERNATIONAL: TAX EVASION AND IMMIGRATION OFFENCES TARGETED IN UK

In September 2013, Kwai Fun Li, a Chinese restaurant owner from Glasgow in Scotland was ordered to surrender £722,000 (NZ$1.4 million) in cash and assets after the Courts found she had benefited from tax evasion and the employment of illegal immigrants[5]. The operation was led by Home Office Criminal and Financial Investigation officers and the Serious Organised Crime Agency, and, in the first instance, resulted in a fine of just £6,000 (NZ$12,000). Ten years ago this would have been the final result. The wide ranging powers now afforded under UK asset recovery regimes, however, mean that "such cases of 'criminal lifestyle' offending no longer conclude at conviction"[6], and prosecutors were able to pursue Li's assets to prevent her benefiting from her criminal activities.

INTERNATIONAL: US TOMATO KING'S ASSETS RESTRAINED IN AUSTRALIA

In November 2013 almost AUD$50 million (NZ$53 million) in tainted cash was restrained from the Californian tomato king, Scott Sayler. Sayler, who was jailed in the US for racketeering and price-fixing, was exposed by a joint FBI and IRS operation that found evidence of bribery, price manipulation, and the falsification of food quality tests that allowed mouldy tomatoes to be processed into a variety of pre-packaged foods. The Australian Federal Police (AFP) used evidence from this investigation to demonstrate to the Victorian Supreme Court that funds held by the liquidators and

[3] http://www.dpmc.govt.nz/sites/all/files/publications/indicators_and_progress_report_october_2013.pdf
[4] http://www.stuff.co.nz/waikato-times/news/6377873/P-dealer-gets-17-years-jail
[5] http://news.stv.tv/scotland/240652-kwai-fun-li-ordererd-to-pay-720000-for-employing-illegal-immigrants/
[6] http://news.stv.tv/scotland/240652-kwai-fun-li-ordererd-to-pay-720000-for-employing-illegal-immigrants/

receivers of Sayler's collapsed business interests in Australia were the proceeds of racketeering offences. This is the largest case mounted under the commonwealth's 10-year-old proceeds of crime legislation and relies on a provision that allows the pursuit of funds in Australia that are suspected of being the proceeds of crimes committed overseas.

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.

Money Laundering through use of third party intermediaries

Using third party intermediaries to conduct money transactions is a very common technique in money laundering. Use of intermediaries can be effective at all stages of money laundering in obscuring the origin of proceeds of crime and the involvement of, or beneficial ownership by, criminals. AML activity has increased the incentives for using intermediaries while advances in technology have increased the opportunity for money launderers to use more complex arrangements using various intermediaries. There are broadly two types of intermediaries discussed here – those who conduct non-specialised services such as funds transfer on behalf of others and those who offer specialised services to conduct services on behalf of others, such as offering a professional service or access to a particular financial vehicle.

Use of third party intermediaries may be as simple as handing cash or transferring funds to a third party and instructing them to make a transaction on the criminal's behalf. These simple uses of intermediaries may involve knowing cooperation by a family member or a junior member of a crime syndicate or involve an unwitting 'mule' as is often facilitated through internet based recruitment scams. In these simpler activities, intermediaries may be used to make transactions such as making cash deposits (e.g. 'smurfing'), to remit cash overseas, to purchase assets or to hold assets in the intermediary's name on behalf of criminals.

Intermediaries may also lend special expertise to more complex laundering schemes. This may occur where a professional facilitator acts as an intermediary to lend an air of legitimacy to the transaction and/or to obscure criminals' involvement or the origin of funds used to conduct a transaction. For example making structured cash deposits to a lawyer's client account to then fund an asset purchase. Again, involvement as an intermediary may be unwitting or complicit.

Intermediaries can also be used to gain access to specialised products or financial services which may be needed for laundering or other criminal transactions. For example professionals may act as intermediaries, or set up trusts or legal persons to act as intermediaries, to move money to offshore accounts. Repeated use of such intermediaries can create a seemingly impenetrable web of transactions designed to frustrate efforts to trace the criminal origin of funds.

Launderers may also use intermediaries as nominees to be director or shareholders of shell companies used as fronts for laundering. In these cases, the nominee may be in a different country to the launderers and have little real connection to the criminals who they are acting for.

Assets, such as vehicles or real estate may also be purchased in third partys' names to integrate proceeds of crime. In these instances there is a high incentive to use family members or other close associates as intermediaries so that the criminals may enjoy the fruits of their offending and to ensure that their assets are legally held by someone they can trust.

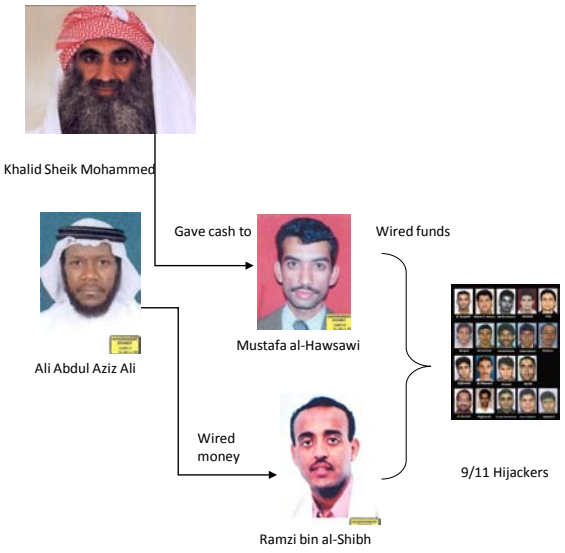
Although it may not be possible to spot use of intermediaries in all instances, there are often some red-flags that may indicate that intermediaries are being used to obscure criminal activity, for example:

- unexplained activity that does not fit the profile of the customer;
- customers who do not know the origin of funds;
- customers who do not know the receiver of funds (for example in cases where money is being remitted overseas);
- another individual accompanying the person making the transaction and instructing them;
- purchases of valuable assets made in third a third party's name;
- unusual transactions involving a professional or company account (for example multiple large cash deposits to a client account);
- involvement of a company with offshore directors; or
- unusually complex transaction arrangements involving multiple countries and/or jurisdictions.

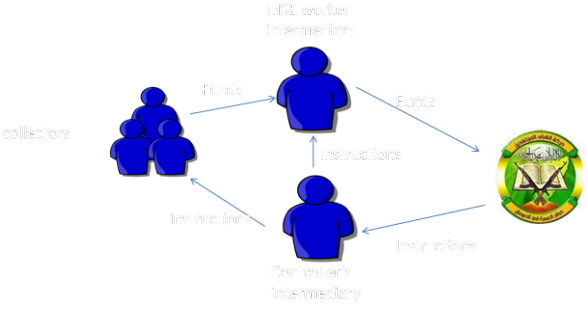
Terrorism Financing through use of intermediaries

Terrorist financing may use many of the same intermediaries as money laundering. Using intermediaries reduces the risk of discovery for terrorist finances by making it harder for authorities to link payments to terrorist organisations and for financial institutions to conduct effective KYC. This is especially relevant where an individual or organisation is a subject of a watch list as using intermediaries is an obvious and effective means of defeating these restrictions. However, using intermediaries is also not without its risks, requiring either an expanded circle of trust or deception of additional individuals/institutions increasing opportunity for detection.

The hierarchical/semi-hierarchical and/or networked structure of terrorist groups makes use of intermediaries a logical means of moving funds either from the origin of fund raising or from organisers to operational terrorist cells. In addition to directly providing cash to the 9/11 hijackers, the organisers of the Khalid Sheik Mohammed used a simple arrangement of trusted intermediaries within the terrorist organisation to wire funds to the hijackers as shown in the diagram below.



Intermediaries may also be used in fundraising activity. In the example of US residents providing funding to al Shabaab reported in previous QTRs, one of the individuals collecting funds who worked at a registered MSB acted as an intermediary for the other collectors to move their funds to Somalia. This arrangement allowed all members of the network to gain access to specialist services which the MSB provided. Meanwhile, a separate individual acted as the intermediary for the al Shabaab controllers in Somalia.



Red flags are largely the same as money laundering by intermediaries, in particular:

- unable to trace origin of funds
- transactions do not fit expected financial profile of customer – for example unexplained remittance to/from high risk jurisdiction

New Zealand Case Studies

Operation Keyboard

Police conducted a financial investigation into a large drug importation and supply ring centred in Lithuania and New Zealand that culminated in multiple convictions for money laundering and drug offences along with restraint of almost three million dollars worth of property, vehicles, cash and other assets.

Concurrent with its drug offending, including multiple importations of ecstasy and LSD, the syndicate involved in the case laundered millions of dollars using intermediaries. The use of intermediaries allowed the central New Zealand-based figure of the drug supply ring, Ronald Brown, to maintain a front of being an unemployment and later sickness beneficiary. The vast majority of transactions identified during the financial investigation involved intermediaries for Brown rather than Brown himself to deflect any possible scrutiny of Brown's finances.

However, even excluding money laundering transactions, Brown's life-style would have appeared suspicious given his declared source of income as being a long term benefit. While on the unemployment benefit, Brown owned several high value vehicles, acquired a bar and later established a company with no identifiable business purpose. Brown's business practices were also unusual, for example business expenses for the bar were paid in cash. Brown was able to use intermediaries in interactions with the financial institutions and dealers which may have otherwise aroused suspicions about his unusual financial profile.

Brown used intermediaries to conduct transactions to place the cash proceeds of his drug supply so as to integrate the funds in the form of high value asset. Brown would give cash to one or more intermediaries who would purchase the vehicle from a dealer either using Brown's cash or banking that cash and using a bank cheque. In some instances Brown's company was used as a front by the intermediary. When the vehicle was purchased, it was registered either in a Brown family member's name or in Brown's company's name.

Brown also used intermediaries to send proceeds to multiple countries overseas. This was accomplished by intermediaries banking cash and wiring funds or by cash deposits to remitters. In one instance this involved the same individual remitting hundreds of thousands of dollars in multiple transactions over a few months with little explanation. Cash was also carried internationally by Lithuanian cash couriers using false passports.

In February 2011, Brown was sentenced to 11-1/2 years' imprisonment after admitting importing ecstasy, LSD and methamphetamine, and using a passport in a false name. A number of other individuals involved have also been convicted of drugs and money laundering offences while others are still before the court. The Lithuania based 'mastermind' of the syndicate, Rokas Karpavicius, was also recently convicted and sentenced to six years and three months imprisonment.

Typologies: use of third party intermediaries, use of front companies; wire transfers; cash deposits; purchase of assets (vehicles)

Money Laundering Indicators:

- unexplained activity that does not fit the profile of the customer;
- customers who do not know the origin of funds;
- customers who do not know the receiver of funds (for example in cases where money is being remitted overseas);
- another individual accompanying the person making the transaction and instructing them;
- purchases of valuable assets made in third a third party's name;
- large cash transactions to purchase assets (vehicles)

Operation Ark

Christopher Chase and Lee Vincent, a New Zealand citizen resident in Thailand, jointly owned a New Zealand 'legal high' business. In addition to selling unrestricted party drugs, the business was used as a front for distribution of illicit drugs. Money generated by both the licit and illicit activity was mingled and the cash generated by these businesses was taken on a regular basis to Vincent's mother's home for temporary storage. The cash was packed into boxes, generally in the form of bundles of $20 and $50 notes. The boxes were then picked up by couriers, who transported the cash to Hong Kong where it was deposited in the bank accounts of three companies beneficially owned by Vincent. Bank statements

cash seized as part of Operation Ark

for these Hong Kong accounts were sent to Vincent's mother's address in New Zealand. The money laundering process was completed by loans made by one of the Hong Kong companies to another New Zealand company. Chase controlled a trust that was a 50 per cent shareholder in the New Zealand company. A small portion of the cash, around $184,000, was retained by Vincent's mother for her own purposes.

Court proceedings are ongoing and to date around NZD23 million has been restrained.

Typologies: comingling; denomination conversion; cash couriering; shell companies, use of loans.

AUSTRAC Typologies[7]

The following case study has been taken from the 2013 AUSTRAC Typologies Report.

AUSTRAC information initiated a multi-agency investigation into a syndicate responsible for importing more than AUD1.5 million of ecstasy concealed in children's toys.

AUSTRAC referred multiple suspect transaction reports (SUSTRs) to law enforcement, detailing apparent structuring of cash deposits by syndicate members into their bank accounts. Bank staff observed the members of the syndicate undertaking a number of suspicious activities.

The suspects:

- arrived at bank branches together
- went to separate bank tellers to conduct structured deposits
- left the bank branches together
- then entered another bank nearby, indicating that the suspects were undertaking structuring activities at multiple banks.

In just four months these accounts received 113 deposits of AUD9,000 each, totaling more than AUD1 million. Two syndicate members travelled to the United Kingdom to organise the purchase of more than 25 kilograms of ecstasy. In the five months leading up to the importation, the syndicate used multiple banks to send 19 international funds transfer instructions (IFTIs), worth more than AUD250,000, to multiple beneficiaries in the United Kingdom. The syndicate also conducted one funds transfer to Germany worth AUD290,000. Authorities suspected these funds were used to purchase the drugs from overseas suppliers.

Once the drugs were purchased overseas, the syndicate concealed them in children's toys and mailed them to the home address of a syndicate member in Australia. When the shipment of drugs arrived in Australia, authorities replaced the drugs and allowed the packages to be delivered as arranged as part of a controlled delivery. When the shipment was delivered, law enforcement arrested and charged the suspects with importing a commercial quantity of border-controlled drugs, dealing with proceeds of crime and structuring transactions to avoid reporting requirements. Law enforcement restrained AUD750,000 held in bank accounts operated by the syndicate and AUD100,000 cash found in a safety deposit box.

The syndicate members were sentenced to periods of imprisonment ranging from nine to 14 years.

- High-value international funds transfers from Australia with no apparent logical reason
- Multiple customers attend the same bank branch as a group and conducting simultaneous
- structured cash deposits
- Multiple high-value international funds transfers within a short time frame
- Structuring cash deposits to avoid threshold reporting requirements
- Sudden increase in transactional activity inconsistent with customer's established profile and/or transaction history

[7] **AUSTRAC Yearly Typology report 2013 http://www.austrac.gov.au/files/typ13_full.pdf**

Domestic and International AML/CFT News

NEW ZEALAND:

Keyboard conviction

Lithuanian national Rokas Karpavicius found guilty in October of three counts of money laundering and of importing a Class A controlled drug relating to Operation Keyboard discussed in the case studies section above. Karpavicius, who played the controlling role in the transnational drug supply and money laundering operation, was arrested in Latvia in late 2012 following the triggering of an Interpol "red notice" as he travelled to Turkey and extradited to New Zealand to face charges.

Multi-Agency Approach Dismantles major drug importation gang

Pseudoephedrine seized as part of operation Ghost

December 2013 saw the termination of Operation Ghost[8], an eighteen month long operation that targeted an organised criminal group importing pseudoephedrine, a precursor for the manufacture of methamphetamine, into New Zealand. The Organised and Financial Crime Agency of New Zealand (OFCANZ) lead operation involved OFCANZ, Police, and Customs, with assistance from the Ministry of Primary Industries, Inland Revenue, the Ministry of Business, Innovation, and Employment, and the Department of Internal Affairs. Aid was also provided by the National Narcotics Control Commission from the People's Republic of China and the Hong Kong Narcotics Bureau. The termination of the Operation involved 250 officers from Police, OFCANZ and Customs executed 40 search warrants, at residential and business premises across Auckland and Waikato, at the conclusion of an 18 month investigation. Pseudoephedrine seized during the Operation is estimated to be enough to produce up to 100 kilograms of methamphetamine which has a corresponding street value of $100 million. The termination led to restraint of an estimated $14 million worth of assets and criminal charges against a number of individuals. Enquiries and Court action are ongoing.

AUSTRALIA

In January, Australian authorities announced that a national taskforce, Eligo, made up of the Australian Crime Commission, the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Australian Federal Police in partnership with the Australian Customs and Border Protection Service and State and Territory police, has been operating for a year to target criminal abuse of alternative remittance and informal value transfer systems.

Cash seized as part of taskforce Eligo

The taskforce has reportedly seized more than $580 million worth of drugs and assets, including $26 million in cash. The task force has also disrupted 18 serious and organised crime groups and identified 128 criminal targets previously unknown to law enforcement. By following the financial trail of the organised crime groups, authorities detected and closed down three commercial amphetamine laboratories, including one of the largest and most sophisticated clandestine laboratory ever discovered by Victoria Police. The complex criminal networks uncovered operated across the country and were linked to more than 20 countries. It has also been reported that one of the overseas exchange houses used by the network had been diverted some of the money to financing of Hezbollah.

[8] http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11173240
http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11166891

UNITED STATES

JPMorgan Chase has agreed to pay more than US$2 billion (NZ$2.4b) of penalties, the largest forfeiture a bank has ever had to pay to resolve anti-money laundering violations. JPMorgan is admitting to a list of failures to explore red flags it found which should have led it to report suspicious activity involving Bernard Madoff's Ponzi scheme.

SPAIN

The Spanish king's youngest daughter has been summoned by a Spanish court in relation to tax and money-laundering charges linked to the business affairs of her husband who is under investigation for alleged embezzlement of public funds.

VATICAN/ITALY

A former Vatican prelate, Monsignor Nunzio Scarano, who is already standing trial for smuggling cash from Switzerland was charged with new money laundering charges by Italian police. Italian Police also announced that they seized €6.5 million in real estate and bank accounts related to the case.

The new charges relate to a laundering scheme where Scarano allegedly withdrew over €500,000 in cash from his Vatican account and brought it to Italy. Scarano then gave 50 intermediaries €10,000 each and had them transfer funds to his Italian account. The money was then used to pay the mortgage on a property. Police said the money involved in both cases originated from an important Italian shipping family.

UNITED STATES

Two prominent Bitcoin traders were arrested in the United States in January on charges relating to selling Bitcoins to users of the online drugs marketplace The Silk Road. The traders are being charged with conspiracy to commit money laundering and operating an unlicensed money transmitting business. One of the traders also faces charges of willful failure to file a suspicious activity report.

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