

Financial Intelligence Unit

New Zealand Police

Quarterly Typology Report

Second Quarter (Q2) FY2016-17

(1 October – 31 December)

HUMAN TRAFFICKING and PEOPLE SMUGGLING

(Issued April 2017)

INTRODUCTION

This report is the second Quarterly Typology Report (QTR) of 2016/2017 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

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

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.

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 that is the proceeds of an offence
- ♦ knowing or believing that such property is the proceeds of an offence, or being reckless as to whether it is the proceeds of an offence, and
- ♦ applies even though the person who committed the offence has not been charged or convicted

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

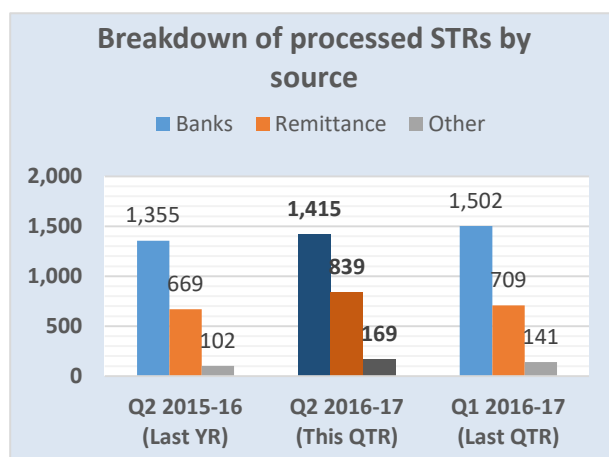
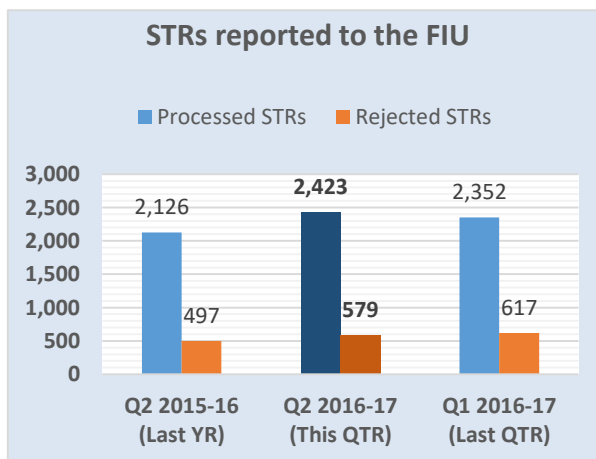
Financial Intelligence Unit updates

Information on the FIU is provided separately in permanent [Annex 2](#).

SUSPICIOUS TRANSACTION REPORTING TO THE FIU

The number of reported suspicious transaction reports (STRs) processed by the FIU in Q2 2016-17 was **2,423**. This total is 71 reports more than in the last quarter, and considerably greater compared to the same Q2 last financial year.

The number of rejected STRs has decreased to **579** from 617 in previous quarter. Comparing to the same Q2 last financial year, the FIU rejected about 16 per cent more reports.



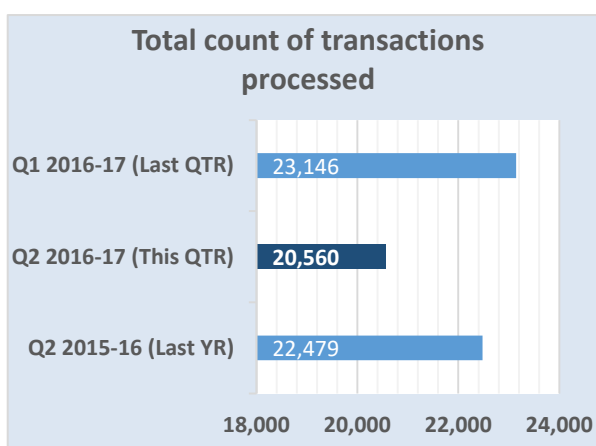
STR SUBMISSION BY SOURCE

The majority of STRs are submitted by banks and remittance service providers. The breakdown of the processed reports for Q2 2016-17 is similar to the previous quarter, but with a slightly greater proportion coming from remittance versus banks.

Comparing Q2 number of processed STRs received from money remitters with the same Q2 last financial year, there has been a 25 per cent increase.

TRANSACTIONS IN STRS

In Q2 2016-17, the number of transactions in accepted STRs was **20,560** and has increased by 2,586 transactions from the previous quarter, and is 9 per cent less than in the same Q2 last financial year.



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)

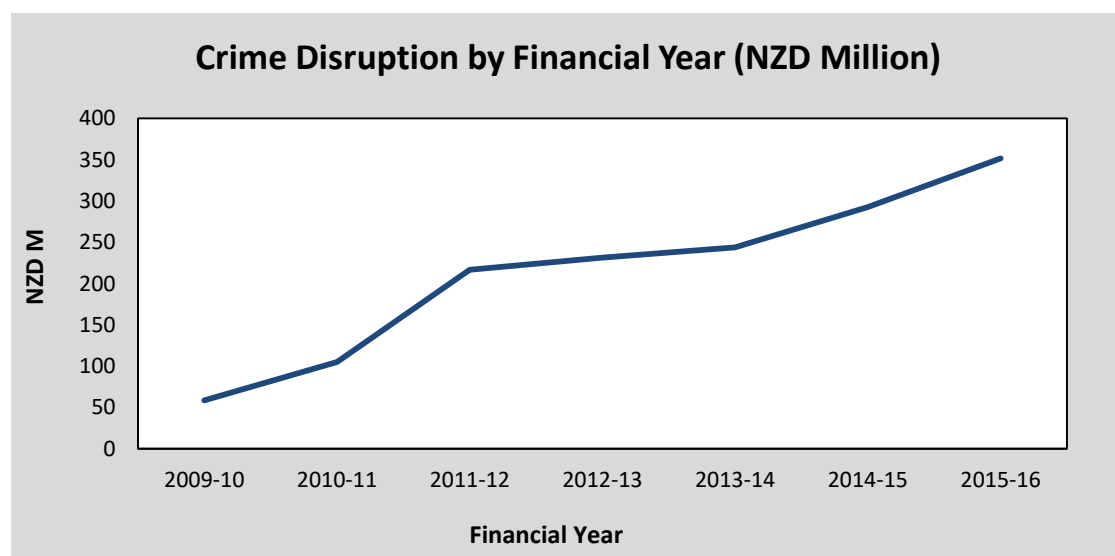
As at 31 December 2016, New Zealand Police held Restraining Orders at over an estimated **NZD262 million** worth of assets. Since CPRA came into effect, an estimated **NZD161 million** worth of assets have been subject to Forfeiture Orders. For the quarterly period ending December 2016, **NZD5.0 million** worth of assets were restrained, and **NZD8.1 million** were forfeited.

NZD Million	As at 31-Dec-16
Value of Forfeitures	161
Value of Restraints	262
Fraud, Money Laundering & Tax Evasion	129
Drugs & Other Offending	133

Note that these values are drawn from a dynamic database, where information about cases can be continuously updated.

CRIME DISRUPTION

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



Connections between money laundering and human trafficking/ people smuggling

The 2016 Global Slavery Index estimates nearly 46 million people are subject to some form of modern slavery in the world today.³ This presents a number of significant challenges for those involved in the prevention of money laundering generated through the activities of human trafficking and people smuggling.

HUMAN TRAFFICKING

As at 2014, with the exception of North Korea, all countries had adopted domestic legislation criminalising some form of modern day slavery. Modern slavery is an umbrella term used to describe a range of related criminal practices, including human trafficking, forced and compulsory labour, bonded labour, and sexual or criminal exploitation, among others. Yet slavery, in the form of human trafficking, is a flourishing criminal enterprise. Human trafficking is now recognised as the modern day form of slavery that exploits and provides commercial gain – a crime against the person, requiring no border crossing and exploitation that is based on involuntary participation.

Article 3(a) of the Trafficking in Persons Protocol⁴ defines human trafficking as

“the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.”

According to Organisation for the Security and Cooperation in Europe (OSCE⁵), trafficking represents a process rather than a single offence – a process involving different stages or nodes through which victims pass. Such stages typically involve different persons at each stage of the 3-stage process: (1) recruitment/ abduction, (2) transfer and transportation to a point of exploitation, and (3) exploitation.

Trafficked people, like drugs and weapons trafficking, are unfortunately considered just another commodity in a range of criminal activities perpetrated by domestic and foreign individuals and organised crime groups. Through collaboration, organised crime is able to maximise illicit financial gain. Human trafficking is a high-value business for criminals. It represents an opportunity for repeat exploitation and repeated sales, unlike drugs that can only be sold once. Also attractive is the fact that internationally, human trafficking carries low risk of losing business due to low levels of detection and successful prosecutions. Success is further managed by the organised criminals involved through coercion of victims in combination with the use of well-known, considered money laundering methods.

³ http://www.globalslaveryindex.org/findings/?gclid=CN2SsJ_Kw8MCFcRQ7Aod8H0A8g

⁴ <https://www.osce.org/odihr/19223?download=true>

⁵ <http://www.osce.org/>

PEOPLE SMUGGLING

People smuggling (also known as smuggling of migrants) differs from human trafficking in the fact those participating do so on a voluntary basis. People smuggling is considered a crime against the border as the smuggling process requires a border crossing, making it a transportation based criminal activity. For people smuggling, the focus is on the movement of people, rather than their exploitation.

In Europe, estimates within a joint EUROPOL-INTERPOL Report on Migrant Smuggling Networks indicate the annual turnover of migrant smuggling was worth an estimated USD5-6 billion in 2015,⁶ representing one of the main profit-generating activities for organised criminals in Europe. Driven in many instances by the desire for better employment and economic opportunities, personal and/or familial betterment, and/or to escape persecution, violence or conflict. It is clear that although human trafficking and people smuggling have different characteristics, both generate large amounts of money.

Article 3(a) and (b) of the Smuggling of Migrants Protocol⁷ defines people smuggling as

"the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State Party of which the person is not a national or a permanent resident."

"Illegal entry" shall mean crossing borders without complying with the necessary requirements for legal entry into the receiving State.

Although participation is voluntary, smuggled migrants can become vulnerable to abuse and exploitation due to the circumstances in which they are transported. Circumstances include suffocating in containers, perishing in deserts or drowning at sea. Although people smuggling affects almost every country in the world, undermining the integrity of countries and communities, and costing thousands of people their lives every year, the number of people smuggled each year remains unverifiable.

CONNECTIONS TO MONEY LAUNDERING

With significant numbers of people involved in the activities of human trafficking and people smuggling, criminals must disguise their money laundering methods through what they hope will appear to be normal financial transactions in a normal business context. Similar to many other predicate crimes which support the need for money laundering, human trafficking and people smuggling create large amounts of cash, simply because those who seek to participate⁸ or those who are exploited along the way either pay cash or cash is paid in return for a service⁹ they provide.

⁶ <https://www.europol.europa.eu/newsroom/news/europol-and-interpol-issue-comprehensive-review-of-migrant-smuggling-networks>

⁷ https://www.unodc.org/documents/southeastasiaandpacific/2011/04/som-indonesia/convention_smug_eng.pdf

⁸ Those who seek to be smuggled across a border typically pay for the service using cash.

⁹ Trafficked persons exploited during the process will be paid for in cash. This cash will be paid to the person controlling the exploited individual(s). This process limits the formation of a 'paper trail'.

An assessment by the International Labour Organisation in 2014 estimated 21 million slaves generated annual profits of USD150 billion.¹⁰ Another study in 2003 found that a single sex slave could earn their controller USD250,000 a year.¹¹

The very nature of these activities also presents a number of issues in the prevention and detection of money laundering activities at all three stages of the process – placement, layering and integration. For the reason that billion-dollar profit margins cannot legally enter financial institutions unreported, human traffickers resort to a range of money laundering schemes. Money service businesses are often pinpointed as a means for migrants to pay smugglers for passage, but according to INTERPOL this may only amount to around 2 per cent.¹² With a large proportion cash, bank accounts become a necessity to process day to day operations and profits.

Depending on the level of sophistication and size of the networks involved in human trafficking and people smuggling, several money laundering methods are likely to be used to place, layer and integrate the mainly cash derived profits into the legitimate economy. Couriers may be utilised to carry large amounts of money across borders. This could be overland, through concealment or by air, smugglers or their relatives own legal enterprises may be used to place criminal proceeds – thus providing a facade of legitimacy for their income. Money laundering may also take the form of direct investment in high-value commodities. Proceeds may be invested in real estate and legal businesses in both the country of origin and the destination.

Legal business structures can also facilitate migration flow. However, the issue arises when determining to what extent such structures are complicit in smuggling activities or whether they were purposefully targeted. Vulnerable sectors or industries which may be used to facilitate laundering of illicit funds generated by human trafficking and people smuggling include catering, hotels, transport companies, shops, barbershops, internet cafés and travel agencies. Importantly, such businesses may also be used along the trafficking and smuggling routes to support the facilitation activities of the networks (for instance, by providing logistical support) or directly launder the proceeds of smuggling activities.”¹³

PREVENTATIVE AND INVESTIGATIVE CHALLENGES

There are a number of direct challenges caused to society by these forms of crime, even when participants are voluntarily involved, as in the case of people smuggling. In its totality as a business activity (similar to almost all other predicate offences), human trafficking and people smuggling present a number of challenges which create risk for the legitimate financial sector because of the range of different actors performing a range of different roles. Participants include small-scale smugglers arranging ad hoc services to larger smuggling networks dividing the work among the actors involved. These actors can have different functions: coordinator or organiser, recruiter, transporter or guide,

¹⁰ http://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_243201/lang--en/index.htm

¹¹ <http://www.acams.org/wp-content/uploads/2015/08/Human-Trafficking-Monies-in-the-Community-Banks-N-Lake.pdf>

¹² <https://www.gtnews.com/articles/migrant-smuggling-and-money-laundering-does-europe-appreciate-the-threat/>

¹³ https://www.europol.europa.eu/sites/default/files/publications/ep-ip_report_executive_summary.pdf

spotter, driver, messenger, enforcer, service provider or supplier (including corrupt officials, taxi drivers or financiers, for example).¹⁴

Given the large scale of funds involved in this business and the inevitability that the proceeds are laundered through the financial system, the financial sector faces many challenges in prevention and investigation. These challenges are multiplied because of the various techniques available to those involved, both facilitators and victims. For example:

- investing in cash intensive businesses, such as nightclubs or strip bars, and perhaps real estate (which may also be involved in predicate offending)
- wiring funds through money services businesses and sending money across international borders using international courier services
- using funds to procure supplies or boats for smuggling
- using victims to facilitate money laundering by acting as personal/ business account holders
- using victims to deposit funds below the reporting threshold

Until recently, anti-money laundering technology was not used sufficiently to identify human trafficking to law enforcement agencies. However, changes to data collection have meant reliable money laundering and human trafficking typologies are now being used.¹⁵ Yet, as outlined in a report by the Financial Action Task Force on Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants, the number of suspicious transaction or activity reports that designate human trafficking or people smuggling are low in comparison with other serious predicate offences.

Cash businesses are likely to pose the most significant challenge in preventing and investigating the laundering of money derived from human trafficking and people smuggling. While acknowledging the rational decision making process of those involved, cash businesses are by their very nature susceptible to the depositing (co-mingling) of illicit cash as such businesses provide a direct avenue into the legitimate financial sector. Businesses operating with large volumes of cash, for instance, massage parlors, employers of domestic servants, and hospitality and agriculture companies — can become ideal money laundering fronts despite financial monitoring which seeks to reveal their true business intent and practices.

While the hallmark of many detection systems is the identification of normal and customary behaviours, often it is what lies between those systems that can indicate human trafficking activities, such as low dollar purchases indicating victims may be being given access to necessities, but have insufficient funds to escape their captors.

¹⁴ https://www.unodc.org/documents/human-trafficking/Basic_Training_Manual_e-books_English_Combined.pdf

¹⁵ <http://www.antimoneylaunderinglaw.com/2010/12/connection-between-human-trafficking-and-money-laundering.html>

CASE STUDIES

Example 1 – Spain

In 2015, Spanish authorities, supported by EUROPOL were effective in dismantling a Chinese network involved in the laundering of criminal proceeds from human trafficking for the purpose of labour exploitation, the production of counterfeit goods and excise tax fraud. Relying on intermediaries and third parties, the organised crime groups established complex corporate structures and various accounts to transfer money to China. The group also offered money laundering and international remittance services to other organised groups based in the European Union at a negotiated percentage of the laundered funds. Between 2009 and 2015, the European branch of this organised crime group laundered over EUR340 million.¹⁶

Example 2 – Australia¹⁷

An investigation disrupting an international people smuggling operation resulted in the arrest and conviction of two Australia-based facilitators. Using information supplied by AUSTRAC, law enforcement was able to establish a people smuggling syndicate using boats to illegally transport foreign nationals from Indonesia to Australia. The majority of prospective customers were Iraqi and Iranian nationals and the syndicate allegedly charged between AUD4,500 and AUD10,000 per person.

AUSTRAC analysis of financial transaction reports demonstrates how over a five-year period suspect B sent 28 international funds transfer instructions (IFTIs) via remittance service providers out of Australia totalling more than AUD42,000. The IFTIs of between AUD100 and AUD5,000 were mainly sent to Indonesia. A small number of the IFTIs were sent with payment details describing them as 'gift' or 'personal'.

AUSTRAC information also included threshold transaction reports (TTRs) indicating

- over a two-month period, bank accounts held in the name of suspect B received two cash deposits totalling more than AUD37,000.
- over a one-year period, suspect B made four large cash withdrawals totalling more than AUD57,000. The cash withdrawals were conducted at various bank branches and were conducted on separate days.

AUSTRAC information also indicated that suspect B sent and received IFTIs while in Indonesia. AUSTRAC's financial intelligence database recorded suspect B as:

- an Indonesia-based 'ordering' customer, sending three IFTIs to Australia from Indonesia over a 10-day period, totalling more than AUD7,000. The 'details of payment' section of the IFTI report for these transactions was left blank by suspect B.
- an Indonesia-based beneficiary, indicating he received six IFTIs totalling more than AUD20,000 sent from Australia to Indonesia over a two-month period.

¹⁶ Page 18, https://www.europol.europa.eu/sites/default/files/documents/report_socata2017_1.pdf

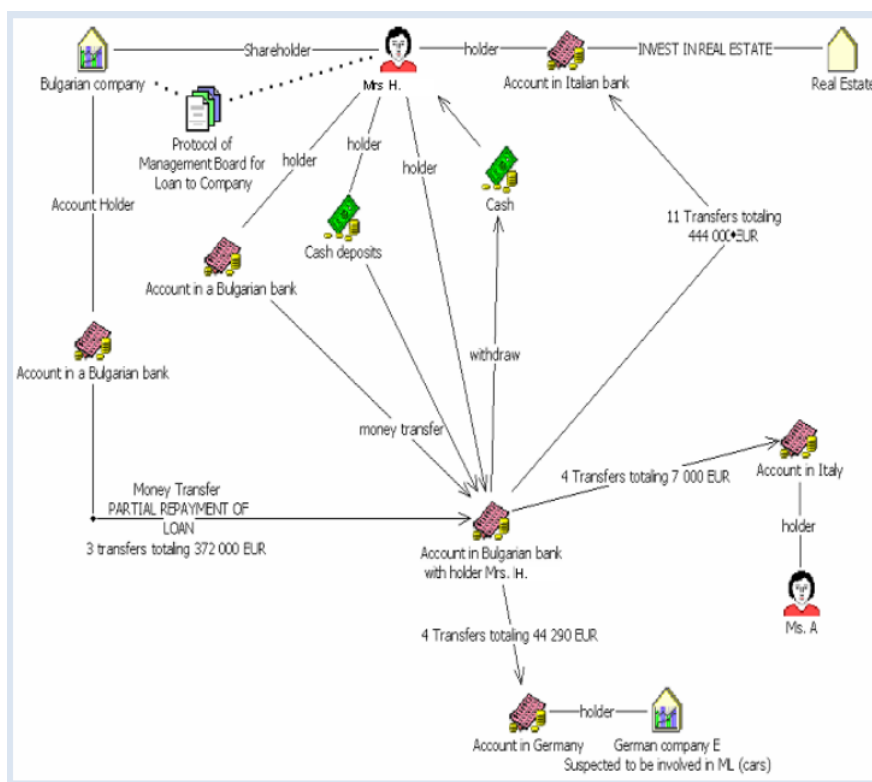
¹⁷ <http://www.austrac.gov.au/case-studies/austrac-information-revealed-extent-people-smuggling-operation>

Indicators arising from the investigation included:

- cash withdrawals conducted over multiple days
- customer undertaking transactions that appear inconsistent with their profile and/or transaction history
- multiple electronic transfers from third parties
- multiple international funds transfers to a country of interest to authorities
- multiple low-value international value transfers
- unusually large volume of cash deposits and withdrawals

Example 3 – Bulgaria¹⁸

Mr K, the leader of an organised crime group (later killed in Amsterdam) and Mr H, (an associate also deceased) managed human trafficking on behalf of the organised crime group supplying prostitutes to Italy. Also identified was the smuggling of counterfeit goods and counterfeit documents, supplying a large network of brothels and striptease clubs in Bulgaria and the involvement of relatives in money laundering operations (wife, stepmother, brother, others).



The Bulgarian FIU received four STRs highlighting the activities taking place:

¹⁸ Page 32, <http://www.fatf-gafi.org/media/fatf/documents/reports/Trafficking%20in%20Human%20Beings%20and%20Smuggling%20of%20Migrants.pdf>

- STR 1 – cash courier
 - Mr A participates in two of the companies owned by Mrs H.
 - Mr A imported and declared EUR200,000, origin unknown. He travels abroad regularly and usually stays some hours before going back to Bulgaria.
- STR 2 and 3 – purchase of expensive cars
 - Mr A's wife imports an expensive car from Germany. She is the partner of Mrs H in one of the companies and related to two other companies through her husband. The money used to buy the car is from unknown origin.
 - at least five relatives have also imported cars.
- STR 4 - placement of cash via third person
 - Mrs H's mother is the owner of a retail business. She opened a bank account and deposited EUR150,000 in cash in large denomination bank notes.
 - the funds were transferred to the Ministry of Agriculture and Forests under an order for changing the status of forest land into land for other purposes.
 - other deposits of large amounts in cash were found. They were suspicious because of large denomination notes.

Indicators arising from the investigation included:

- structuring via commercial entities and transfer of money using contract for loan
- loans provided by a shareholder to the related legal person and subsequent transfer back, fictitious loan
- significant share of the company's capital in no-term deposits – incommensurate financial turnover
- use of cash courier and repeated cash withdrawals
- use of straw persons
- inexplicable lifestyle compared to the client profile
- relations with persons with suspected or known criminal history

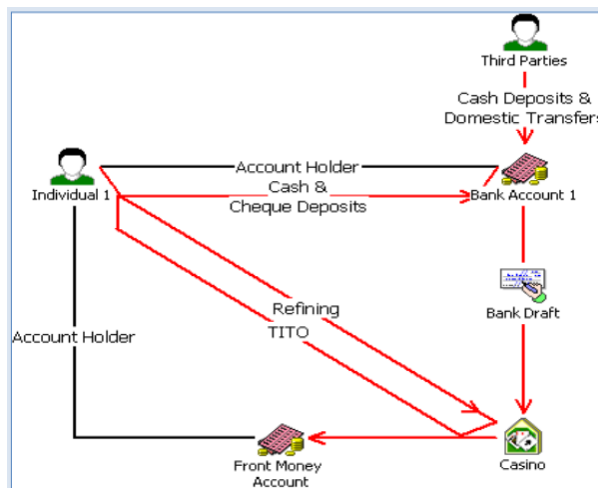
Example 4 – Canada¹⁹

The Canadian Financial Intelligence Unit (FINTRAC) received information from a Canadian law enforcement agency regarding Individual 1 who was suspected of involvement in migrant smuggling. Analysis revealed Individual 1 made several cash and cheque deposits to a personal bank account. The financial institution also reported that the account received a large number of cash deposits from third parties from across the country, as well as domestic wire transfers. Immediately following the deposits to the personal account, Individual 1 purchased bank drafts payable to a casino. The financial institution also reported that it suspected that Individual 1 used an alias to open another account at their institution.

Reporting from the casino provided insight into suspected money laundering activity. According to the casino, Individual 1 engaged in refining activity, converting large amounts of small denomination bills (USD 20s) to large denomination bills. Funds were often deposited to the front money account of Individual 1. Individual 1 purchased a large amount of casino chips, and on at least a few instances, the casino reported that the gaming of Individual 1 did not reflect the payouts being requested.

The casino also reported that Individual 1 used the casino's Ticket in Ticket out (TITO) service. The TITO service is a type of voucher system for casino slot machines designed to replace coins or tokens. Traditionally, slot machine jackpots were paid out by coins or tokens falling into the slot tray, which patrons would collect in buckets. TITO replaces these coins or tokens with a slip of paper, or ticket, with a unique bar code. The ticket can be fed into other slot machines to continue play, scanned at cashier stations for a cheque or cash, or redeemed at an automated redemption machine.

The problem with the TITO service is that it is difficult for casinos to monitor the behaviour of customers using the service; it is also not possible to verify the identity of customers using the service in combination with an automated redemption machine.



Considering all of the available information, FINTRAC suspected that Individual 1 used financial institutions and casinos to launder the proceeds of migrant smuggling activity. Specifically, FINTRAC suspects that the financial institution account was used primarily to deposit cheques from other

¹⁹ Page 36, <http://www.fatf-gafi.org/media/fatf/documents/reports/Trafficking%20in%20Human%20Beings%20and%20Smuggling%20of%20Migrants.pdf>

individuals, as well as to allow third parties to deposit cash or provide domestic wires. Following these, deposits bank drafts payable to a casino were purchased. Individual 1 also made cash deposits at the financial institution, however the bulk of cash transactions of Individual 1 appear to have been undertaken at the casino. Based on reporting from the casino, FINTRAC suspects that Individual 1 used the casino to refine any small denomination bills to large denomination bills. Individual 1 purchased casino chips, and following minimal gaming, would redeem them – either immediately requesting a casino cheque, or depositing the proceeds into the front money account. The TITO machines may have been used in the same way, and for refining.

Indicators arising from the investigation included:

- large number of cash deposits from third parties across the country
- purchase of bank drafts payable to a casino immediately after the deposits
- use of the TITO machine in the casino while minimal gaming is observed

Example 4 – New Zealand

In 2016, a jury in the High Court at Auckland found 46-year-old Faroz Ali guilty of 15 counts of trafficking Fijians to New Zealand on false promises of NZD900 weekly wages for fruit picking. He charged the workers exorbitant fees and then exploited them upon arrival by forcing them to work illegally and live in overcrowded conditions, underpaying them and threatening them with deportation if they complained. Ali was also found guilty on 16 counts of aiding and abetting people to enter or remain in the country unlawfully. He earlier pleaded guilty to charges of exploitation, including failing to pay workers minimum wage or holiday pay, as well as aiding and abetting workers to breach the conditions of their visas.

MANAGING ONGOING RISK

From the financial crime perspective, preventing money laundering through the various means possible is paramount to preventing financial gain and further investment in the practices and processes which allow exploitation of people.

In New Zealand, cross sector focus remains on preventing human trafficking becoming a problem. While New Zealand's geographical circumstances provide a barrier to both human trafficking and people smuggling, New Zealand is not immune from situations leading on from these activities. In a recent case – Operation Masala²⁰ – labour exploitation was identified by an investigation initiated by New Zealand IRD which demonstrated the value in financial monitoring.

In practice, it can be difficult to distinguish between people smuggling and human trafficking. With both crimes, criminal networks profit from a business involving the recruitment, harbouring and

²⁰ Initiated by New Zealand Inland Revenue Department (IRD), following eight years of auditing the Masala restaurant chain. IRD's investigation revealed large-scale tax evasion, evasion from personal income tax, company income tax, PAYE and GST. In December 2015, 33 properties, with the combined value of approximately NZD34 million was restrained under Criminal Proceeds (Recovery) Act 2009.

transportation of human beings. The life of a smuggled migrant can be endangered and/ or they can become a victim of other crimes in the course of being smuggled. This extensive process of multiple and specific practices requires a correspondingly wide ranging preventative approach using multi-disciplinary teams and international cooperation.

In looking for specific indicators of money laundering associated with human trafficking and people smuggling, it is vital to consider contextual factors that, although not indicators on their own, provide insight into how businesses are targeted by criminals to launder funds that have been generated by exploiting victims. This includes looking at the modelling of financial flows, the collection and analysis of relevant data, finding weak points in the business, and the disruption of financial flows.

Since human trafficking and people smuggling rely on a business or 'commercial methodology', investigations need to include a parallel and complementary financial investigation.

With the continuing growth of professionals in the financial industry, together with advocates for human trafficking victims, institution and technology-based rules and typologies for transaction monitoring systems which seek to capture specific patterns and behaviours are on the increase. Looking for 'ring activity' is now facilitating terrorist financing, drug rings and human trafficking rings to be more easily identified.

Financial institutions are in a unique position to spot red flags in [transaction] activity and report them to law enforcement. However, professionals need to understand the problem first. Other than filing suspicious transaction reports, compliance professionals should periodically review accounts, and remain aware of current human trafficking indicators. This can mean training cashiers to be on the lookout for a number of warning signs that may indicate human trafficking for sexual or labour exploitation.

RED FLAGS

A FATF report titled 'Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants'²¹ published in 2011 provides a list of red flag indicators to assist financial institutions in detecting money laundering originating from activities associated with human trafficking and people smuggling. While many of these red flag indicators are generic across other typologies²² a number of non-generic and specific indicators that were identified, include:

Banks

- a common mobile number, address and employment references are used to open multiple accounts in different names
- frequent money transfer to 'risk' countries
- concentration of 'risk' nationalities among the opening of accounts
- money rapidly withdrawn from accounts, from one ATM, or several ATMs in close proximity

²¹ <http://www.fatf-gafi.org/media/fatf/documents/reports/Trafficking%20in%20Human%20Beings%20and%20Smuggling%20of%20Migrants.pdf>

²² A full list of red flag indicators identified from the questionnaires and case studies is annexed in the published FATF Report

- frequent deposits or withdrawals with no apparent business source
- third party cash deposits are made at various bank branches and via ATMs
- transactions undertaken that appear inconsistent with customer profile
- unusual withdrawals, deposits or wire activity inconsistent with normal business practices, or dramatic and unexplained change in account activity
- numerous incoming money transfers or personal cheques deposited into business accounts for no apparent legitimate purpose

Money Service Businesses

- small amounts sent to different recipients
- small amounts sent with high frequency to unconnected persons
- frequent transfers to 'risk' countries
- multiple customers conducting international funds transfers to the same overseas beneficiary

Dealers in High Value Goods

- transactions funded with cash
- goods purchased for personal export to 'risk' jurisdictions

Casinos

- purchase of casino chips which may be redeemed following minimum gaming
- refining activity (exchanging small denomination bills into large denomination bills)
- currency exchange
- deposit of cash in bank drafts for casino front money account

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