Financial Intelligence Unit

New Zealand Police

Quarterly Typology Report
Fourth Quarter (Q4) FY2015-16

(1 April – 30 June)

ALTERNATIVE BANKING PLATFORMS

(Issued September 2016)

INTRODUCTION

This report is the fourth Quarterly Typology Report (QTR) of 2015/2016 produced by the Financial Intelligence Unit (FIU), part of the New Zealand Police Financial Crime Group. As the QTR 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 QTR as part of its obligations under section 142(b)(i)[1] and section 143(b)[2] of the AML/CFT Act 2009.

PURPOSE

The purpose of the QTR is to provide an accurate picture of current, emerging and longer term factors impacting on the AML/CFT environment. The QTR 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 QTR is a law enforcement document. However, it does not include sensitive reporting or restricted information and is published on the FIU website. The QTR is produced using a variety of sources and qualitative/quantitative data.

[1] Section 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

[2] Section 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

DEFINITION OF MONEY LAUNDERING

Under New Zealand legislation the money laundering offence is defined in section 243 of the Crimes Act 1961 and section 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
- 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

Financial Intelligence Unit

Information on the FIU is provided separately in permanent **Annex 2**.

SUSPICIOUS TRANSACTION REPORTING TO THE FIU

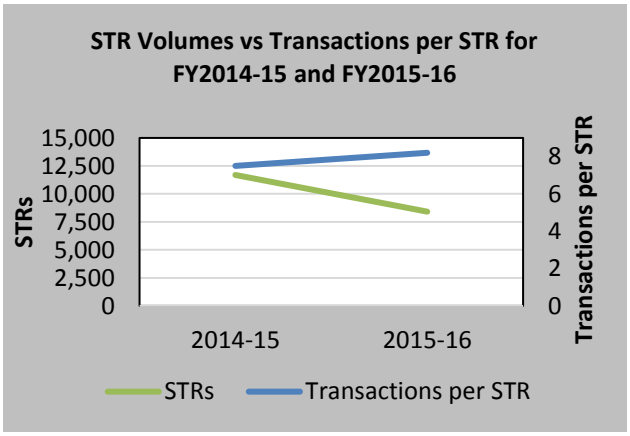
Suspicious transaction reports	FY2015-16	FY2014-15	FY2013-14	FY2012-13
Accepted	**8,418**	11,691	10,355	n/a
Rejected	**2,011**	1,077	1,846	n/a
Total	**10,429**	12,768	12,201	2,600

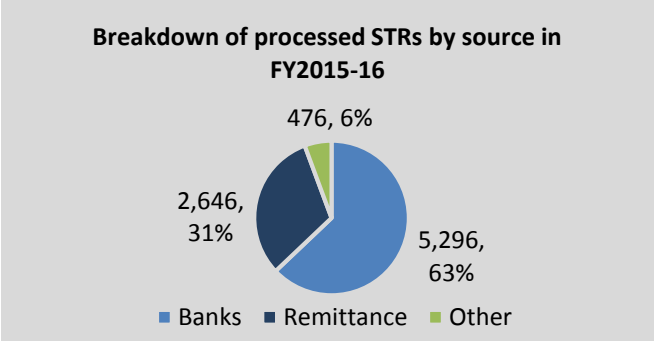
The number of accepted suspicious transaction reports (STRs) has decreased by 3,273 STRs to **8,418** in FY2015-16 from 11,691 in the previous FY. A closer analysis of the reporting shows two divergent trends have occurred in the two main sectors – over the past year, there was a steady increase in banks' reporting and a significant decrease in STRs from the remittance sector. Both trends have been driven by continuous refinement and improvement of transaction reporting processes by reporting entities, which have led to higher-quality STRs as the AML/CFT regime has matured.

The number of rejected STRs for FY2015-16 increased. The temporary increase in rejections resulted from implementation of the goAML upgrade changes, which took place in December 2015, but has subsequently subsided.

STR VOLUMES VS TRANSACTIONS

Although the number of accepted STRs is lower for FY2015-16, the number of transactions per accepted STR has increased to **8.2** from 7.5 in the previous FY2014-15.





STR SUBMISSION BY SOURCE

The majority of STRs are submitted by banks and remittance sector providers. From the accepted 8,418 STRs in FY2015-16, **63%** of those were submitted by banks and **31%** by the remittance sector.

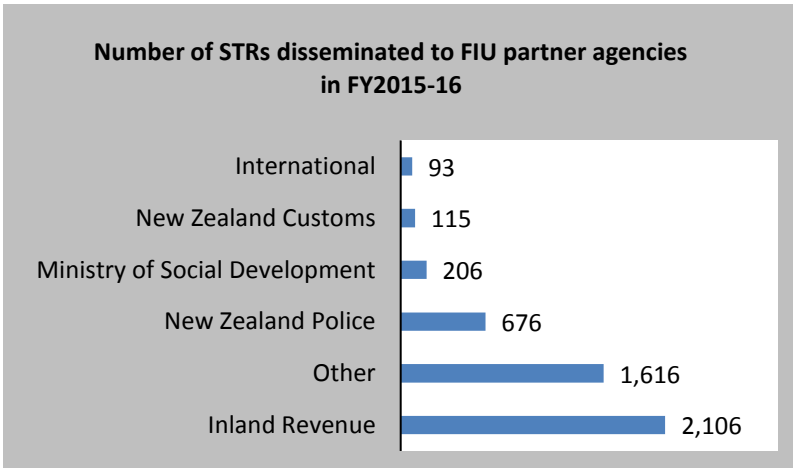
DISSEMINATION OF FIU INTELLIGENCE INFORMATION

The FIU collects and collates information provided by external parties and reporting entities, especially banks and other financial institutions. After the required analysis, intelligence products such as STR content reports, STR spreadsheets and intelligence reports are sent to other investigative and intelligence units within Police, sector supervisors, domestic partner agencies and to relevant international agencies.

STR content reports are basic intelligence products that comprise of the reporting entities grounds for suspicion, the reported transactions and biodata. Often the FIU will add additional value to the STR content report by including information held in Police intelligence systems. These STR content reports primarily contain data from the reported relevant STRs, and also border cash reports and suspicious property reports.

STR spreadsheets are a collection documents for the detection, investigation and prosecution of offences by different prosecuting authorities within the New Zealand government. Once the collection phase is completed, the STRs are exported to a spreadsheet in their raw form. With the exception of the Police spreadsheets they do not have any added value from Police intelligence systems.

Intelligence reports are produced by the FIU intelligence analysts and they involve a wide collection of data including information from the reported STRs. These reports contain data analysis of the STRs, drawn inferences and recommendations made to the intended recipient.



In FY2015-16 FIU produced **238** intelligence products for domestic dissemination, which contained a total of **3,481 STRs**. **40** intelligence products containing **93 STRs** were sent to law enforcement agencies overseas.

These disseminated STRs indicated offences including **tax evasion**, **drug dealing**, **money laundering**, **fraud**, **theft**, **people smuggling**, **online child exploitation**, **customs offences**, **immigration offences** and **terrorist financing**.

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.

CRIMINAL PROCEEDS (RECOVERY) ACT 2009 (CPRA)

As at 30 June 2016, New Zealand Police held Restraining Orders an estimated **NZD264 million** worth of assets. Since CPRA came into effect, an estimated **NZD91 million** worth of assets have been subject to Forfeiture Orders. For the quarterly period ending June 2016, **NZD6.9 million** worth of assets were restrained, and **NZD1.1 million** were forfeited. The majority of restrained assets related to cases where **cannabis offending** (e.g., cultivation, supply) was the predicate offence.

NZD M	This QTR	Last QTR	Last Year
Value of Forfeitures[1]	**1.1**	**2.9**	**2.6**
Value of Restraints[2]	**7.0**	**7.3**	**7.8**
Fraud	-	-	0.4
Money Laundering	-	-	-
Tax Evasion	**2.0**	-	-
Drugs and other offending	**5.0**	7.3	7.4

[1]Value of Forfeitures is based on the date of the Forfeiture Order.

[2]Value of Restraints is based on the date of the Restraining Order, and in very rare cases, this might include assets that are no longer in restraint. For each case CPRA case, a main predicate offence will be identified.
Note that these values are drawn from a dynamic database, where information about cases can be continuously updated.

REPORTED FIGURES OF FIU INTELLIGENCE CONTRIBUTING TO ASSET RECOVERY (AS %) FOR 2009 TO 2016

NZD M	%	FIU information	Total
New Cases	**14%**	**151**	**1,073**
Restraints	**50%**	**192.84**	**386.04**
Forfeitures	**33%**	**29.68**	**91.05**

14% of the 1,073 cases since the beginning of the Criminal Proceeds (Recovery) Act in 2009, are reported to have received and/or requested FIU information, often in the form of Intelligence Reports or STR Content Reports.

These 14% of cases represent a disproportionate value of assets, with an estimated 50% of restrained assets and 33% of forfeited assets (by value).

OBSERVATIONS – HAMILTON ASSET RECOVERY UNIT

Introduction

CPRA is now seven years old, and all ARUs in New Zealand are seeing increased referrals, with notable increases from government agencies outside of Police. Domestic, criminally-acquired, and laundered funds have been forfeited from a wide range of crime types, including frauds against government, tax related crimes and crimes associated with drugs and organised crime. Foreign predicate crimes have featured in a number of recent investigations and a notable forfeiture was achieved as a

result of a joint China / New Zealand investigation which evidenced the laundering of funds in New Zealand obtained through a series of frauds committed in China. This outcome reflects New Zealand's commitment to work with foreign jurisdictions to recover criminal proceeds that have been concealed in New Zealand.

Real-estate

A common theme has been the acquisition of real estate, this typology has been evident in several investigations. Predicate crime types have included a range of domestic income-generating crime types. The New Zealand property market is very strong and we are seeing an increase in investment in this sector. Concerns have been raised in the media regarding the source and legitimacy of foreign investor funds with specific reference to China, real estate therefore remains a sector of interest.

Trusts, Companies and other Legal persons

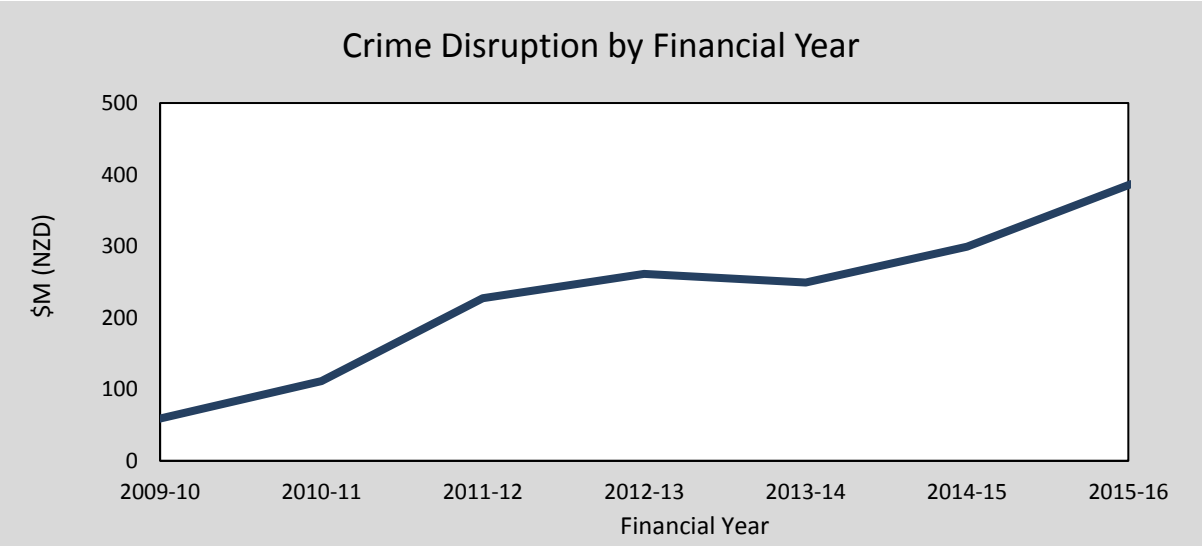
The use of trusts, companies to conceal beneficial ownership and disguise control of property, continue to feature in more significant investigations. The creation and of these has involved the use of various professionals notably lawyers located in both New Zealand and in foreign jurisdictions. The use of foreign companies has featured in some investigations when it has been identified that funds applied to purchase property have been disguised through the use of elaborate loan arrangements with foreign companies which operate in Asia but which have been formed in foreign jurisdictions.

Other trends

The use of third party banking facilities and the concealment of property using third parties names continues to be a common typology. As a result of the AML/CFT legislation, we have seen greater compliance within the financial sector which has resulted in more frequent and larger value cash discoveries being made during policing operations. The acquisition of high value vehicles and other high value items of property is consistent in most cases, as is the use of criminally acquired income at casinos.

CRIME DISRUPTION

According to the Proceeds of Crime Disruption Index (POCDI), every NZD1 worth of assets restrained contributes to an estimated NZD3.30 in crime disruption, and NZD3.50 for every NZD1 worth of assets forfeited. The below graph shows the estimated amount of crime disruption achieved since the CPRA was enacted, by financial year.



ALTERNATIVE BANKING PLATFORMS

WHAT IS AN ALTERNATIVE BANKING PLATFORM?

Alternative banking platforms are systems that provide the functionality of a bank but operate outside the traditional global banking space. They are also known as payment platforms or virtual banks.

The Australian Criminal Intelligence Commission has described alternative banking platforms as entities facilitating the operation of a bank (in effect providing the functionality of a bank) outside of the regulatory system. Services provided include an online banking interface, which sits above and coordinates one or multiple bank accounts, supported by company structures, in various international locations.[3]

According to EUROPOL,[4] alternative banking platforms have become a vehicle for transferring both small and large amounts of money. They have been used for layering of funds and anonymously purchasing crime enablers such as software, counterfeited documents, credit cards etc. These are largely used to commit other crimes such as economic and financial frauds, organised terrorism and other offences.

Alternative banking platforms operate like an Informal Value Transfer System or electronic hawala network transferring value between clients within an online banking platform. This provides a ledger for a pooling account or accounts that can be then held with regular financial institutions. Funds can remain within one pooling account as long as value transfers between clients are balanced by the software.

Alternative banking platforms are often created by specialist facilitators specifically for the purpose of circumventing anti-money laundering reporting legislation and law enforcement attention. They most commonly operate in tax havens including Panama, the Caribbean, the Far East and the Gulf region.

ALTERNATIVE BANKING IN NEW ZEALAND

In New Zealand, the Financial Intelligence Unit of New Zealand Police (NZ-FIU) has identified a number of instances where New Zealand Offshore Finance Companies (NZOFCs)[5] have been established using particular New Zealand Trust and Company Service Providers (TCSPs) to support the movement of illegal proceeds. Frequently, NZOFCs identified by the NZ-FIU use similar criminal methodologies to alternative banking platforms.

ALTERNATIVE BANKING PLATFORM METHODOLOGY

The NZ-FIU has observed that criminal alternative banking platforms using a New Zealand legal entity structure have often been established by a New Zealand TCSP acting on behalf of overseas clients. The entity structure that is used to form the alternative banking platform is a New Zealand limited liability company or, in some cases, a limited partnership.

[3] Australian Criminal Intelligence Commission "Organised Crime in Australia 2015" https://www.acic.gov.au/sites/g/files/net1491/f/2016/06/oca2015.pdf?v=1467241691

[4] EUROPOL Brochure 2015 "Alternative Banking Platforms" https://issuu.com/martinksinan/docs/fin_brozurka_en/1

[5] An NZOFC is a New Zealand registered company that offers financial services overseas.

Shareholders will either be New Zealand nominee shareholding companies owned by the TCSP or entities registered overseas. Virtual offices have also been used as the location of the registered office in New Zealand. Hence the beneficial owner of the alternative banking platform is generally hidden.

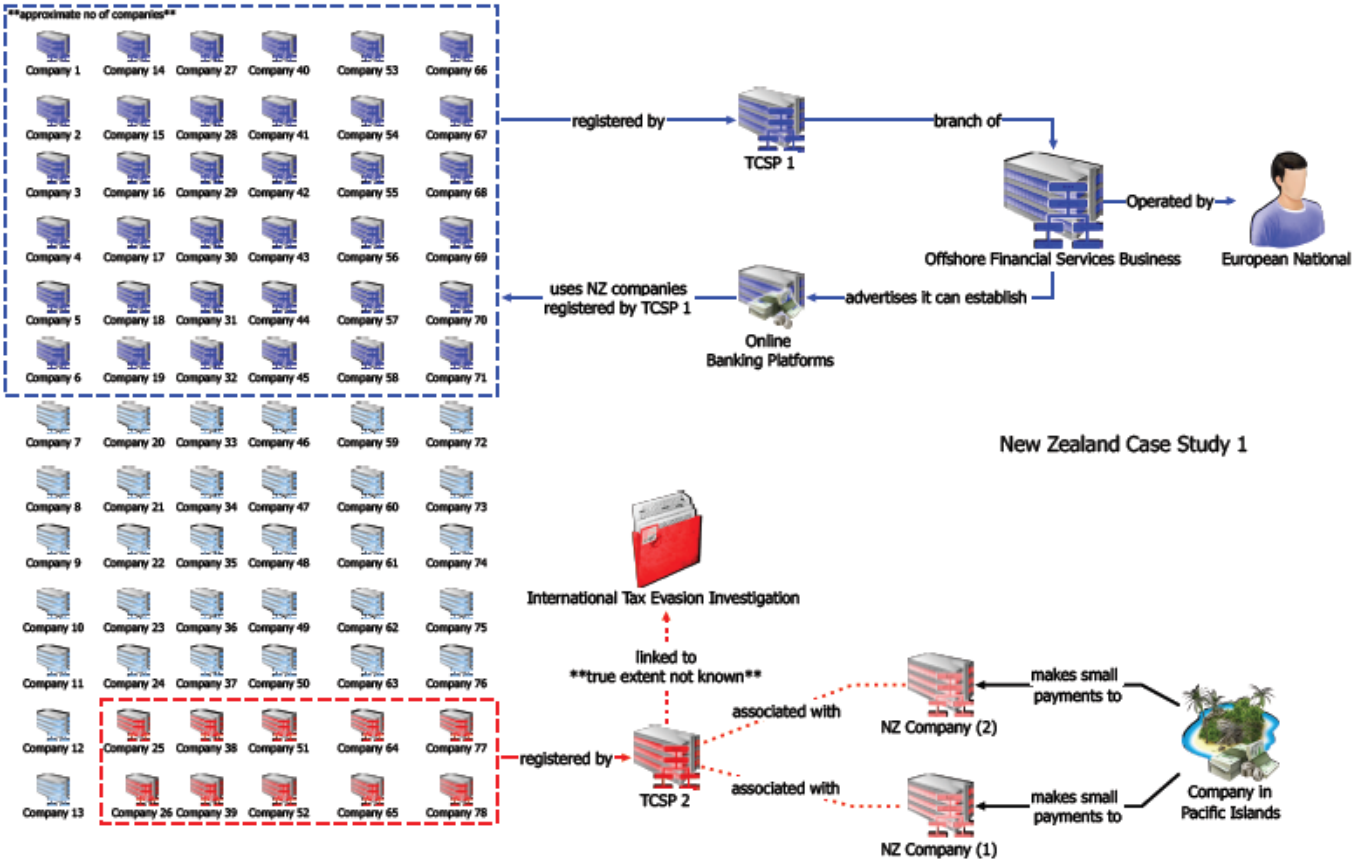
Websites established for the alternative banking platform often promote the alternative banking platform's status as a New Zealand registered company implying it was regulated by reputable laws in New Zealand. Websites may also provide a disclaimer to ensure they were not breaching banking legislation in New Zealand. The disclaimer may look something like:

> *"XYZ Savings & Loans Limited is not a registered bank in New Zealand. We operate as a New Zealand Offshore Finance Company".*

Websites may also offer financial services, such as opening investment accounts, debit and credit cards and financial planning services. High investment returns through trading on the foreign exchange market may also be identified.

NEW ZEALAND CASE STUDY 1

Between 2010 and 2013 the NZ-FIU and Reserve Bank of New Zealand received queries from overseas questioning the legitimacy of 78 New Zealand registered companies that appeared to be operating overseas as alternative banking platforms. Nearly 60% of the questioned companies were registered by two TCSPs in New Zealand.



Intelligence gathered by the NZ-FIU indicated that TCSP1 was a company formation branch of an offshore financial services business, operated by a European national. This offshore financial services business advertised on its website that it could establish online banks for clients using a banking software application. The European national used companies registered in New Zealand by TCSP1 to establish alternative banking platforms.

TCSP2 had a link to an international tax evasion investigation. The true extent of the link was not known by the NZ-FIU, however, the New Zealand arm of the operation identified TCSP2 was associated with two New Zealand registered companies that received small payments from a company in one of the Pacific islands. The NZ-FIU identified at least ten NZOFCs registered by TCSP2.

NEW ZEALAND CASE STUDY 2 – OP LOC (*UNISTATE*)[6]

In March 2013, the Federal Bureau of Investigation of the United States (FBI) contacted the NZ-FIU requesting all information held on a New Zealand company called Unistate, its bona fides and the legitimacy of all recorded addresses. It was alleged by the FBI that Unistate was part of a fraudulent scheme operated in the United States in 2009 whereby fraudulent letters of credit were used.

Background on Unistate

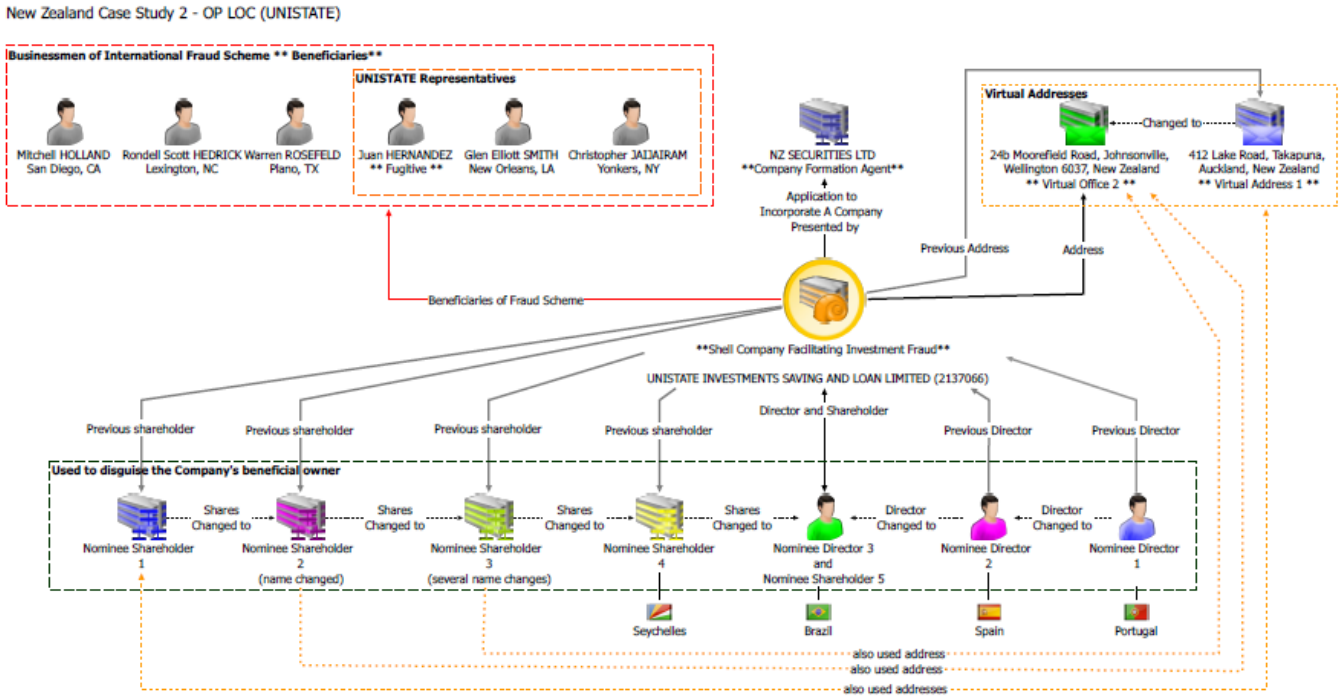
- Unistate was a suspected shell company facilitating investment fraud by overseas persons.
- Unistate was registered by a New Zealand company formation agent called NZ Securities Ltd.
- Nominee directors and shareholders were used in the formation. These directors acted purely as nominees. During the time Unistate was registered as a company (5 June 2008 to 29 February 2012) directorship changed three different times. In the same period, the shareholders of Unistate changed four times.
- The company structure used to form Unistate was that similar to nine other New Zealand companies identified by overseas law enforcement agencies to have facilitated fraud in various foreign jurisdictions.

Main features of Unistate

- It was registered by a Company Formation Agent.
- Numerous nominee directors and nominee shareholders were used to disguise the company's beneficial owner.
- The company did not have a physical presence in New Zealand.
- The registered physical address for Unistate was 412 Lake Road, Takapuna, Auckland, the address for the registering NZ Securities Ltd – a company formation agent previously utilised by New Zealand registered shell companies controlled by overseas criminals.

Unistate was registered on 5 June 2008 and struck off the New Zealand Companies Register on 29 February 2012.

[6] https://www.fbi.gov/contact-us/field-offices/jacksonville/news/press-releases/jury-convicts-businessmen-of-international-fraud-scheme



Outcome

Evidence (Brief of Evidence and Exhibits) provided to the FBI by the NZ-FIU, along with evidence given by the then NZ-FIU Manager (Pat O'Sullivan) in April 2015 supported several successful convictions in a Florida law court.

OVERSEAS CASE STUDY – EUROPE

Operation VERTIGO[7] began when investigators from the Netherlands and Germany observed a large number of VAT (value added tax) reimbursements from certain companies. In this instance, the criminal network used alternative banking platforms across the globe to facilitate crime-related money transfers and associated money laundering activities amounting to several hundred million euros.

[7] Major Europe-wide VAT fraud network busted with the support of Eurojust and Europol
http://www.eurojust.europa.eu/press/PressReleases/Pages/2015/2015-03-03.aspx

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 Coordination 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 on Money Laundering. The FIU can be contacted at: **fiu@police.govt.nz**

Annex 3

TYPOLOGY INDICATORS

GENERAL INDICATORS

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

- Transactions involving locations with poor AML/CFT regimes or high exposure to corruption
- Significant and/or frequent transactions in contrast to known or expected business activity
- Significant and/or frequent transactions in contrast to known employment status
- Ambiguous or inconsistent explanations as to the source and/or purpose of funds

- Where relevant, money presented in unusual condition, for example, damp, odorous or coated with substance
- Where relevant, nervous or uncooperative behaviour exhibited by employees and/or customers

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

- Purchase/sale of real estate above/below market value irrespective of economic disadvantage
- Cash purchases of valuable assets with cash and/or cash deposits for valuable assets
- Low value property purchased with improvements paid for in cash before reselling
- Rapid repayment of loans/mortgages with cash or funds from an unlikely source

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

Possible indicators (specific)

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

Additional Indicators:

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers involving accounts located in high-risk countries or known tax havens
- Transfers to offshore jurisdictions with no business rationale
- Multiple transfers sent to same person overseas by different people
- Departure from New Zealand shortly after transferring funds
- Transfers of funds between various accounts that show no economic sense (i.e. multiple transfers incurring bank fees where one single transfer would have been sufficient)

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

CASH DEPOSITS — placement of cash into the financial system.

Possible indicators (specific)

- Large cash deposits followed immediately by withdrawals or electronic transfers

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

- Known or suspected criminal entities establishing trust or bank accounts under charity names
- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers involving accounts located in high-risk countries or known tax havens
- Transfers to numerous offshore jurisdictions with no business rationale
- Entities that use third parties to distribute funds or have weak financial governance mechanisms

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

Possible indicators (specific)

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

- Limited or no securities transactions recorded before settlement requested

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

Possible indicators (specific)

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

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

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