Financial Intelligence Unit
New Zealand Police

Quarterly Typology Report
Fourth Quarter (Q4)
2013/2014

(Issued July 2014)

INTRODUCTION

This report is the fourth Quarterly Typology Report for 2013/2014 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.

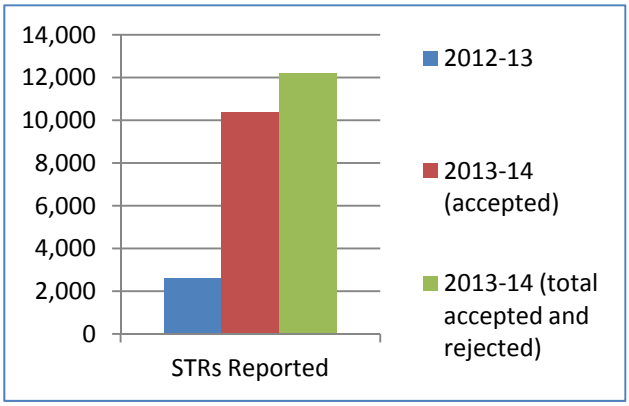
Financial Intelligence Unit and partner agencies - Updates

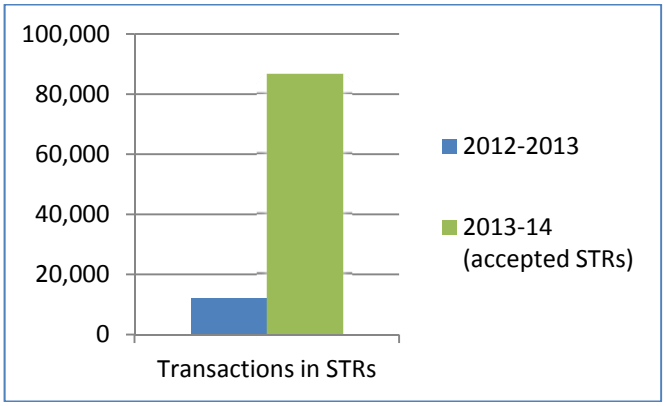
NOTE: Information on the Financial Intelligence Unit is provided as a permanent annex (refer Annex 2).

FIU STATISTICS

STR reporting has increased significantly since the commencement of the AML/CFT Act reporting regime on 30 June 2013. The number of STR has increased from around 2,600 in 2012-13 (down from around 4600 in 2009-10) to 10,353 STRs accepted in 2013-14 (during 2013 1846 STRs were also rejected by the FIU).

The number of transactions in STRs has also increased indicating the higher quality of STRs since the commencement of the new reporting regime. In 2012-13 10,448 transactions worth NZD 516 million (about 4 transactions per STR) were reported to the FIU compared to 2013-14 when 86,937 transactions worth (over 8 transactions per STR) NZD 3.5 billion were reported in accepted STRs.





FINANCIAL INTELLIGENCE RESULTS – 2013-14

The FIU responded to over 770 requests for information in the year ending 30 June 2014 included 67 requests from overseas partners. The majority of domestic requests were from within Police, and requests were also received from OFCANZ and other government law enforcement agencies. The information disseminated from STRs has supported many domestic and transnational investigations involving the distribution of illicit drugs; large scale fraud and embezzlement and tax evasion.

In addition to large scale offending, reports of small transactions have assisted the FIU to produce intelligence which has helped Police to detect victims of email scams and offenders involved in online purchase of child exploitation material. This has assisted with Police's prevention first programme by identifying victims that the Police can help avoid revictimisation and identifying potential offenders that otherwise may have continue offending unnoticed.

goAML UPGRADE

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

FIU-ACAMS SEMINAR

The FIU-ACAMS Seminar was held on 10-11 July at Te Papa in Wellington. A total of 265 participants from the financial sector, government and law enforcement took part. This year's seminar focused on the first year of the new AML/CFT regime. Useful information was shared regarding how to comply sufficiently with the AML/CFT legislation and law enforcement were able to share success stories regarding the sharing of financial intelligence sourced from reporting entities.

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 JUNE 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 now being used to target the drug trade and to help those affected by it get treatment. The second 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[2] [i]n April 2013. Nine initiatives were allocated funding to the total value of $6.4 million. These included a programme to improve outcomes for pregnant women with substance abuse disorders, assistance for whānau interventions for alcohol and other drug clients in communities, funds to update the NZ Drug Harm Index, and expansion of the National Crime and Cannabis Operation and of the Asset Recovery Units in order to tackle organised crime and drug offending and further reduce the financial base of offending.

Since the CPRA came into effect the ARUs have investigated assets worth an estimated $361 million.

At the end of May 2014:

- Forfeiture Orders for assets worth an estimated $45.9 were in place (see key terms below).
- Restraining Orders were in place over assets worth an estimated $160 million pending further investigation and court action (see key terms below).

NEW ZEALAND: OPERATION GRANITE

In June 2014, assets valued at an estimated $126,000 were forfeited from an organised crime syndicate headed by Matthew Newton[3]. Operation GRANITE, a joint Police and Customs operation[4], analysed 20,000 phone calls and text messages[5] as part of the investigation into a group who were using properties across the Christchurch area to commercially manufacture, distribute, and sell methamphetamine[6]. 15 search warrants were executed, with the assistance of the Armed Offenders Squad. These raids located 3 methamphetamine laboratories containing pseudoephedrine tablets capable of manufacturing $300,000 worth of drugs. The offenders received a range of sentences, from home detention to more than five years imprisonment. 6 sums of cash/bank accounts, 3 cars, and 1 motorcycle were forfeited from those involved.

NEW ZEALAND: OPERATION GHOST

May 2014 saw the forfeiture of $575,000 of assets associated with Operation GHOST. Operation GHOST was a joint Police, Customs, and OFCANZ operation that targeted a group of Asian organised crime figures operating in New Zealand[7]. This syndicate used shipping containers to bring enough pseudoephedrine from China to manufacture $100 million of methamphetamine. The 18-month long operation terminated in December 2013 with 250 officers executing 40 search warrants at residential and business addresses across Auckland and Waikato[8]. In addition to the precursor drugs, an estimated $21 million worth of assets were restrained including $1.5 million in cash. 11 cash sums/bank accounts, 1 car, and 1 residential property were forfeit from one of the offenders involved in the importation of 250kg of the pseudoephedrine. This offender left New Zealand on the day of the seizures and is currently believed to be in China. A further 146 assets worth an estimated $20 million remain on restraint pending further investigations.

INTERNATIONAL: INTERNATIONAL CORRUPTION & ASSET FORFEITURE

International asset forfeiture regimes are increasingly being used to target corruption and fraud. The Serious Fraud Office in the UK has restrained almost US$23 million (NZ$26.2 million) worth of assets alleged to be funds laundered

[2] http://www.dpmc.govt.nz/dpmc/publications/methamphetamine
[3] http://www.courtnews.co.nz/story.php?id=4675
[4] http://www.police.govt.nz/news/release/24276
[5] http://www.odt.co.nz/112074/operation-granite-drug-accused-remanded
[6] http://www.stuff.co.nz/the-press/news/7697454/Five-guilty-in-Operation-Granite-trial
[7] http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11173240
[8] http://www.stuff.co.nz/national/crime/9475938/Huge-drug-haul-after-18-month-investigation

from corruption in the Ukraine[9]. The UK action is accompanied by an EU-wide asset freeze against 22 individuals suspected of misappropriating Ukrainian state assets, including the seizure of US$190 million (NZ$217 million) of assets linked to former President Yanukovich by Swiss authorities[10]. It is claimed that US$70 billion (NZ$80 billion) has gone missing from the public balance sheets while Yanukovich's government was in power.

In the US former mayor Ray Nagin has been ordered to pay back US$501,200 (NZ$572,000) connected to illicit gains he made during his tenure as mayor of New Orleans[11]. Nagin was convicted on 20 counts including bribery, money laundering, and tax fraud for accepting cash and gifts in exchange for lucrative city contracts. Nagin is also expected to serve a lengthy prison sentence on top of the asset forfeiture order.

In Tel Aviv former Bank Hapoalim chairman and Israel Salt Industries director Dan Dankner has been made subject to a NIS1 million (NZ$333,000) forfeiture order following his conviction on bribery and money laundering charges in the Holyland real estate trial[12]. Dankner used his position to transfer NIS1.3 million (NZ$433,000) of bribe money to real estate investor Shmuel Duchner, who was alleged to have bribed public officials to advance construction of the Holyland project in Jerusalem. The money given to Duchner was passed on to the former Israel Lands Authority chief Ya'acov Efrati to persuade him to make land rulings favourable to Dankner's interests. Dankner has also been convicted on fraud and breach of trust and harming the proper management of a banking corporation. He will serve three years in prison for his offences and has received a NIS 500,000 (NZ$166,000) fine in addition to the asset forfeiture order.

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.

[9] http://www.ibtimes.co.uk/uk-freezes-23m-ukraine-assets-frozen-money-laundering-investigation-1446487
[10] http://www.thelocal.ch/20140604/swiss-outline-ukrainian-asset-seizures
[11] http://www.nola.com/politics/index.ssf/2014/05/judge_ray_nagin_must_forfeit_5.html
[12] http://www.jpost.com/National-News/Former-Bank-Hapoalim-chairman-to-serve-3-years-in-prison-352127

Co-Mingling with Business Revenue

Businesses, particularly cash businesses, have long been identified as a vulnerability for money laundering. The association of money laundering with businesses, particularly cash businesses is so strong that the term money laundering itself may have been derived from comingling proceeds of mafia related crime with the licit proceeds of US launderettes. Businesses remain an attractive option for money laundering and terrorist financing as illicit transactions though businesses are more likely to appear to be normal licit transactions. In particular, the regularity with which ordinary businesses conduct transactions and transfers similar to launderers, the large number of business and the perception that laundering through businesses is unlikely to be detected make businesses an attractive vehicle for laundering. Businesses offer three principle functions for launderers:

- To act as a front (so that criminal proceeds may be mingled with the legitimate turnover of the company);
- The potential to fund transactions connected to laundering rings; and
- The opportunity to integrate criminal wealth by investing in a legitimate business and generating legitimate earnings.

Similarly, terrorist financiers may be interested in using businesses to:

- Act as a front through which funding may be layered; and
- As a source of funds which may be diverted to terrorism.

Opportunities to launder

Stats New Zealand information shows that approximately half a million businesses exist in New Zealand with NZ$73billion of sales in retail alone during the year to March 2014. This large number of businesses, which may engage in high volume and/or high value transactions, creates opportunities to co-mingle illegal proceeds amongst legitimate business activity.

Businesses are a particularly attractive option for obscuring the money trail at placement and layering phases. The classic technique of mingling cash proceeds with cash takings from a business to place funds in financial institution establishes a legitimate origin for the cash and may be relied on to avoid detection by a financial institution or to defeat law enforcement criminal proceeds investigation.

At the layering stage, moving funds through business accounts may be used to avoid suspicion or to place a layer between the financial institution and the individual involved. Whether or not the transactional business transactions are used, techniques similar to those used in trade-based money laundering may be employed. For example, abuse of a business creates opportunities to create documentation such as records, accounts and invoices which may appear to explain a legitimate source of the proceeds. Use of a business controlled by a third party may also effectively obscure the involvement of beneficial criminal owners in a particular transaction.

In addition to the money laundering opportunities, criminals may be attracted to businesses because the industries provide access to other facilitators of crime. For example, transport, pharmacies, prostitution, bars may all be used to facilitate trafficking and sale of illicit drug.

Ultimately, criminals involved in proceeds generating offending are for the most part motivated by profit. Integrating proceeds into a legitimate business to provide legitimate and potentially lower risk, earnings may be attractive to many criminals. Similarly, terrorist financiers may be attracted to business ventures as a relatively low risk, and unsuspicious means of raising funds that will later be diverted.

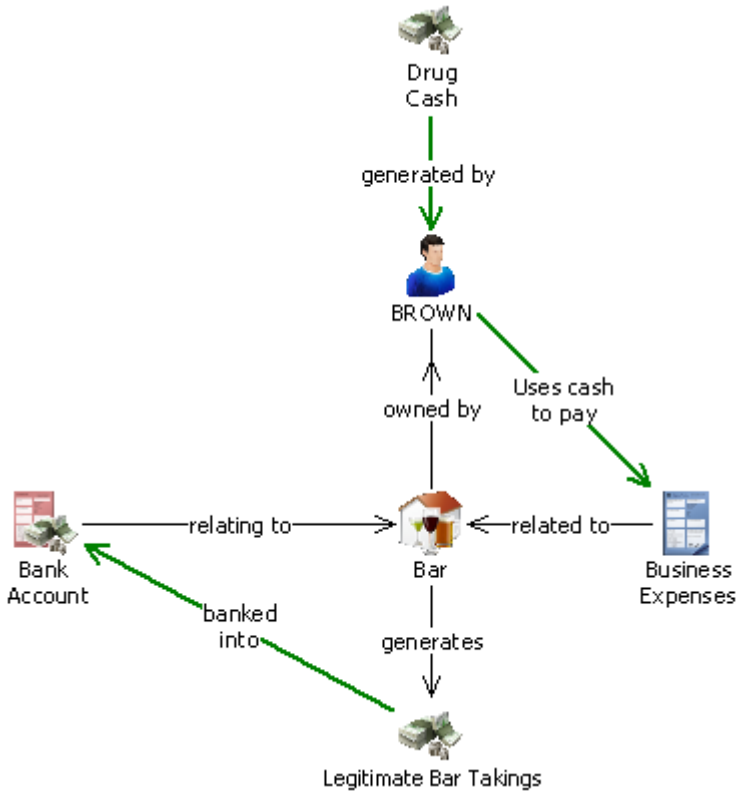
New Zealand Case Studies

OPERATION KEYBOARD

Bars are a classic business to launder cash proceeds through as:

- drinks are often purchased in cash, in multiple small untraceable and easily forged transactions; and
- takings may be variable providing an opportunity to explain unusual cash deposits.

In Operation Keyboard, which was discussed in the Second QTR for 2013/14, a central figure of a drug supply ring used a central Auckland bar to co-mingle the proceeds of drug sales. Ron Brown's declared source of income was an unemployment and later sickness benefit. However, in 2007, Brown was able to purchase the K' Rd Pool Bar & Lounge. While the business was run at a loss, the bar was an effective mechanism for Brown to place the proceeds of his drug offending without having to deposit cash from drug sales at financial institutions. Placement was achieved by paying business expenses with drug cash and banking the bar takings as per a legitimate bar in the business account that Brown maintained beneficial ownership of. This relatively simple mechanism allowed Brown to effectively swap the drug cash for the ostensibly clean bar takings.



Part of the money laundering in Operation Keyboard involved effectively swapping drug money for ostensibly legitimate bar takings.

ABUSE OF ROAD CONTRACTING AND FORESTRY BUSINESSES (CURRENTLY BEFORE COURTS)

In 2013 the High Court restrained around $1.8 million worth of assets related to a drug supply network connected to a roading contractor. Court proceedings are ongoing and no indication of settlement and no resolution date has been set.

The Crown alleges that the principle offender and a number of associates were involved in a national drug supply network that used the roading contractor's roading and forestry businesses to facilitate offending. The businesses provided ideal fronts for drug distribution and/or manufacture, providing the principle offender with a reason for local and domestic travel required for drug related transactions. While Police is aware of extensive movement ostensibly related to these businesses, Police has not been able to substantiate corresponding legitimate business activity.

The offenders also appear to have used these companies to co-mingle the proceeds of the offending. Such businesses provide an opportunity to explain the illicit earnings from drug supply. The principle offender ensured that his businesses maintained good records of apparent earnings by using professional accountants. In addition to facilitation of predicate

offending, the nationally dispersed business interests also would have provided an opportunity to select professional service providers which may have allowed the offenders to select professionals who would be unable to detect illicit activity. These types of arrangements could also allow criminals to seek remote professional services and/or to change professional service providers so as to prevent professionals gaining a full appreciation of any unusual business activity. In this case, maintaining professionally facilitated business records and declaring earnings for tax helped the offenders to maintain an air of legitimacy.

Using such businesses as fronts for criminal activity may also make law enforcement investigation to establish illicit earnings more complex. However, despite the extensive and well documented earnings, corresponding legitimate business has not been established giving a strong indication that the illegitimate earnings from drug supply were co-mingled with whatever legitimate earnings the businesses made.

OPERATION ACACIA

A methamphetamine manufacturer operated a business buying and selling building materials supplied from demolitions. Police financial analysis of the business accounts showed that approximately $150,000 cash had been deposited over a five and a half year period. Over half of the cash deposits were banked in 2008 and 2009; a period where the business declared it was making a loss and where evidence showed the offender was manufacturing methamphetamine. It is therefore likely that some of the cash was the proceeds of drug sales as this level of legitimate deposits would have been sufficient to nullify the loss. In addition, the offender did not declare all the cash deposits as income for tax purposes.

Later, in the civil criminal-proceeds case, the offender argued that the cash deposits were the proceeds of legitimate business sale; however, he could not substantiate this because he did not keep proper business records. The offender's business, therefore, created the ideal opportunity to launder drug proceeds because it was a cash business and he could disguise the drug cash as legitimate income.

Partial payments were made from the business account towards personal bonus bonds, a marina berth and property thus converting the criminal proceeds into assets and completing the money laundering process. Cash withdrawals were also made from the business account, potentially to conduct further illicit transactions without an audit trail.

Outcome:
The offender was sentenced to 17 years prison for the manufacture and supply of methamphetamine. His residential home, rural land, cars, a digger, a marina berth and bank accounts were forfeited to the crown in order to repatriate an estimated $1.6million that he earned from selling methamphetamine.

AUSTRAC Typologies[13]

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

SENIOR PUBLIC SERVANTS STOLE $1.7 MILLION FROM STATE GOVERNMENT

AUSTRAC assisted law enforcement to investigate two senior public servants charged with stealing more than AUD1.7 million cash from a state government department.

The public servants, who were married, generated false invoices through their own private company for work they never carried out. The suspects submitted the false invoices to a government department, which paid the suspects' private company for the non-existent services.

At the direction of her husband, the female suspect used companies she controlled to launder the illicit funds by co-mingling the proceeds of the fraud with legitimate funds generated by the companies. The female suspect dealt with the companies' accountant and gave him the false impression that the illicit funds paid to the companies had been earned through legitimate sources. Income tax was paid on the illicit funds to give the transactions a further appearance of legitimacy.

A suspect transaction report (SUSTR) submitted to AUSTRAC identified that a number of domestic electronic transfers from a third party, an Australia-based company, were paid into the business accounts of companies owned by both suspects. Once the funds were paid into the couple's business accounts they were then transferred into personal accounts held in the suspects' names.

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

AUSTRAC also received three significant cash transaction reports (SCTR) detailing how the suspects withdrew AUD115,000 cash from their personal accounts over a six-week period.

AUSTRAC prepared a financial assessment report which assisted investigating authorities to identify bank accounts linked to the suspects. Of particular interest to authorities were bank accounts held in the names of the suspects' children. AUSTRAC information showed that AUD50,000 had been withdrawn from these accounts; withdrawals that authorities suspected had been undertaken by the suspects.

Suspect A was charged with 17 counts of stealing as a servant and was sentenced to eight years jail. Suspect B was charged with 14 counts of stealing as a servant and was sentenced to four years imprisonment.

Indicators

Account activity inconsistent with customer profile

Cash deposits into business account followed by transfers to personal account

Significant cash withdrawals over a short period of time

Use of children's accounts for transactions

Use of third-party company accounts in an attempt to lend transactions a veneer of legitimacy

Domestic and International AML/CFT News

NEW ZEALAND

Companies and Limited Partnership Bill passes

The Companies and Limited Partnerships Amendment Bill received Royal Assent on 2 July 2014. The Bill creates the Companies Amendment Act 2014 and the Limited Partnerships Amendment Act 2014. This legislation assists with the prevention of misuse of New Zealand companies (shell companies) and Limited Partnerships by overseas criminal organisations.

The amendments will require all New Zealand-registered companies to have a director who is resident in New Zealand (or an enforcement country), and all directors will be required to disclose their date and place of birth to the registrar of companies. If a company has an ultimate holding company it will need to disclose the details of that company. Parallel legislation will place near identical requirements on limited partnership. The legislation amendments will also give new powers to the Registrar of Companies to better investigate companies and limited partnerships.

Introduction of Organised Crime and Anti-corruption Legislation Bill

The Organised Crime and Anti-corruption Legislation Bill was introduced to Parliament on 25 June 2014 and implements a number of new measures to respond to the threat posed by international and domestic organised crime. Key measures in the Bill include:

- requiring financial institutions to report international wire transfers and physical cash over transactions of $10,000 to the FIU;
- amending the money laundering offence to specify that intent to conceal is not required
- introducing new offences to address identity crime, including selling or passing on unlawfully obtained identity information;
- revising the foreign bribery offence, including clarifying the circumstances in which a corporation is liable for foreign bribery; and
- increasing penalties for bribery and corruption in the private sector to bring them into line with public sector bribery offences.

UNITED STATES

BNP Paribas fined

US regulators have imposed a US$8.97billion fine against French bank BNP Paribas for breaking US sanctions against Sudan, Iran and Cuba. The total penalty is by far the most severe ever imposed on a major bank. In addition, the US Federal Reserve says it intends to pursue civil enforcement action against a number of BNP Paribas employees and former employees.

BNP Paribas allegedly used obfuscated method of payment messages to conceal the involvement of sanctioned entities in US dollar transactions processed through BNPP New York and other financial institutions in the United States and removed information which may have identified the involvement of the sanctioned entities. BNP Paribas also allegedly actively colluded with other financial institutions and the sanctioned entities to ensure that sanctioned entities' involvement was hidden by complex structured payments.

QATAR/FRANCE

Report on illegal bettering markets

A study by Paris-Sorbonne University and the International Centre for Sports Security estimated that USD140 billion per annum is laundered through illegal betting. The two year study estimated the overall size of the sports betting market to be USD200 – 500 billion. The study found that of the 8,000-plus operators that offer legal sports betting services around the world, more than 80% are based in lightly-regulated markets creating opportunities for the owners of the companies are able to remain anonymous.

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