Financial Intelligence Unit
New Zealand Police

Quarterly Typology Report
Third Quarter (Q3)
2013/2014

(Issued May 2014)

INTRODUCTION

This report is the third Quarterly Typology Report of 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 TRAINING

FIU continues to provide training to reporting entities on STR reporting to the still-expanding user base. During the third quarter, most training outside of Wellington was conducted through conference calls. The value of this time spent educating new users is seen immediately with a quicker turnaround time in the validating and acceptance of subsequent reports. The feedback received is always very positive and this helps forge good contact points for these businesses.

FIU SEMINAR

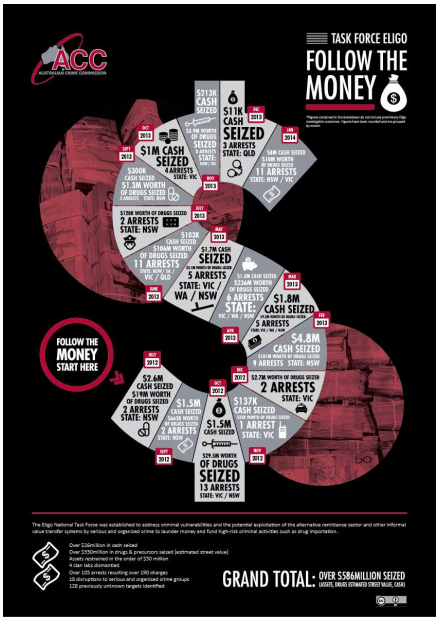
The Annual FIU Seminar will be held at Te Papa 10-11 July 2014 in association with ACAMS. The seminar is attended by about 300 people every year AML risk and compliance professionals from both the private and public sectors. This year's topic will focus on 'The new legislation…one year on'. Presentations will include:

- An update from sector supervisors… one year on
- Managing money laundering risks in today's environment
- Preparing for audits of risk assessment and AML/CFT programmes
- Case studies from the Asset Recovery Unit
- Case study on scams and their victims
- Case study from the Online Child Exploitation across New Zealand Unit

Registration will open soon at www.acams.org.nz

AUSTRALIA TASKFORCE ELIGO

Following announcement that the Australian Crime Commission led Taskforce Eligo has seized over AUD 26 million in cash, AUD 30 million in assets and AUD 530 million worth of drugs, the ACC published infographics on Taskforce Eligo and Money Laundering. The infographics can be found at:
https://www.crimecommission.gov.au/media-centre/release/australian-crime-commission-multimedia/money-laundering-infographics



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 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 $333 million.

At the end of February 2014:

- Forfeiture Orders for assets worth an estimated $37.6 were in place (see key terms below).
- Restraining Orders were in place over assets worth an estimated $154 million pending further investigation and court action (see key terms below).

NEW ZEALAND: FORFEITURE OF DRUG KING-PIN'S FARM (see case study below)

In February 2014, the farm of methamphetamine cook and dealer, Timothy Clifford, was forfeited to the Crown following a long term operation conducted by Police in the Waikato . The forfeiture was part of Operation CAPE, which smashed a $1 million a year methamphetamine manufacturing and dealing ring. This ring also involved Stephen Gray, who was sentenced to 12 years in prison and from whom more than $5 million worth of assets were forfeited in March 2013.
The 2720 acre farm at Waitetuna had been purchased by Timothy Clifford with funds laundered through a firm of accountants. Analysis of Clifford's financial accounts showed that he had received an income of around $4.1 million between June 1999 and May 2003 from drug offending. The farm was used to manufacture methamphetamine and to store the chemical precursors. A large number of firearms were also recovered from the property including two fully automatic assault rifles.

NEW ZEALAND: ASSETS FORFEIT FROM DISHONEST ACCOUNTANT

In March 2014, assets valued at an estimated $1.4 million were forfeited from accountant Gary Soffe, who used funds stolen from the trust accounts of his clients to fund a lavish lifestyle. For years Soffe was considered 'one of the family' but behind their back the Hamilton-based accountant siphoned off funds and used them to build a mansion complete with hydro-slide and to fund purchases such as vehicles, company shares, boats, and a holiday home in Fiji. His actions were concealed by a complex set of entities that were used to hide his fraud, often under the guise of legitimate transactions'. Soffe was caught when Inland Revenue noted discrepancies between his assets and his declared income. He has been sentenced to more than five years imprisonment and his status as a chartered accountant has been suspended by the Institute of Chartered Accountants.

INTERNATIONAL: THE FILIPINO PORK BARREL SCAM

An estimated P30 million (NZ$777,000) in bank accounts and insurance policies has been made subject to Provisional Asset Preservation Orders in the Philippines following reports of the Pork Barrel Scam . The Pork Barrel Scam was identified by the Anti Money Laundering Council in the Philippines when they identified that, despite having little legitimate income, large sums were appearing in the bank accounts and other monetary investments of business woman Janet Lim-Napoles . The scam involved the funding of ghost projects from the Priority Development Assistance Fund (PDAF); a lump sum discretionary fund that is granted to each member of Congress to enable them to allocate it to local development projects . In the scam, projects were run by companies owned by Napoles but no tangible results were produced. Instead, funds were processed through fake foundations and non-government organisations established under the JLN Group of Companies, which saw Napoles' employees including a nanny named as directors. The funds are alleged to have been split between Napoles, members of the Philippine Congress, officials facilitating the transfer of PDAF funds, and local mayors and governors.

47 real estate properties and 16 vehicles have also been restrained on the grounds that they were purchased using funds obtained via the scam. Investigations are ongoing.

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 and terrorist financing through professionals' client accounts

The use of client accounts operated by professionals such as lawyers and accountants, has been identified by FATF as a potential vulnerability to money laundering and financing of terrorism. The use of client accounts may enable criminals to place money with the financial system and/or use the account as part of their layering activity with fewer questions being asked by financial institutions because of the perceived respectability and legitimacy added by the involvement of professional service.[2]

Client accounts may be used to obscure beneficial ownership of funds that are used in a transaction and ultimately the involvement of launderers in the purchase of assets. This hinders law enforcement agencies' and financial institutions' efforts to detect and track transactions involving criminal proceeds through professionals' client accounts.

Key reasons that client accounts are attractive to launderers and terrorist financiers

In particular, client accounts may be attractive to criminals as they can:

- be used as part of the first step in converting the cash proceeds of crime into other less suspicious assets;
- permit access to the financial system when the criminal may be otherwise suspicious or undesirable to a financial institution;
- serve to help hide ownership of criminally derived funds or other assets; and
- be used as an essential link between different money laundering techniques, such as purchasing real estate, setting up shell companies/trusts and transferring the proceeds of crime.

Thus, abuse of client accounts is attractive to criminals at all three stages of money laundering. The client account may be an attractive option to place funds, particularly if the criminal perceives that they are likely to attract less CDD by using professional services to place proceeds in the client account than would be attracted by approaching a financial institution. Client accounts are also useful in layering, particularly where the launderer or terrorist financier wants to access services, or make transactions, that may not be otherwise accessible or would seem unusual for the individual involved. Finally, client accounts are an attractive vehicle through which to integrate proceeds into sectors such as real estate as use of legal services is common practice in such transactions.

As with other money laundering techniques, abusing the client account is an attempt to make the movement or use of criminal proceeds seem more legitimate and within normal behaviour. Therefore, launderers and terrorist financiers may attempt to avoid obvious stereotypical behaviour. Therefore, placement in cash is unusual and likely to be suspicious, but by no means the only form that criminal proceeds may be placed in to the account, particularly in the layering stage. Professionals and financial institutions should also be vigilant to more subtle red flags to unusual and suspicious transactions.

Means of abusing client accounts

The FATF identified three principal means of abusing client accounts for money laundering and terrorist financing:

Making transactions through the client account without an underlying legal service

Professional standards should prevent abuse of client accounts to make money laundering transactions without underlying professional services. However, criminals may seek to use client accounts as a deposit taking facility to layer transactions without seeking legal services, despite professional controls. This may require either misleading the legal professionals involved or seeking out a professional willing to turn a blind eye to, or play a complicit role in, the activity.

The particular red flags for instances where clients seek to use client accounts to make transactions without underlying legal services include:

- clients actively avoiding personal contact without good reason
- clients willing to make uneconomic transactions, for example being willing to pay legal fees despite not gaining any added value from involvement of the firm
- clients asking for unexplained or unusual speed of transactions
- clients requesting transactions to third parties without substantiating the reason for the payment.

[2] ***Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals***, FATF 2013 p19 http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf

Clients seeking advice or services to structure payments so as to avoid AML/CFT controls

Professionals should also be vigilant to protect their services from being used to structure transactions to avoid AML/CFT controls. General due diligence, including enhanced due diligence in relation to high risk customers/transactions, should mitigate the risk of exploitation to structure. Failure to conduct due diligence risks reckless involvement in a money laundering transaction or an offence against the AML/CFT Act 2009 in addition to the breach of professional obligation.

As with other forms of structuring, the classic objective of structuring through client accounts would be to avoid reporting thresholds. However, where there are not reporting thresholds, as in New Zealand, structuring may still be conducted to avoid suspicion of financial institutions, to avoid CDD thresholds, or to avoid perceived thresholds. Structuring may also involve breaking up transactions and funds into smaller sums in the names of third parties.

Specific red flags for abuse of client accounts to structure money laundering or terrorist financing transactions include:

- purchase of property for family members in unusual circumstances, for example where they is little personal contact
- unusual third party funding of transactions
- significant private funding and transfers structured in to smaller unexplained transactions
- unusual investments, for example a high level of investment in a dormant company
- unusually high price paid for property.

Aborted transactions

Criminals may seek to use aborted transactions to circumvent professional restrictions preventing conducting transactions without an underlying professional service. The method used is to apparently seek to make a legitimate transaction using the client account. However, before the transaction is completed, the client will abort the transaction, which can legitimately occur for a number of reasons. Aborted transactions become particularly risky when funds are then repaid to third parties who reportedly had an interest in the proposed transaction.

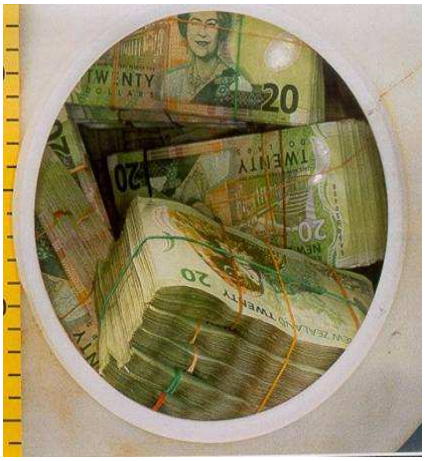
Specific red flags for aborted transactions include:

- repayment to multiple third parties
- a third party appears to be controlling the transaction
- unusual demand for speed
- client avoids contact.

For more information on vulnerabilities in client accounts, and vulnerabilities of legal professionals generally, please refer to the FATF guidance document *Risk Based Approach Guidance for Legal Professionals,* available on the FATF website at: http://www.fatf-gafi.org/topics/fatfrecommendations/documents/riskbasedapproachguidanceforlegalprofessionals.html

New Zealand Case Studies

Operation Rock



Two offenders involved in the importation of ecstacy laundered large amounts of cash through a lawyer's trust account. A total of $400,000 cash was given to the lawyer who banked it into his trust account on behalf of the two offenders. The lawyer had conducted no due diligence on the offenders and did not report an STR. However, the bank that held the lawyer's trust account submitted suspicious transaction reports when the lawyer deposited $100,000 on four occassions. The offenders had instructed the lawyer the cash was being held on behalf of their company registered in Gilbraltar. This alleged company was a shell company that "lent" one of the offenders the $400,000 in order to purchase a property in Auckland. Another lawyer was engaged by the offender to facilitate this "loan" and the purchase of the house in the offender's name. The funds for the purchase of the house therefore looked legitimate (a loan from a company). Effectively, two lawyers from different law firms had been involved in the money laundering process.

Typologies:

Use of professionals
Shell company
Loan back method used to purchase property

Money Laundering Indicators:

- Unexplained large cash deposits

Operation Cape (see also ARU update)

Timothy Clifford, a methamphetamine manufacturer and dealer in the Waikato region, used an accountant to receive cash from his drug dealing and convert it into various purchases of farm land over a number of years . He used two of his farm employees to collect and take cash from drug sales to the accountants office. The accountant had 12 accounts held at different banks in which he would bank the cash. The accounts were held for his accountancy practice, a gift shop he and his wife owned,his personal accounts and a company account he was nominee director and shareholder of on behalf of the drug offender. The accountant went to different branches across the Waikato region and banked the cash into the various accounts. Some excuses he gave about the source of the cash were "it was cash takings from a client who owned a bar" or "it was his cash takings from a stall he operated at a market". The deposited cash would then be electronically transferred to his accountancy practice to be held on behalf of Clifford. With his accumulated wealth, Clifford purchased farm land in the name of his family trust. The trustee of his trust was a corporate trustee company that the accountant was the director and shareholder of. This trust arrangment enabled Clifford to hide the fact he owned the farm land . It was estimated that, over ten years, the Clifford had accumulated $4.8 million from his drug offending. He was sentenced to 12 years prison and his farm land (valued at approximately $5million) was forfeited to the crown.
Whilst it was clear the accountant had engaged in money laundering, he was used as a witness against Clifford in exchange for immunity from prosecution.

Money Laundering Indicators:

- Large cash deposits
- Use of third parties
- Use of a professional
- Co-mingling of criminal proceeds with legitimate business
- Use of nominee directors/shareholders to hide the ownership of business
- Purchase of real estate
- Use of trust to hide the ownership of real estate

AUSTRAC Typologies[3]

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

Complex 'round robin' tax evasion scheme involving Vanuatu based accountant

'Round robin' tax evasion schemes essentially aim to make funds movements appear as payments to other parties while, in reality, the funds ultimately return to the original beneficiary.

In this case enquiries identified that the principal promoter and operator of a tax evasion scheme was a senior partner of an accountancy firm based in Vanuatu. Analysis of AUSTRAC information uncovered the round robin tax evasion scheme which involved the transfer of funds between Australia-based individuals and bank accounts of companies in other countries to evade tax in Australia. The method used to facilitate tax evasion was:

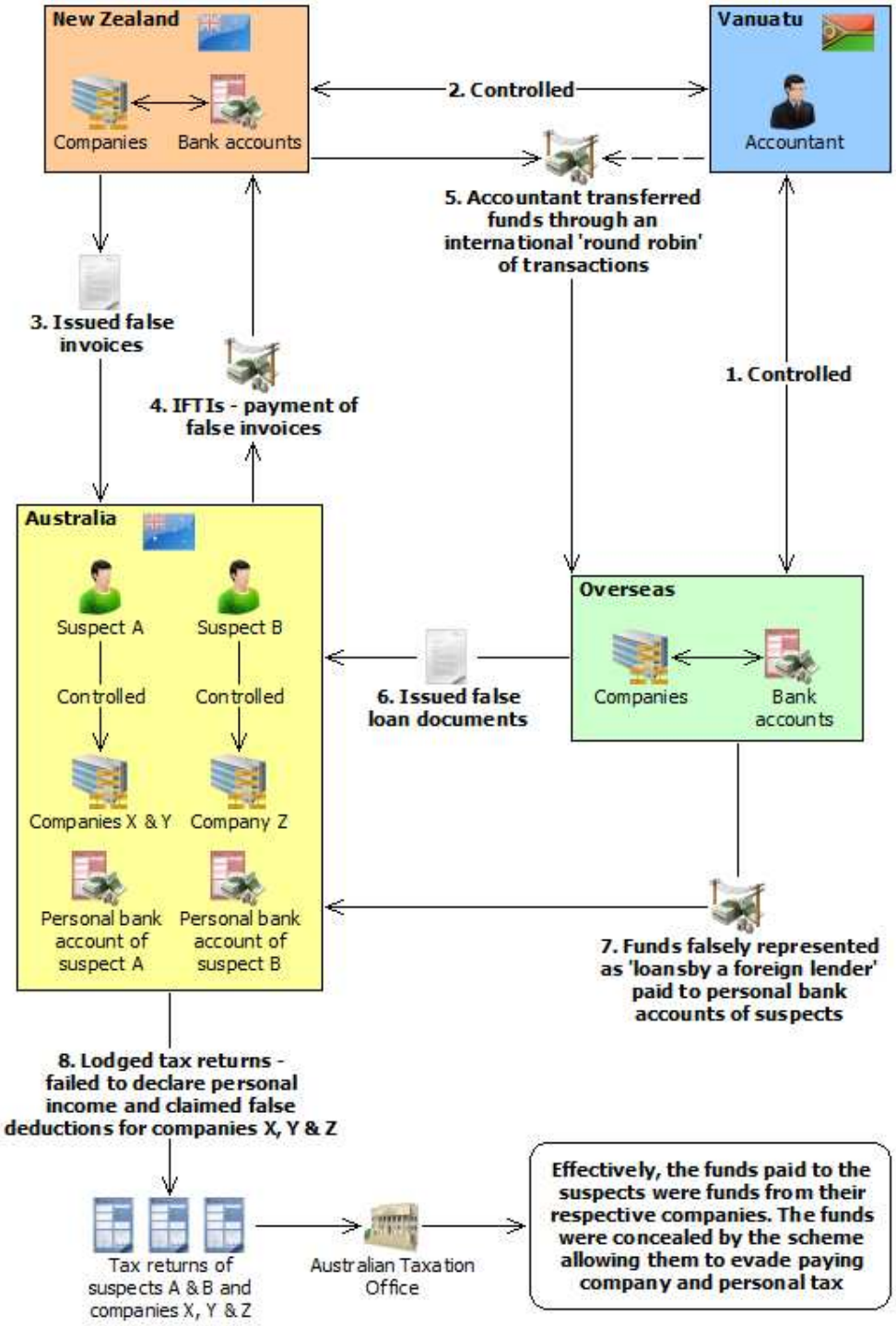
1. Suspects in Australia transferred funds from their companies' accounts to the bank accounts of companies in New Zealand. The New Zealand companies and the bank accounts were controlled by the Vanuatu-based accountant, who was a signatory to the bank accounts.
2. The payments were falsely described in the suspects' companies' records as expenses in the form of 'management and consultancy fees'. False invoices were created for the fictitious expenses. No evidence was available to show that any consulting work had been carried out. The invoice amounts matched the amounts paid to the bank accounts in New Zealand.
3. The false expense payments were claimed as deductible expenses in the tax returns of the Australian companies, fraudulently reducing the companies' taxable income and the amount of tax they were assessed as liable to pay.
4. The accountant then transferred the funds under the guise of international 'loans' through a series of round robin international transactions, through accounts held in the name of companies owned and operated by the accountant.
5. The accountant transferred the funds into the personal bank accounts of the suspects in Australia. The funds were transferred via an overseas company controlled by the accountant, separate to the companies in New Zealand that received the funds originally.
6. In order to disguise the funds as loans, false documents were created purporting to be international loan agreements with a foreign lender. Loans are not assessable income and are tax free.
7. The funds, disguised as international loans, were not disclosed in the suspects' personal tax returns. The suspects were thus assessed as liable for less tax than they should have been, thereby avoiding income tax obligations.
8. Effectively, the 'loans' paid to the suspects were funds from their respective companies but were disguised by the scheme, allowing them to evade approximately AUD750,000 company and personal tax.

Both suspects in Australia were ultimately convicted of tax evasion and fraud offences and sentenced to three years imprisonment. The suspects also became liable to pay penalties and interest to the Australian Taxation Office of more than AUD1 million and AUD900,000 respectively. The accountant was convicted of conspiring to defraud the Commonwealth and was sentenced to eight years and 11 months imprisonment.

Indicatorsof 'round robin' tax evasion*:*

- Account activity inconsistent with customer profile
- Customer receives international funds transfers declared as loans from a foreign lender
- Customers undertaking complicated transfers without a business rationale
- Different ordering customers sending international funds transfers to the same beneficiaries
- False invoices created for services not carried out
- International funds transfers to a high-risk jurisdiction
- Multiple high-value international funds transfers to and from Australia with no apparent logical reason

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


New Zealand
Companies
Bank accounts
2. Controlled
Vanuatu
Accountant
5. Accountant transferred funds through an international 'round robin' of transactions
3. Issued false invoices
4. IFTIs - payment of false invoices
1. Controlled
Australia
Suspect A
Suspect B
Controlled
Controlled
Companies X & Y
Company Z
Personal bank account of suspect A
Personal bank account of suspect B
Overseas
Companies
Bank accounts
6. Issued false loan documents
7. Funds falsely represented as 'loans by a foreign lender' paid to personal bank accounts of suspects
8. Lodged tax returns - failed to declare personal income and claimed false deductions for companies X, Y & Z
Tax returns of suspects A & B and companies X, Y & Z
Australian Taxation Office
Effectively, the funds paid to the suspects were funds from their respective companies. The funds were concealed by the scheme allowing them to evade paying company and personal tax

Domestic and International AML/CFT News

NEW ZEALAND:

Police shut down Head Hunters led drug ring

Police arrested eight suspects on 5 May following the termination of a lengthy investigation into the manufacture and supply of methamphetamine in the Auckland region.

The investigation, code named Operation Genoa, has also led to the restraint of over in excess of $2 million in cash and $3 million in assets including a Ferrari, Porsche, Maserati and numerous other motor vehicles, a 30 foot launch, five properties, gold bullion, and silver ingots.

The eight suspects arrested will face a range of charges including manufacturing methamphetamine, money laundering, unlawful possession of a restricted weapon, obtaining a false documents and participating in an organised criminal group.

Two of those apprehended are senior patched members of the Head Hunters gang.

INTERNATIONAL

United States

Criminal charges reportedly close for Credit Suisse and BNP Paribas

The New York Times reported in May that Federal prosecutors are nearing criminal charges against Credit Suisse for offering tax shelter to Americans and BNP Paribas for Sanctions violations.

Potential Record Fines for Sanction Violations for BNP Paribas

French bank BNP Paribas announced in February that it has set aside USD1.1 bn to pay potential penalties for breaches to US sanction. According to reporting to the Wall Street Journal, if such a fine were imposed, it would be the highest ever imposed for sanctions violations (the higher fine imposed on HSBC last year included money penalties for money laundering violations).

HP Agrees to Pay Fines for Laundering Funds to Pay Bribes for Government Contracts

In April, it was reported that HP had agreed to pay USD108m in fines following the company's admission to having created shell companies and bank accounts to launder funds to pay bribes to secure government contracts in Russia, Poland and Mexico.

Laundering through Online Gambling Sites

In April, computer security software company McAfee published a report[4] that found that criminals are easily able to use online gambling sites to launder proceeds of crime made through ransomware and other methods of cyber theft. The main factors facilitating laundering through online gambling are reported to be the rise of unlicensed sites and online anonymity, which may be enhanced by using Bitcoins and the Tor network. Of particular note, is the number of unlicensed online gaming sites, which McAfee reports to be ten times the number of licensed sites.

[4] ***Jackpot! Money Laundering Through Online Gambling,*** McAffee 2014 http://www.mcafee.com/us/resources/white-papers/wp-jackpot-money-laundering-gambling-summary.pdf

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