

Financial Intelligence Unit

New Zealand Police

Quarterly Typology Report

Second Quarter (Q2)

2015/2016

(Issued March 2016)

INTRODUCTION

This report is the second 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

¹Section 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

²Section 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 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 updates

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

FIU QUARTERLY STATISTICS

Suspicious transaction reports (STRs)

The number of reported STRs processed by the FIU in Q2 2015-16 was 2,125. This total is slightly higher than the total in Q1, but is 567 reports fewer than during the same Q2 last financial year.

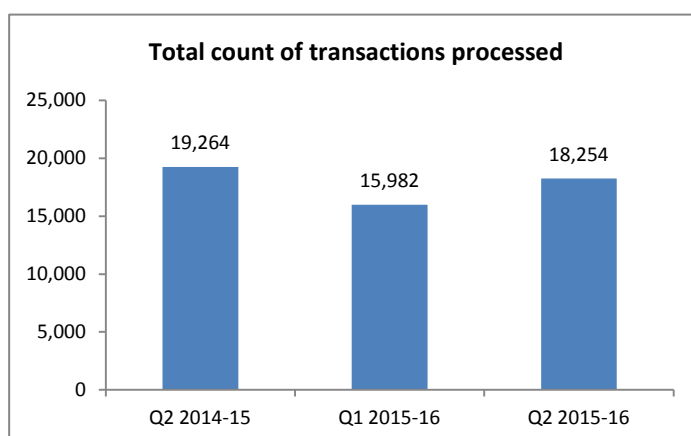
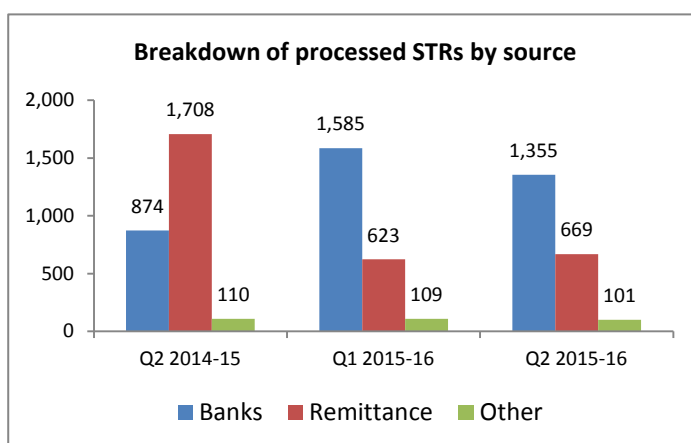
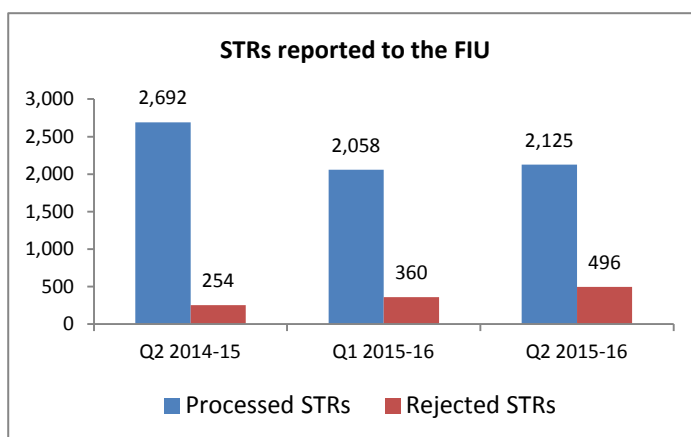
The number of rejected STRs went also up in Q2 2015-16 to 496 from 360 in previous quarter. The increase in rejections resulted from new requirements following the goAML upgrade changes which took place in December 2015. Rejection rates have subsequently declined.

The majority of STRs are submitted by banks and remittance service providers. The breakdown of the processed reports indicates that while total reports has declined, two divergent trends have occurred in the two main sectors. Over the past year, the FIU has observed a gradual increase in banks' reporting and a significant decrease in STRs from the remittance sector.

The banks' reporting has increased from 874 in Q2 2014-15 to 1,355 in the same quarter this year. Conversely, the number of processed STRs received from money remitters reduced from 1,708 to 669.

Both trends have been driven by continued improvement of transaction reporting processes by reporting entities which have led to fewer, but higher quality STRs as the AML/CFT regime has matured.

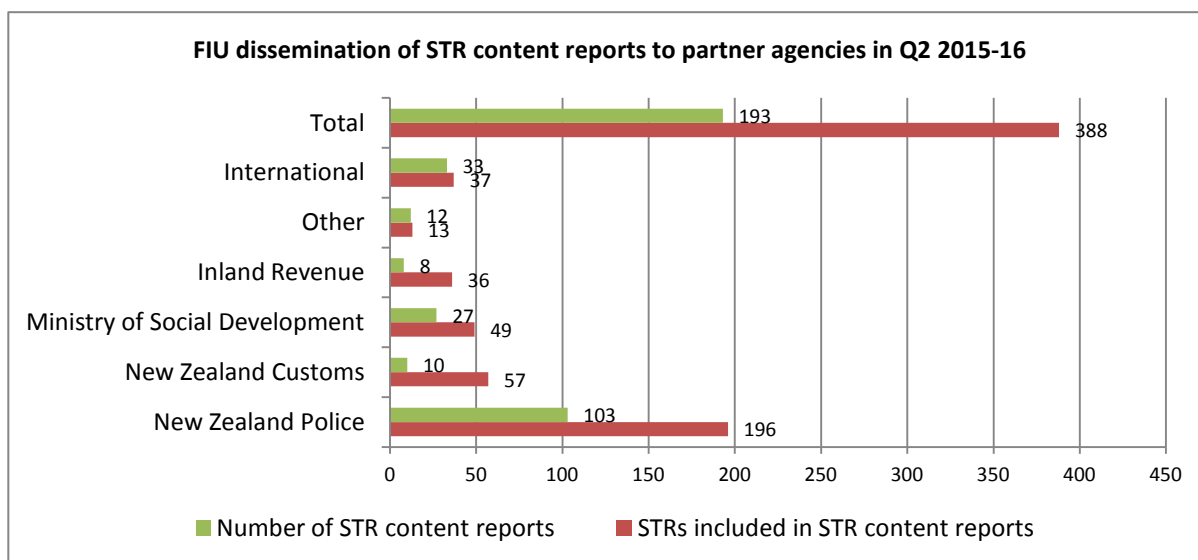
The number of transactions in accepted STRs has increased to 18,254 in Q2 this quarter, although this is 1,000 less than in Q2 2014-15.



STR content reports

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.

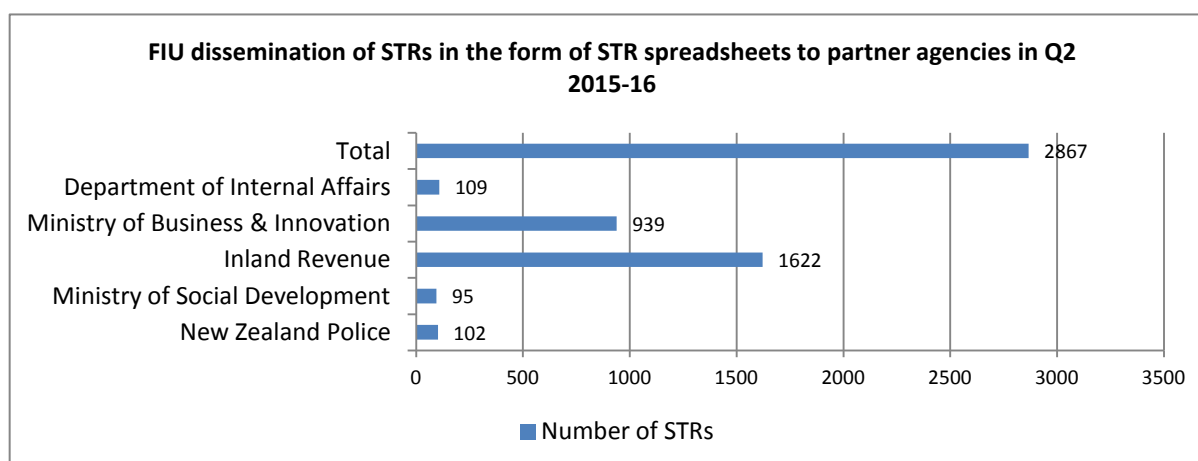
An STR content report is a basic intelligence product that comprises of the reporting entities grounds for suspicion, the reported transactions and biodata. Often the FIU will add additional value to the STR content report by including information held in Police intelligence systems. These STR content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



In the second quarter of the current financial year, the FIU disseminated a total of 193 STR contents reports, half of which were sent to various New Zealand Police units. The other recipients included domestic and international law enforcement agencies. There were a total of 388 STRs included in these STR content reports for this quarter.

STR spreadsheets

An STR spreadsheet is a collection document 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.

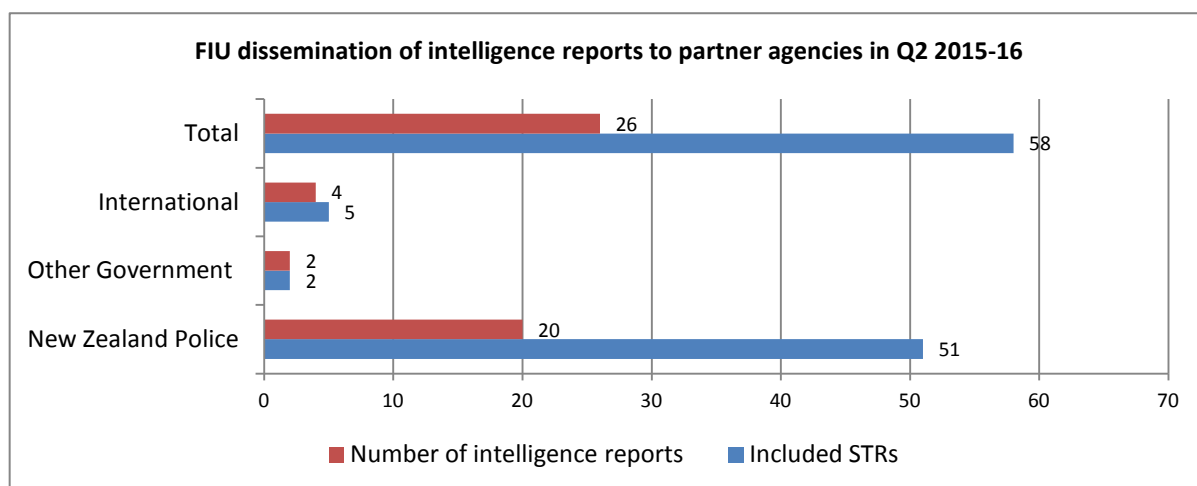


The FIU distributed 18 STR spreadsheets in Q2 2015-16 to six partner agencies, which included raw data of a total of 2,867 STRs.

Intelligence reports

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.

During Q2 2015-16 the FIU has produced 26 intelligence reports which contained analysis of a total of 58 STRs.



FIU UPDATES

FIU Conference 2016

The 2016 FIU-ACAMS conference will be held at Te Papa, Wellington on 14-15 September. The focus of the conference this year will be around the police-private AML/CFT partnership. The FIU is currently finalising the arrangements for the event and will be sending out information through the goAML message board in the coming weeks. Please contact the FIU at FCG.Seminar@police.govt.nz if any questions arise about the conference.

goAML 4.2 upgrade

goAML is a United Nations Office on Drugs and Crime (UNODC) developed application. The application allows rapid analysis of financial data, and secure exchange of information between the FIU, reporting entities and law enforcement and intelligence groups. goAML is the prescribed method by which reporting entities submit suspicious transaction reports to the FIU.

A major goAML upgrade to version 4.2 has been successfully implemented by UNODC at the NZ FIU in December 2015. New documentation and reference documents have been provided to reporting entities through the FIU website and goAML Message Board. Training to reporting entities is now delivered using the new version.

Organised Crime and Anti-Corruption Legislation Bill

The Organised Crime and Anti-Corruption Legislation Bill received Royal Assent in November 2015. The Bill led to 15 amendment acts, most of which are already in effect. There were three AML/CFT amendments:

- the money laundering offence has been amended to specify that intention to conceal is not a requirement of the offence. This will now comply with international obligations from the Financial Action Task Force and the United Nations Convention against Transnational Organised Crime
- the five-year imprisonment threshold has been removed from the money laundering offence, thus making it easier for Police to prosecute money laundering
- financial institutions and casinos will be required to report on all international transfers over NZD1,000 and all physical cash transactions over NZD10,000 to the FIU

The commencement date for these changes is 1 July 2017.

2015 APG Typologies Workshop

The FIU attended the 2015 APG Typologies and Capacity Building Workshop which was held in Kathmandu, Nepal from 16 to 20 November 2015. The workshop involved approximately 230 delegates from 38 jurisdictions and ten international organisations, including the FATF and United Nations, as well as 39 representatives from the private sector. In addition to the plenary discussions there were three parallel breakout sessions: (1) assessing regional developments with terrorist financing, (2) securing a financial intelligence unit, and (3) wildlife crime financial flows.

The FIU participated in the first breakout session the aim of which was to share regional experiences and considering opportunities to deepen international cooperation in assessing and responding to terrorist financing risks. The terrorist financing breakout session also aimed to complement and feed into the FATF's work by sharing regional experience and considering opportunities to deepen international cooperation to assess and respond to terrorist financing risks.

Counter-Terrorism Financing Summit 2015

In November, the first counter-terrorism financing summit in our region in Sydney was co-hosted by the financial intelligence units of Australia and Indonesia: the Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Pusat Pelaporan Dan Analisis Transaksi Keuangan Indonesian (PPATK). The summit brought together more than 150 leaders and experts in counter-terrorism financing and financial intelligence from around the world, which included the attendance of National Manager for Financial Crime Group of New Zealand Police.

Delegates to the summit also agreed to hold a Counter-Terrorism Financing Summit annually. The next summit will be hosted by Indonesia in August 2016. In addition, the first regional terrorism financing risk assessment will be prepared by Southeast Asian countries and Australia. The assessment will develop an enhanced understanding of the drivers behind terrorism financing, including ideology and the growing terrorist use of social media for funding as it affects Southeast Asia. It will help to identify, target and disrupt terrorism's centre of gravity and show where preventive measures can be strengthened.

Among other steps agreed upon was establishment of a regional framework to help involved maximise intelligence value, detect and deter terrorist attacks and share information faster.

The summit issued “The Sydney Communiqué” outlining concrete steps to be taken to combat terrorist financing worldwide with more urgency. It sought to maximise the use of financial intelligence to combat terrorism. Link to the communiqué: <http://www.austrac.gov.au/sydney-communique>

Egmont Group of Financial Intelligence Units’ Meeting

On 1 February 2016 the Egmont Group of Financial Intelligence Units was held in Monte Carlo, Monaco. Representatives of 102 FIUs, including the Head of New Zealand FIU, met to discuss the increasing actions of terrorists and terrorist organisations, and how the Egmont Group could positively respond to this increasing threat. As a result of this meeting, the participating FIUs adopted the following recommendations and initiatives:

- provide indicators of terrorist financing to industry partners to assist the identification of suspicious financial activity
- engage with domestic intelligence agencies to strive to improve the flow of terrorist financing-related information
- examine the utility of cross-border wire transfer information in the context of combating terrorist financing
- consider the reporting of couriers transporting cash or non-cash instruments across borders
- identify the need to expand the range of reporting entities subject to suspicious transaction reports reporting regime
- update the Egmont foundational documents to enable spontaneous and multilateral information exchange
- implement solutions for appropriate access to more sources of information necessary to share actionable financial intelligence to counter terrorist financing threats
- continue cooperation with the Financial Action Task Force – which sets the international AML/CTF standards – to overcome information access and sharing challenges and ensure the international standards enable effective combating of terrorist financing
- commit to improve FIU capability leveraging expertise and technology to better capitalise on data, exchange intelligence and enable cooperation

To read the communiqué from this meeting, please click here: <http://www.egmontgroup.org/news-and-events/news/2016/2/2/communique-hofiu-monaco-1-feb-2016>

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.

RESTRAINT & FORFEITURE UPDATE

At the end of December 2015:

- Forfeiture orders for assets worth an estimated NZD84.8 million were in place (see key terms below)
- Restraining orders were in place over assets worth an estimated NZD262.7 million pending further investigation and court action (see key terms below)

ASSETS INVESTIGATED

Since the CPRA came into effect, the ARUs have investigated 3,045 assets worth an estimated NZD475.5 million. These assets include:

- 564 residential properties worth an estimated NZD273 million
- 1,124 cash sums/bank accounts worth NZD78 million
- 71 farms/orchards/lifestyle blocks worth an estimated NZD49 million
- 20 commercial properties worth an estimated NZD20 million

Key terms

Investigated assets: These are... "assets that have been investigated since the Criminal Proceeds (Recovery) Act 2009 came into effect on December 1st 2009". Figures reported in this category include subsequently abandoned cases and should not be confused with **restrained** assets.

Restrained assets: These are... "assets that have been taken from the control of alleged offenders and placed in the hands of the Official Assignee whilst further investigations take place".

Forfeited assets: These are... "assets that, following their initial restraint, have been forfeited to the Crown". The NZD value of these orders does not represent the sum that will be returned to government accounts. Forfeiture orders are subject to appeals and costs and third party interests must be paid out of the asset value.

Profit forfeiture order: This is an order made as a result of civil proceedings instituted by the Crown against a person in order to recover a debt due to it. The maximum recoverable amount, which is determined by calculating the value of any benefit received by criminal offending minus the value of any assets forfeited to the crime, is recovered by the Official Assignee on behalf of the Crown.

Terrorist financing

WHAT IS TERRORIST FINANCING?

Terrorist financing is the process by which terrorists fund their operations in order to perform terrorist acts. Terrorists need financial support to carry out their activities and to achieve their goals. The definition set by the United Nations in the International Convention for the Suppression of the Financing of Terrorism³, states that a person commits the crime of financing of terrorism "if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an offense within the scope of the Convention.

In New Zealand the Convention is implemented by criminalising terrorist financing under the Terrorism Suppression Act 2002. Pursuant to 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

While money laundering is the process of concealing the illicit origin of proceeds of crimes, terrorist financing is the collection or the provision of funds for terrorist purposes. In the case of money laundering, the funds are always of illicit origin, whereas in the case of terrorist financing, funds can stem from both legal and illicit sources. The primary goal of individuals or entities involved in the financing of terrorism is, therefore, not necessarily to conceal the sources of the money but to conceal both the funding activity and the nature of the funded activity.

FINANCING OF TERRORISM IN NEW ZEALAND

New Zealand is known as being as a country with a very benign terrorist threat environment. The current threat level remains below New Zealand's partner countries. However, while the domestic threat of terrorism is low, New Zealand is still exposed to two categories of threats relating to financing of terrorism overseas:

- financiers of overseas groups within New Zealand
- overseas-based groups who may seek to use New Zealand as a conduit for funds

Overseas-based groups may seek to exploit New Zealand as a source or conduit for funds to capitalise on New Zealand's reputation as being low risk for terrorist funding. Funds originating in, or passing through New Zealand may be less likely to attract suspicion internationally.

Terrorist financing is most likely to occur in New Zealand as a form of international illicit capital flows. Although New Zealand's limited experience may make specific activity to target the terrorist financing threat difficult, AML activity to counter transnational laundering is likely to mitigate the deficiencies of specific counter measures for terrorist financing, provided counter measures are flexible enough to counter both threats.

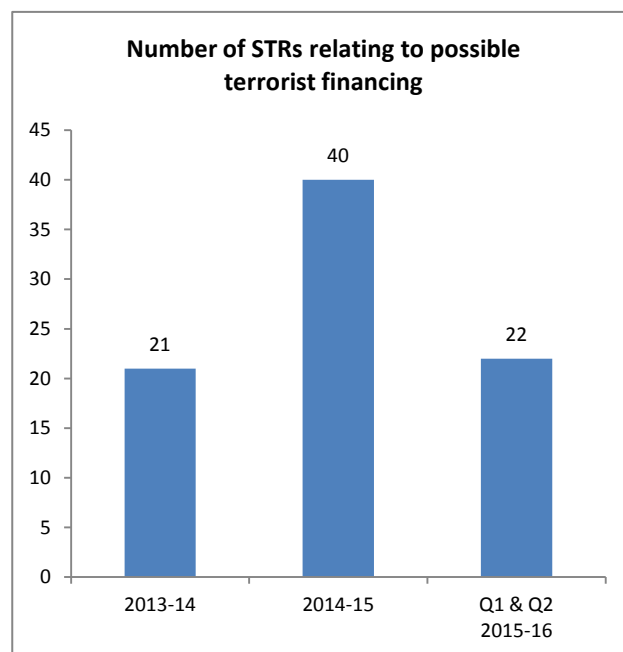
³ <http://www.un.org/law/cod/finterr.htm>

Suspicious transaction reporting on financing terrorism

For the period from the commencement of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 on 30 June 2013 to 31 December 2015 the FIU received a total of 83 STRs that have indication of possible relation to terrorist financing, which is 0.316% of all processed STRs.

The total number for each financial year includes suspicious transaction reports that were assessed by reporting entities as relating to possible terrorist financing, as well as those suspicious transaction reports assessed by the FIU as relating to possible terrorist financing to date.

The STR statistics suggest that there has been a slight increase in STRs related to possible terrorist financing. The increase in STRs – those reported by financial institutions and identified by the FIU – is a reflection of the recent acts of terrorism around the world, which have increased awareness and alertness of terrorism generally, as well as FIU's targeted training and guidance provided to the New Zealand financial institutions on indicators of terrorist financing.

**TRADITIONAL TERRORIST FINANCING METHODS AND TECHNIQUES**

FATF and members of its global network have undertaken a focused research on terrorist financing methods and risks⁴ which has shown that terrorist organisations rely on numerous sources of income and that they use a range of methods to move funds, often internationally, to their end point without being detected. Reports used for this research make it clear that terrorist organisations raise funds through inherently criminal means (i.e. narcotics, arms, human trafficking, wildlife, minerals, antiques and art) and through legitimate activities (i.e. collection of donations, cash deposits, wire transfers).

*Income generation*Donations

One financing stream used by terrorist organisations is donations from supporters in countries around the world and those donations can come from a wide-variety of sources. An analysis of terrorist financing-related law enforcement cases and prosecutions in the United States since 2001 found that approximately 33% of these cases involved direct financial support from individuals to terrorist networks⁵. Once raised, donations are passed to a network of facilitators who move the money to terrorist groups without detection. They do this by making a series of small transfers at money transfer shops, small enough to not need identification documents, or by using cash couriers who take the funds across borders.

Non-profit organisations

The FATF research also found that non-profit organisations (NPOs) can be abused and misused for terrorist financing purposes. The NPOs at most risk of terrorist abuse are those engaged in “service” activities which are operating in close proximity to an active terrorist threat⁶. NPOs that send funds to counterpart or “correspondent” NPOs located in or close

⁴ FATF report “Emerging Terrorist Financing Risks”, October 2015

⁵ US Department of Treasury (2015), United States National Terrorist financing risk assessment, US Department of Treasury, Washington, United States, www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

⁶ FATF report “Risk of terrorist abuse in non-profit organisations”, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html

to where terrorists operate are vulnerable to exploitation. Unless proper due diligence is done on the counterpart NPO with sound auditing of how donated money is used, control over the use of donations can be weak and at risk of diversion to terrorist organisations.

According to Australian contribution to the FATF research, charities and NPOs which operate in crises and war zones are at increased risk of being infiltrated and exploited by terrorist groups in these areas. Australia has also advised that funds sent to Syria and neighbouring countries for humanitarian aid are at increased risk of being used for financing terrorism if they are sent through less-established or start-up charities and NPOs that do not have proper due diligence measures/controls in place, according to the cases identified by Australia⁷.

Some obvious red flags for NPOs involvement in terrorist financing may include: the use of funds is not consistent with the organisation's purpose; transactions with no link between the stated activity and the recipient; and, frequent deposits to or withdrawals by individuals with any apparent relationships.

In New Zealand, the Charities Services and FIU have identified a few instances where they have grounds to suspect possible terrorist financing activity through NPOs. One case previously reported in the media related to alleged funding links to Hamas and al-Qaida. In addition it raised red flags as the NPO involved is essentially an overseas entity which had created New Zealand links to satisfy legislative requirements. The NPO registered as a New Zealand registered company and engaged a new Zealand law firm to establish New Zealand addresses for its charity. It satisfied the Charities Act 2005 and has been registered but has now been placed on the Charities Services' monitoring list. Other cases relate to unproven allegations of radicalising, terrorist financing and money laundering in a couple of New Zealand-based charities. None of these Charities Services' cases had reasonable grounds to be progressed to investigations into suspected terrorist financing as yet. In all cases of suspected radicalising and/or terrorist financing the relevant New Zealand law enforcement agencies have been notified.

Financial activity through high risk jurisdictions

Proceeds of various criminal activities are known to be a source for terrorist funding. In the Australasia region reports⁸ have indicated that some terrorist financing has occurred via professional money laundering through high risk jurisdictions.

The following are some of the globally observed indicators that might point to possible terrorist financing: funds are sent or received from high risk countries; recipients or senders are nationals of countries known to support terrorist activity; foreign currency exchanges that are followed within a short time by wire transfers to high jurisdiction countries; establishment of companies by nationals of terrorism-prone countries followed by international transactional activity within these accounts; and, countries involved are FATF non-cooperative countries and territories.

Fraud

Fraud appears to be another way used to generate funds for terrorism. A Spanish case study was used in the FATF report where insurance fraud was detected to simulate traffic accidents. Since 2007, members of this plot committed several sporadic frauds to obtain benefits without raising suspicion, such as faking traffic accidents and hiring bogus policies. Compensations provided by insurance companies were quickly withdrawn in cash. An increase in the number of frauds was observed in 2012, and a chronological overlap was established between the most obvious cases of fraud (involving members of a terrorist cell) and terrorists sent to join terrorist organisations like Movement for Unity and Jihad in West Africa (MUJWA or MUJAO) and ISIL. It was clear that the individuals needed to obtain funds quickly, because they disregarded the need to keep their operations secret by faking numerous and rough traffic accidents which exposed them to detection.

Although this type of fraud is known to have occurred in New Zealand, it cannot be linked to financing terrorism.

⁷ AUSTRAC report "Terrorism financing in Australia 2014", Commonwealth of Australia, West Chatswood, Australia, 2014, www.austrac.gov.au/sites/default/files/documents/terrorism-financing-in-australia-2014.pdf

⁸ <http://www.smh.com.au/national/terrorists-taking-cut-of-millions-in-drug-money-20140122-3196s.html>

Scamming banks

One way terrorists can get funds is by scamming banks. Fraudulent loan applications provide a key source of funds for jihadists wanting to travel to the conflict zone to join the groups, funding their journey. One media report on the Paris terrorist attacks in November 2015 noted that one future jihadist was able to get a loan of EUR15,000 from ING Bank in Belgium⁹ with very few questions asked.

Also, a married couple who killed 14 people in a California shooting rampage in December 2015, which the United States' FBI is investigating as an act of terrorism, had borrowed about USD28,000 from an online lender, it was deposited into their bank account about two weeks before the attack¹⁰.

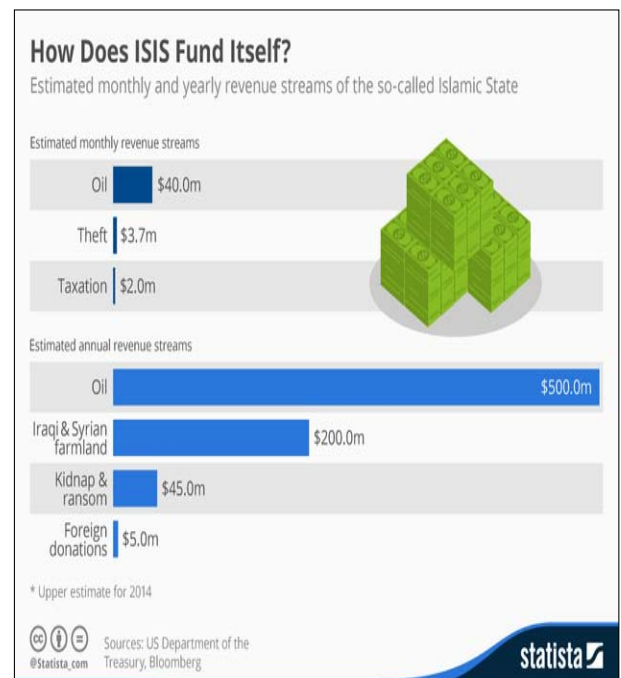
The UK National Risk Assessment of money laundering and terrorist financing¹¹ published in October 2015, states that the use of the banking sector by terrorists remains a threat in the UK, in particular in the context of Syria. Individuals can use cash machines/ATMs to withdraw funds in neighbouring countries where there is a formal banking sector and then carry funds into Syria.

Kidnapping for ransom

Kidnapping for ransom is a growing source of revenue for terrorist groups, including ISIL¹². In their report FATF states that while there is no standard template for kidnapping for ransom, specific groups which have been listed by the United Nations and other entities have engaged in kidnapping for ransom. This includes but is not limited to: The Organisation of Al-Qaida in the Islamic Maghreb (AQIM), Abu Sayyaf Group (ASG), Al Qaeda in the Arabian Peninsula (AQAP), ISIL, Harakat-ul-Ansar (HUA), as well as several terrorist groups in Pakistan.

Cash often plays a significant role in kidnapping for ransom. Following the delivery of a ransom payment in physical cash, cash couriers move the cash to the terrorist group. Ransom payments can also be paid through financial institutions, such as banks, exchange houses, insurance companies, lawyers, or alternative remittance systems such as hawalas. Kidnapping for ransom is particularly relevant to New Zealand as a kidnapping can occur in one jurisdiction and the ransom payment be made in another. There have also been examples of funds which have been raised by relatives (on behalf of the victim), through the sale of assets and loans, and through the use of trusts to store the donation for a ransom payment.

The US Department of the Treasury estimates that the so-called Islamic State raised an estimated USD45 million in 2014 through ransoming hostages. Britain, the United States as well as New Zealand have a strict policy of not paying ransoms to terrorist groups, but individuals may still be compelled to pay ransoms for associates in conflict zones. The estimated monthly and yearly revenue streams of the so-called Islamic State are shown in the chart¹³.



⁹ "How the Paris Attackers Honed Their Assault Through Trial and Error", source http://www.nytimes.com/2015/12/01/world/europe/how-the-paris-attackers-honed-their-assault-through-trial-and-error.html?_r=0

¹⁰ <http://www.reuters.com/article/us-california-shooting-account-idUSKBN0TR27P20151209>

¹¹ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf

¹² FATF report "Organised Maritime Piracy and Related Kidnapping for Ransom", FATF, Paris, 2011, www.fatf-gafi.org/publications/methodsandtrends/documents/organisedmaritimepiracyandrelatedkidnappingforransom.html

¹³ <https://www.statista.com/chart/4106/how-does-isis-fund-itself/>

Legitimate commercial enterprise

Several law enforcement investigations and prosecutions have found a nexus between a commercial enterprise, including used car dealerships and restaurant franchises, and terrorist organisations, where revenue from the commercial enterprise was being routed to support a terrorist organisation. The shipment of cars to the Middle East is considered as another fund raising scheme for a particular terrorist organisation. According to an Eastern and Southern Africa Anti-Money Laundering Group member, used car dealerships imported cars from countries such as the United Kingdom, Japan and Singapore and generated revenue from the sale of these cars as part of a complex money laundering scheme, which was then funnelled to terrorist groups. The owners of those car dealerships were from areas with a high risk of terrorism.

New Zealand FIU has seen reports relating to suspicious used car dealerships but no links to financing terrorism were alleged or found.

Some of the common red flags include: no business rationale or economic justification for transactional activity; large cash withdrawals made from a business account; unusual activity that is inconsistent with the payment policy; and, unusually complex business structures and payment patterns.

Movement of funds

Funds transfers through banks

Funds transfers through banks continue to be the most common, reliable and efficient way to move money internationally, and the banking sector remains vulnerable to terrorist financing. Several FATF reports have referred specially to the use of the bank accounts of NPOs to move funds to terrorist organisations¹⁴.

According to Australia's input to the FATF research, terrorist financing through the banking sector is often small-scale and can be difficult to distinguish from the large number of legitimate financial transactions undertaken each day. Some cases have involved structured deposits of cash into bank accounts followed by international funds transfers out of Australia. More complex methods have used accounts of both legitimate and shell business with an international presence as fronts for sending funds offshore through mainstream financial channels¹⁵. For example, sympathisers of a terrorist group can open savings accounts and provide the debit card associated with the card to a member of the terrorist organisation to enable to access cash via withdrawals from overseas bank ATMs.

Money value transfer systems

Along with the banking sector, the remittance sector has been exploited to move illicit funds and is also vulnerable to terrorist financing. FATF has identified money transfer providers as especially vulnerable to abuse for terrorist financing where they are unregulated, not subject to appropriate AML/CFT supervision or where they operate without a license¹⁶. For example, the FATF report on ISIL¹⁷ notes that a common methodology for financing foreign terrorist fighters is to send money via money remitters who have agents operating in border areas close to ISIL held territory.

Cash

Physical transportation of cash across an international border is still very common¹⁸. Cash continues to be a widespread aspect of terrorist operations, especially foreign currency, such as EUR and USD. From all the border cash reports that New Zealand FIU has received to date, none have been identified as being related to terrorist financing.

¹⁴ FATF report "Emerging Terrorist Financing Risks", October 2015

¹⁵ FATF report "Emerging Terrorist Financing Risks", October 2015

¹⁶ FATF report "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", February 2015

¹⁷ FATF report "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", February 2015

¹⁸ FATF report "Emerging Terrorist Financing Risks", October 2015

CASE STUDY FROM THE UNITED STATES OF AMERICA¹⁹

BSA data helps disrupt terrorism support network

This case out of the United States Attorney's Office for the Southern District of Florida exemplifies how the Bank Secrecy Act of 1970 (BSA, or otherwise known as the Currency and Foreign Transactions Reporting Act) data can intersect with other criminal investigative techniques to paint a full picture of terrorism material support and other threat finance crimes.

The case originated in 2008 with BSA data concerning an individual who was later convicted of conspiring to provide and providing material support to the Pakistani Taliban. The defendant funnelled money to Pakistan as Taliban insurgents fought for greater control in northwest Pakistan.

BSA data was critical in uncovering the diverse and complex methods the individual used to send money from the United States to Pakistan, each of which was designed to conceal and support his activities. Investigators uncovered at least three methods: 1) wire transfers from the United States to Pakistan, where an associate picked up and administered the funds; 2) transfers of funds from cashier's checks drawn on U.S. banks to a bank in Pakistan where co-conspirators could draw checks; and 3) bulk cash carried by family members and other travellers from the United States to Pakistan.

Suspicious activity reporting (the equivalent to New Zealand suspicious transaction reporting) narratives helped explain how funds travelled from the United States to areas of Pakistan. The timing of this case proved extremely helpful in the fight against the Pakistan Taliban as important information gleaned from BSA records proved critical in obtaining other leads. The data led to subpoenas for bank and financial records (admissible evidence), alerted investigators to the use of wire transfers, and revealed the centrality of specific bank accounts to the scheme.

This case demonstrates that AML/CFT reporting, when taken with other resources at the disposal of law enforcement, can effectively disrupt terrorism support networks and mitigate other threats to public safety.

CASE STUDY FROM AUSTRALIA²⁰

Suspects raised funds in preparation for acts of terrorism

The following two related cases were obtained from the AUSTRAC online case hub and illustrate apparently normal patterns of financial behaviour, undertaken through low-value transactions.

PART A – SYDNEY

A joint investigation led to the arrest in November 2005 of nine Sydney suspects who authorities suspected were planning an act of terrorism in conjunction with thirteen Melbourne suspects. The group's activities included military-style training and purchasing materials they planned to use to manufacture explosives.

The investigation revealed that the Sydney-based suspects relied mainly on their own incomes and efforts to fund their training activities and purchases, using their own bank accounts. Members of the group were caught shoplifting batteries, maps and electronic timers. Investigating officers also located stolen railway detonators during the execution of search warrants.

The Sydney suspects regularly used false names to register mobile phones when purchasing supplies and materials for their activities. For example, members of the group established companies in false names and used these companies to avoid suspicion when ordering and purchasing chemicals.

¹⁹ FINCEN, May 2015

²⁰ Published in AUSTRAC's Case Studies Hub online <http://www.austrac.gov.au/case-studies>

Four members of the Sydney group pleaded guilty to various terrorism offences, while the remaining five members were found guilty by a jury of conspiring to commit an act in preparation for a terrorist attack under the *Criminal Code Act 1995*.

Offence: terrorism

Customer: individual

Industry: banking

Designated service: account and deposit-taking services

Indicators: low-value payments undertaken through accounts and low-value cash withdrawals (below the AUD10,000 threshold); use of false identification to establish Australian companies

PART B – MELBOURNE

The same joint investigation also led to the arrest of thirteen Melbourne suspects who, in conjunction with the Sydney suspects, were planning an act of terrorism. The Melbourne group also undertook military-style training and purchased materials to manufacture explosives.

Investigations revealed that the Melbourne-based group funded their planned activities primarily through a series of small cash donations made by the group members to a central fund, known as the “sandoq” (traditionally a box where all financial contributions were held). The majority of the Melbourne group were employed as electricians, tilers or panel beaters.

One individual was alleged to have been the treasurer and holder of the sandoq. Another group member approved group members to use funds from the sandoq. All members contributed to the sandoq, with some contributing AUD100 per month. The fund was worth approximately AUD19,000 at the time the group was arrested.

The suspects were also engaged in systematic credit card fraud, whereby they paid taxi drivers to provide them with the credit card numbers of unsuspecting taxi passengers. In addition, third parties provided the group with extra funds raised from a car re-birthing racket.

The group undertook the fundraising activities for the purpose of purchasing weapons and materials for a planned terrorist attack.

Nine members of the Melbourne group were found guilty of being members of a terrorist organisation. Four members were acquitted. Seven group members were also found guilty of committing acts in preparation for a terrorist attack under the *Criminal Code Act 1995*.

Offence: terrorism

Customer: individual

Industry: banking

Designated service: account and deposit-taking services

Indicators: multiple individuals contributing cash to a central fund (sandoq); frequent contributions made to the sandoq by members of the group and through proceeds of business activities; individual members contributed up to AUD100 per month

FIRST CONVICTION OF TERROR FINANCING IN THE NETHERLANDS²¹

Two brothers Hatim and Suleymaan R., raised in the Netherlands, were involved in a recent conviction in the Netherlands. Hatim has been on the Dutch terrorist list since 2014 but is believed to have been in Syria since 2013. He was sentenced to six years in prison in absentia in December for terrorist activity. On 15 March 2016, a Rotterdam court found Suleymaan, the 28-year old bus driver, guilty of sending EUR17,000 to his brother, which the judge determined constituted financial support to a terrorist. His 18-month sentence marked the first conviction in the Netherlands based on a newly-sharpened law against terror financing.

CASE STUDY FROM AN OVERSEAS JURISDICTION

The New Zealand FIU received the following case study from a partner FIU.

Suspected terrorist financing

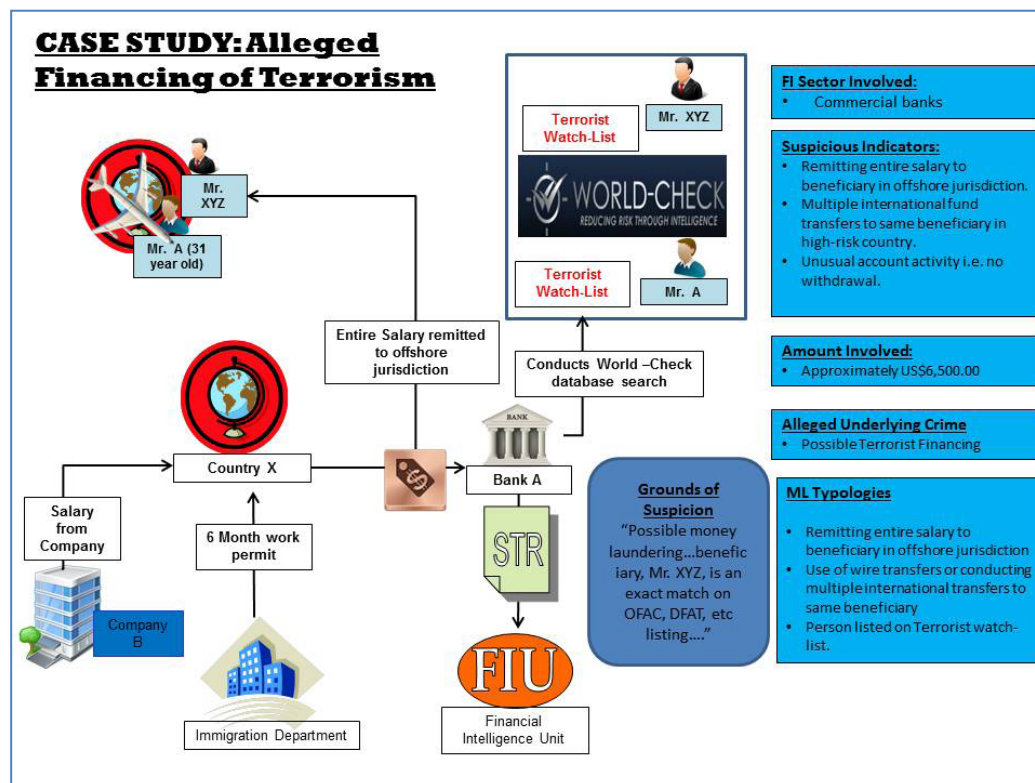
A suspicious transaction report was reported by a commercial bank on a foreign national, Mr A. He maintained a personal account at the local bank and conducted an international remittance to his home country. He was employed by Company B.

The bank established through their due diligence checks that Mr A and the beneficiary, Mr XYZ of the international remittance were reported an International Watch list as “suspected terrorists”.

The FIU checks confirmed the adverse findings by the bank and it was established that a group of foreigners with the same nationality were operating from the same address as Company B.

Possible offence: terrorist financing





Indicators: foreigners were adversely reported individuals on an International Watch list



²¹ <http://fd.nl/economie-politiek/1143505/celstraf-voor-financieren-van-broer-bij-isis-in-syrie>

WORLD'S RICHEST 10 TERRORIST ORGANISATIONS







Forbes magazine has ranked the 10 richest terrorist organisations worldwide in 2015-2016. This list aims to give an overview of the current terrorist organisations, their conflict areas and provide a rough estimate of the groups' annual turnover. For full Forbes article, please click here <http://www.forbes.com/sites/forbesinternational/2014/12/12/the-worlds-10-richest-terrorist-organizations/#922bb572ffae>

Ranking	Name	Annual turnover* ²²
1 ISIL Iraq, Syria and Jordan 	<p>ISIL is reputedly the richest terror organisation to date. Its annual turnover amounts to around USD2 billion, and some analysts estimate the number to be USD3 billion.</p> <p>Main funding sources: oil trade, kidnapping and ransom, collection of protection and taxes, bank robberies and looting.</p> <p>Goal: the establishment of an Islamic State in Iraq, Syria, Jordan, Lebanon and Palestine</p>	USD2 billion
2 HAMAS Gaza Strip and West Bank 	<p><i>Please note while the political wing of Hamas is not designated as a terrorist group by New Zealand, the military wing is.</i></p> <p>Hamas's militant coup resulted in taking over of the Gaza strip in 2007.</p> <p>Main funding sources: taxes and fees, financial aid and donations (especially Qatar).</p> <p>Purpose: militant struggle against the state of Israel and the establishment of a Palestinian Islamic state from the sea to the Jordan River</p>	USD1 billion* ²³
3 FARC Colombia 	<p>FARC, the Revolutionary Armed Forces of Colombia (Fuerzas Armadas Revolucionarias de Colombia), is an underground Marxist and anti-imperialist activist group and a key player in the bloody struggle that's ravaged Columbia for more than 50 years.</p> <p>Main funding sources: drug production and drug trafficking, kidnapping and ransom, mining of minerals (especially gold), fees and taxes.</p> <p>Purpose: elimination of the capitalist regime and the establishment of a Marxist-socialist welfare</p>	USD600 million
4 Hezbollah Lebanon 	<p><i>Please note while the political wing of Hezbollah is not designated as a terrorist group by New Zealand, the military wing is.</i></p> <p>Main sources of income: financial assistance and donations (especially Iran), production and trafficking of drugs</p> <p>Purpose: militant struggle against the state of Israel and establishing an Islamic state in Lebanon</p> <p>Established as a militant group fighting for the Shiite population in Lebanon and against Israel, Hezbollah, like Hamas, has a strong political arm, which is not designated in New Zealand, that became one of the major powers in Lebanon. Hezbollah has a network of nursing institutes, which provides relief, welfare, education and livelihood to large</p>	USD500 million* ²⁴

²² *Forbes's estimate

²³ *This figure includes both military and political wings estimates

²⁴ *This figure includes both military and political wings estimates

	segments of the Shiite population in need.	
5 Taliban Afghanistan and Pakistan 	<p>The Taliban is a militant political movement that ruled Afghanistan from 1996 to 2001 and applied the rule of Sunni Islamic Sharia law.</p> <p>Main funding sources: drug trafficking (mainly production of opium and heroin), sponsorship fees and taxes, financial assistance and donations.</p> <p>Goal: the establishment of an Islamic theocracy in Afghanistan</p>	USD400 million
6 Al-Qaeda and its affiliates Afghanistan and Pakistan 	<p>Al-Qaeda is one of the most lethal terror organisations.</p> <p>Main sources of finance: financial assistance and donations, kidnapping, ransom and drug trafficking.</p> <p>Purpose: formation of global Islamist front against opposing and secular Muslim governments and Western States</p>	USD150 million
7 Lashkar-e-Taiba Pakistan and India 	<p>Lashkar-e-Taiba, "army of the righteous" to its followers, is a Pakistani radical Islamic terror group, considered to be one of the dominant groups in Southeast Asia.</p> <p>Main sources of finance: financial assistance and donations.</p> <p>Purpose: integration of Kashmir India with Pakistani Kashmir under Islamic rule</p>	USD100 million
8 Al-Shabaab Somalia, Kenya and Uganda 	<p>Al-Shabaab is the largest militant organisation in Somalia, founded in 2006.</p> <p>Main funding sources: kidnappings and ransom, illegal trade and pirate activity, sponsorship fees and taxes</p> <p>Purpose: removal of foreign forces from Somalia and the establishment of an Islamic caliphate.</p>	USD70 million
9 Real IRA Northern Ireland, Ireland and United Kingdom 	<p>Real IRA is a radical faction of the IRA (Irish Republican Army), established by activists who oppose the peace agreement signed in April 1998. This faction is considered to be the strongest resistance organisation operating against the British, and it is defined as a terrorist organisation by the EU, the USA and New Zealand amongst others.</p> <p>Main funding sources: smuggling and illegal trade, aid and donations</p> <p>Purpose: creation of a united Irish state, which includes Northern Ireland and Ireland</p>	USD50 million
10 Boko Haram Nigeria and Cameroon 	<p>Boko Haram means "Western education is a sin". It opposes education according to western values because they believe it contradicts the Islamic faith.</p> <p>Main funding sources: kidnappings and ransom, fees and taxes, protection, bank robberies and looting</p> <p>Goal: fighting secularism and Western influences, overthrow of Christian-secularism and the establishment of Islamic law in Nigeria</p>	USD25 million

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.

TYPES - 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

TYPOLGY 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