# NEW ZEALAND POLICE

# FINANCIAL INTELLIGENCE UNIT

## SUSPICIOUS ACTIVITY REPORTING GUIDELINE

2018

# *Contents*


Foreword ..... 1
Overview ..... 2
Risk assessments and AML/CFT programmes ..... 2
Suspicious Activity Reporting is a key detection tool ..... 2
AML/CFT Programmes are intended to be preventative ..... 2
Terrorism financing is similar to, but not the same as, money laundering ..... 2
Introduction ..... 3
Background ..... 3
Purpose ..... 3
Scope ..... 3
Disclaimer ..... 4
Money laundering and terrorism financing basics ..... 5
What is money laundering? ..... 5
Definition of money laundering ..... 5
Terrorism financing and security matters ..... 6
Reporting suspicious activity about security matters ..... 6
What is a terrorist act? ..... 6
Definition of terrorism financing ..... 6
Terrorist designations ..... 7
Reporting a Suspicious Property Report under the TSA ..... 7
Suspicious Activity Reports (SARs) ..... 8
What are SARs? ..... 8
Activities to report ..... 8
The circumstances that trigger SARs ..... 8
When to report? ..... 9
Identifying suspicious activity ..... 10
Countries with insufficient AML/CFT systems ..... 11
Who should identify suspicious activity? ..... 12
Auditors ..... 12
Who must report? ..... 12
What must be reported? ..... 12
When Legal Privilege applies ..... 13
What happens after reporting? ..... 13
What is ‘tipping off’? ..... 14

How to report? 14
Oral reports 14
Follow-up to SARs 14
Feedback about SARs 15
What are Prescribed Transaction Reports? 15
Typologies 16
What are typologies? 16
Common typologies 16
Indicators and warnings 18
What are indicators and warnings? 18
General indicators 18
Industry specific indicators 22
Use and disclosure of information by the FIU 31
Investigations and prosecutions 31
International cooperation 31
Prevention and disruption 32
Protections 33
Protection of a person reporting suspicious activity 33
Immunity from liability for disclosure of information 33
Disclosure of information in judicial proceedings 33
Acting in compliance with the AML/CFT Act 33
Offences and penalties 34
Offences relating to suspicious activity reporting 34
Penalties 35

# *Foreword*

This guidance has been issued by the Financial Intelligence Unit (**FIU**) on behalf of the Commissioner of Police.

The New Zealand Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) environment is undergoing changes which affect the way we detect, analyse and report suspected money laundering, terrorism financing and other serious criminal offending.

This guidance, together with our goAML reporting instructions, aims to generate knowledge and understanding about these changes to inform internal policies, procedures and controls for the reporting of suspicious activity by reporting entities.

Offenders continually exploit services offered by reporting entities in an attempt to obscure their illicit activities and proceeds. By analysing customer behaviour, including the value, volume, and frequency of transactions, reporting entities can detect and report suspicious activity. These reports provide crucial information to assist the New Zealand Police and its partner agencies to investigate serious crime through the use of financial intelligence.

This guidance provides examples of suspicious behaviour regarded internationally as indicators of money laundering, terrorism financing, and other serious offending. While the presence of one or more indicators may not be evidence of criminal activity, it may raise suspicion. Multiple indicators should act as a warning sign that additional inquiries may need to be undertaken. In some cases obvious signs of criminality may be apparent, whereas in others making enquiries about customer activity may trigger suspicion. If suspicion exists, a Suspicious Activity Report (SAR) must be submitted to the FIU.

This guidance draws on material produced by the New Zealand FIU, domestic partner agencies, the Financial Action Task Force, and international FIUs. It should be read in conjunction with the sector risk assessments issued by the AML/CFT supervisors and the National Risk Assessment.

The FIU and New Zealand Police acknowledge the significant work already undertaken by reporting entities and the value of co-operation across the sector in achieving success. We look forward to continuing success in this new and challenging environment.

Mike Bush MNZM
Commissioner of Police

# *Overview*

## Risk assessments and AML/CFT programmes

Reporting entities' AML/CFT programmes should be based on well-informed assessments of risk. The Financial Intelligence Unit (**FIU**) and anti-money laundering and countering the financing of terrorism (**AML/CFT**) supervisors publish advice on national-level risks and on sector and industry specific risks. Reporting entities must have regard to that advice in developing their AML/CFT risk assessments and AML/CFT programmes. Reporting entities must also assess the risks of dealing with overseas jurisdictions. Much of the advice on the money laundering and terrorism financing risks for foreign jurisdictions is publicly produced by independent international bodies such as the Financial Action Task Force. Reporting entities also need to document their procedures for submitting Suspicious Activity Reports (**SARs**) in the AML/CFT programme and may wish to refer to this SAR Guideline for that purpose.

## Suspicious Activity Reporting is a key detection tool

A key purpose of an AML/CFT programme is to detect criminal activity. The FIU relies on reporting entities to detect and report suspicious activity. SARs are submitted when a reporting entity has facts and observations that objectively give reasonable grounds for suspicion. Reporting entities will need to consider the important indicators of money laundering and terrorism financing, common typologies; information on typologies and indicators are included in this SAR Guideline.

Certain information considered for inclusion in a SAR may be legally privileged and reporting entities need to make this determination prior to submission.

SAR information is analysed by the FIU and may be used for criminal investigations and national security matters. Reporting entities must not 'tip off' any person who may be the subject of a SAR. This is to keep reporting entity staff safe and to ensure that any criminal investigations or security matters are not impeded.

There are serious offences and penalties – both civil and criminal – for failure to submit SARs. However, there are also protections and immunities for reporting entities for SARs.

## AML/CFT programmes are intended to be preventative

Another key purpose for AML/CFT measures is prevention. If customer due diligence cannot be conducted adequately reporting entities are required to take preventive action. This requirement can be triggered for one-off activities or during 'on-boarding' of customers as part of an ongoing business relationship. These actions help to maintain the integrity of New Zealand's financial systems. In addition, a reporting entity may discontinue a business relationship based on their risk assessment.

## Terrorism financing is similar to, but not the same as, money laundering

Terrorism financing is a national security matter. Reporting entities must make Suspicious Property Reports (**SPRs**) under the Terrorism Suppression Act 2002 (**TSA**) to the FIU if there are reasonable grounds to suspect that the services provided are for a United Nations-sanctioned person or listed entity.

New Zealand also has domestic systems for issuing sanctions; reporting entities should be aware of Police and Ministry of Foreign Affairs advisories. Dealing with sanctioned persons or entities, weapons proliferation, terrorism and terrorism financing are all criminal offences which may give rise to money laundering and a SAR should be submitted in these situations.

# *Introduction*

This guidance has been issued to clarify the obligation to report suspicious activity under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (**AML/CFT Act**)

It aims to increase awareness on indicators of suspicious activity and inform reporting entities about the technical requirements to report suspicious transactions and activity.

## Background

Reporting entities are defined in section 5 of the AML/CFT Act. The AML/CFT Act requires reporting entities to conduct a risk assessment and establish an AML/CFT programme. The AML/CFT Programme must include adequate and effective policies, procedures and controls for preventing and detecting money laundering and terrorism financing and for reporting suspicious activity to the Financial Intelligence Unit (**FIU**). Dealers in high value goods are also included in the legislation but have lesser AML/CFT obligations.

## Purpose

This guidance has three main objectives:

1. To explain the basics of money laundering and terrorism financing;
2. To help reporting entities identify suspicious activities by providing specific typologies and indicators;
3. To help reporting entities comply with Suspicious Activity Reporting (**SAR**) obligations by specifying when reports must be made, in what circumstances, what details to include, and how to report them.

In many cases reporting entities will be unaware what the underlying criminal activity is. However, by screening transactions and activities for known indicators and typologies, a reasonable suspicion that the transaction or activity is relevant to criminal offending may arise. In these cases a SAR must be submitted to the FIU.

## Scope

The AML/CFT regime is based on effective risk management. Reporting entities need to assess the money laundering and terrorism financing risks faced by their business operations and establish appropriate mitigations and controls. However, the risks are contextual to international, national, sectoral environments, and to different customer channels and service environments, some of which are not visible to reporting entities and some of which are not visible to government agencies.

International and national-level money laundering and terrorism financing (**ML/TF**) risks are described in the National Risk Assessment (**NRA**) which is available on Police's website. At the sector level, supervisors (Department of Internal Affairs (**DIA**), Financial Markets Authority (**FMA**) and Reserve Bank of New Zealand (**RBNZ**)) produce sector-specific guidance. Sector supervisors provide reporting entities with more detail on which reporting entities attract AML/CFT obligations and the nature of those obligations.

- FIU National Risk Assessment
- RBNZ Sector Risk Assessment
- DIA Phase I Risk Assessment
- DIA Phase II Risk Assessment
- FMA Sector Guidance

Finally, reporting entities are required to have adequate and effective policies, procedures, and controls for reporting on suspicious activity. This SAR guideline document focusses

specifically on the factors visible to supervisors and the FIU that should be considered for SAR reporting. Reporting entities should consider this guidance document in developing internal policies, procedures, and controls on suspicious activity reporting. It will be amended as needed over time as ML/TF risks change.

## Disclaimer

This guidance cannot be relied on as evidence of complying with the requirements of the AML/CFT Act. It also does not constitute legal advice and cannot be relied on as such. Reporting entities will also need to remain aware of emerging risks, typologies and technologies or products that favour anonymity and will need to mitigate those risks appropriately.

# *Money laundering and terrorism financing basics*

## What is money laundering?

The aim of many criminal acts, particularly those linked to organised crime, is to generate profit. Money laundering is the processing of this profit to disguise its illegal origin. Money laundering offers criminals the ability to make the proceeds of crime appear legitimate.

There are three stages involved in money laundering. These are:

**Placement** - The introduction of illegal proceeds into the financial system (for example, the proceeds of selling cannabis deposited into a bank account).

**Layering** - The movement of funds via a series of transactions/conversions to disguise the origin of funds and obscure the audit trail.

**Integration** - The introduction of laundered funds into the legitimate economy through ordinary financial activity (for example, laundered funds are used to invest in - goods, financial or business products, or property).

Opportunities exist to identify money laundering at all three stages.

## Definition of money laundering

Money laundering is defined in section 243 of the Crimes Act 1961. The key elements of a money laundering offence are that in concealing any property or enabling any person to conceal any property, a person:

- Deals with, or assists any other person to deal with, any property that is the proceeds of an offence; and
- Knows or believes that such property is the proceeds of an offence, or is reckless as to whether it is the proceeds of an offence.

## *Terrorism financing and security matters*

Terrorism financing and money laundering both require the movement of funds, preferably for the offender, with minimal scrutiny. The controls established to detect money laundering may often be usefully applied to prevent and detect terrorism financing. Understanding key differences between the two is important. Unlike money launderers, terrorism organisations can raise funds through legitimate sources as well as criminal activity. Historically, terrorism financiers have used specific methods to add complexity or legitimacy to transactions, including the use of alternative remittance services, charitable organisations, and cash couriers.

### Reporting suspicious activity about security matters

Reporting entities are required to report SARs where the underlying offence may be relevant to the enforcement of terrorism-related offences and offences related to national security. In practice this will be *in particular* related to offences against Terrorism Suppression Act 2002 (**TSA**) section 8, the terrorism financing offence. However, note that the TSA also criminalises dealing in weapons of mass destruction, explosives and radioactive material etc and any proceeds from weapons trading may be a predicate offence to money laundering.

New Zealand's sanctions system is currently linked to the United Nations (**UN**). As a UN member, New Zealand is bound to follow the Security Council's decisions. The United Nations Act 1946 means our Government can respond quickly where necessary and impose or remove sanctions when the Security Council makes a decision. Sanctions avoidance may also be a predicate offence to money laundering or terrorism financing. Reporting entities should be aware of any Ministry of Foreign Affairs' financial and economic sanctions that may apply.

**SAR reporting for security matters**

*The FIU encourages expedited SAR reporting in circumstances related to all security matters including suspected terrorism, terrorism financing, weapons proliferation, and sanctions avoidance.*

### What is a terrorist act?

A terrorist act is defined in section 5 of the TSA and includes the following elements:

- An intention to cause significant harm to the human population, economic loss or major environmental damage (or introduce an economically destructive disease);
- Carried out to advance a political, ideological, or religious cause; and
- An intention to induce terror or 'unduly' compel or force a government or international organisation to do something.

### Definition of terrorism financing

Terrorism financing is criminalised in New Zealand in section 8 of the TSA. Under this legislation it is an offence to:

- Provide or 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; and
- Make financial services and related services available to a designated terrorist entity.

## Terrorist designations

The TSA establishes a legal framework for the suppression of terrorism. It is also the mechanism by which New Zealand gives effect to the United Nations Security Council (**UNSC**) mandatory resolutions requiring United Nations (**UN**) member states to take steps to suppress terrorism. An important feature of this framework is the Prime Minister's power under the TSA to designate individuals or groups as terrorist (or associated) entities. Designations can be made on an interim or final basis.

There are two broad lists of entities that are affected by the TSA:

1. Entities listed by the UN as terrorist entities under UNSC Resolutions 1267/1989 and the 1988 List. New Zealand is specifically obliged to take action against the terrorist entities. UN listed entities are defined as designated terrorist entities in the TSA and engage the criminal provisions of the TSA.
2. Non-UN listed entities designated under the TSA under UNSC Resolution 1373. By contrast, while UNSC Resolution 1373 obliges New Zealand to outlaw the financing of, participation in and recruitment to, terrorist entities, it does not specifically identify those entities. This Resolution effectively leaves it to Member States to identify the entities against which they should act.

A designation under the TSA, as well as freezing assets of terrorist entities, makes it a criminal offence to participate in or support the activities of the designated terrorist entity. This includes dealing with the property (including funds or value transfers) of the designated terrorist entity or making property or financial services available to the entity. Other support for terrorist activities such as fundraising, recruiting or harbouring terrorists is a criminal offence whether the group is designated or not.

## Reporting a Suspicious Property Report under the TSA

If a reporting entity deals with an individual or organisation and there are reasonable grounds for suspicion in relation to property owned or controlled by a designated terrorist entity a Suspicious Property Report (**SPR**) must be completed, as described in section 43 of the TSA. Any SPRs reported to the FIU must contain all the information specified in Schedule 5 to the TSA. In practice, reporting entities use the same online system for reporting SPRs as if for SARs.

# *Suspicious Activity Reports (SARs)*

## What are SARs?

SARs are the main source of information available to the FIU to detect suspected offences. A SAR can indicate that suspected criminal activity is occurring through a transaction, a service or series of transactions and/or services.

Reports received by the FIU are analysed for activities and patterns that may indicate criminal offending. During the analysis, various resources are used including other information collected from reporting entities under the AML/CFT Act, and intelligence received from Police, partner agencies, international counterpart agencies, as well as information obtained from open-source databases.

Often, additional information is required from reporting entities to help establish whether the suspicious activity reported in a SAR merits further investigation. This additional information can be vital in determining whether the suspicion of offending translates into actual criminal activity.

Where criminal activity appears to be occurring, cases may be referred to investigative agencies involved in law enforcement, asset recovery, taxation, and national security. Cases may also be referred to supervisors or regulators in certain circumstances (for example, if it may help to prevent further criminal activity, a suspected 'shell company' may be referred to the Companies Office).

## Activities to report

Section 39A of the AML/CFT Act outlines that a reporting entity must report any suspicious activity where:

- a person conducts or seeks to conduct an activity or transaction through a reporting entity; or
- a reporting entity provides or proposes to provide a service to a person; or
- a person requests a reporting entity to provide a service or makes an inquiry to the reporting entity in relation to a service.

**Obligation to report suspicious activity**

*The requirement to report SARs applies to transaction, proposed transaction, service or proposed service, and inquiries. Note there are no monetary thresholds for SARs.*

## The circumstances that trigger SARs

Reporting entities must make a SAR where they have reasonable grounds to suspect that a transaction, proposed transaction, service or proposed service, or the inquiry is or may be relevant to:

- the investigation or prosecution of any person for a money laundering offence; or
- the enforcement of the Misuse of Drugs Act 1975; or
- the enforcement of the Terrorism Suppression Act 2002; or
- the enforcement of the Proceeds of Crime Act 1991 or the Criminal Proceeds (Recovery) Act 2009; or
- the investigation or prosecution of an offence (within the meaning of section 243(1) of the Crimes Act 1961). In this case an offence means an offence (or any offence

described as a crime) that is punishable under New Zealand law, including any act, wherever committed, that would be an offence in New Zealand if committed in New Zealand.

**Reasonable grounds to suspect**

*Suspicious Activity Reporting is based on an objective test. "Where an objective observer would conclude that reasonable grounds for suspicion were known to the reporting entity, it is no defence that the reporting entity did not actually consider the transaction to be suspicious."[1] The test for a SAR is not a subjective test; if a person in your circumstances should have inferred knowledge or formed a suspicion, then a report must be submitted.*

**Predicate offences to money laundering**

*A wide range of profit-motivated offences can give rise to money laundering or terrorism financing. Tax offending, fraud and drug offending are common offences that give rise to money laundering in New Zealand; others may include offending related to national security, weapons proliferation, organised crime groups, immigration and labour fraud, trade and invoice fraud, environmental and conservation crimes, sanctions avoidance, corruption, cybercrime, insider trading and securities fraud, identity theft, pharmaceuticals fraud etc. Importantly, reporting obligations may apply even if the underlying offending occurred overseas.*

*Reporting entities are not expected to know which type of offence underlies any money laundering – especially if it is suspected that any underlying offending is offshore. Rather, the grounds for suspicion should attach to the ML/TF indicators and common ML/TF typologies. However, providing a full description of the reasons for suspicion may assist the FIU to analyse the possible types of offending.*

The AML/CFT Act contains preventative measures as well as detection measures. If adequate customer due diligence cannot be conducted reporting entities must take preventative action by discontinuing the relationship or activity. This can occur when a reporting entity first engages with a customer or during ongoing account monitoring. The reporting entity must also consider whether to make a SAR. The decision to submit a SAR in these circumstances must still meet the same reasonable grounds for suspicion test.

## When to report?

Once reasonable grounds for suspicion exist, a reporting entity must submit a SAR to the FIU as soon as practicable, but no later than three working days.

In practice, we expect that reporting entities will need to conduct enquiries to gather information to establish reasonable ground for suspicion once an unusual event occurs or is flagged by account monitoring. It is likely rare that a single piece of information on its own would meet the threshold of reasonable grounds for suspicion. In most situations we expect a SAR would be filed within three days of the reporting entity gathering sufficient verifying information for reasonable grounds to crystallise suspicion, rather than three days from an initial event.

Reporting entities need to be mindful of the rare circumstance where a single event forms reasonable grounds for suspicion. Situations such as these usually involve an interaction with

[1] Department of Internal Affairs v Ping An Finance (Group) New Zealand Co Ltd [2017] NZHC 2363 at [64] [28 September 2017]

a customer where cash has physical characteristics that are suspicious in and of themselves. An example is cash that smells of cannabis. In these situations additional account monitoring or investigation will not negate the grounds for suspicion. Reporting entities need to ensure that they assess and report such matters within three days of the reporting entity becoming aware of objectively suspicious circumstances.

When deciding whether a matter needs to be reported, reporting entities must ensure reasonable grounds for suspicion exist. It is important reporting entities do not engage in defensive reporting as this practice is not in line with the intentions of the Act, and may lead to the reporting entity breaching other obligations.

**Grounds for suspicion formed by observation and account monitoring**

*Mr A was a member of a casino's loyalty programme and an occasional visitor to the casino. On 3 November casino staff had noticed Mr A was associating with people that had previously come to the attention of casino staff for suspicious activities. The matter was referred to their monitoring team. At this point there were not reasonable grounds for suspicion.*

*After examining Mr A's transaction on 6 November casino staff noticed Mr A's playing habits were changing - he was spending longer at the casino and increasing the size and frequency of his bets.*

*The casino formed a suspicion Mr A was engaged in money laundering or other illicit activity and submitted a SAR on 9 November (within the three day time frame).*

**Grounds for suspicion detected on an initial interaction**

*Ms B was an existing customer of the bank. On 3 March she visited a branch of the bank with $20,000 in $20 notes. The bank's staff member noticed the money was damp and smelt of detergent and believed the money had been washed. Reasonable grounds of suspicion exist that Ms B was engaged in money laundering or other illicit activity; no further investigation was required to corroborate the suspicious state of the cash.*

*The matter was referred to the AML/CFT compliance team who submitted a SAR on 5 March (within the three day time frame).*

## Identifying suspicious activity

As a general rule, a suspicious activity will often be one which is inconsistent with a customer's known activities and profile, with the normal business expected for that type of customer or the normal business expected through the reporting entity.

In many cases reporting entities will be unaware what the underlying criminal activity is. However, by screening activities for indicators, typologies, and unusual transaction behaviours, a suspicion of criminal offending may arise. An activity may have many factors that, when considered individually, do not raise suspicion, but when considered collectively, suggest underlying criminal activity. Key activities indicative of criminality – which may occur domestically or trans-nationally – are listed below:

- An activity may be considered suspicious where it is unusually large for the customer's financial profile, or involves high risk factors (such as the international movement of funds or cash) not consistent with the normal activity for that customer's financial and business profile. Also, a request for the provision of services that are inconsistent with the reporting entity's normal business may give rise to suspicion.

- Comparing the activity to previous account records may be helpful and demonstrate reasonable grounds. Furthermore, attaching this information to the SAR will assist the FIU to understand your reasonable grounds for suspicion. This information can demonstrate how the suspicious transaction or activity in question is unusual and whether any patterns indicating criminal activity exist.
- Activities may also be suspicious if they do not match normal practice for that service. For example, grounds for suspicion may be formed where a reporting entity is asked to form or manage legal persons/arrangements that are unusually complex and opaque without a clear business reason.
- Reporting entities should also be vigilant for unusual activities that can affect the movement of value without the actual transfer of funds. Manipulation of trade invoicing, trade financing, and company or commodity ownership transfers can allow money launderers and terrorism financiers to move the value of criminal proceeds between each other while avoiding controls on transactions. Similarly, unusual loans are commonly set up between criminals and/or with companies and trusts under their control to facilitate the movement of illicit proceeds.
- The customer's or a third party's behaviour may also indicate grounds for suspicion. For example behaviour that indicates that the customer is seeking to avoid AML/CFT controls by using a third party to avoid customer due diligence, using intermediaries, nominee directors and shareholders, or structuring large transactions into a series of smaller ones.

## Countries with insufficient AML/CFT systems

The AML/CFT Act requires enhanced due diligence for non-resident customers from countries with insufficient AML/CFT systems or measures in place. Reporting entities should consider the relative ML/TF risk of foreign jurisdictions in the context of their own customer base and services offered. Reporting entities that conduct international business will need to inform themselves of jurisdiction risks as this can be a factor in suspicious activity reporting.

The FATF is the international body responsible for overseeing the implementation of legal, regulatory and operational measures for combating money laundering and terrorism financing. The FATF statements set out the countries that are high risk and non-cooperative in developing AML/CFT programmes. Also, many other countries have high risks for corruption, drugs, tax havens, human trafficking and smuggling etc. All countries are regularly evaluated by the FATF and by associated regional bodies such as the Asia-Pacific Group on Money Laundering (**APG**). The mutual evaluations from the FATF and APG provide up-to-date jurisdiction assessments. Reporting entities should use this useful information in making assessments of foreign country risk. Further information about both jurisdictions and overseas persons that pose a high risk can be found from the following sources:

- The United Nations Office for Drugs and Organised Crime produces research and analysis of all crimes that are precursors to money laundering, for example drugs trafficking.
- The United States' Office of Foreign Assets Control maintains lists of countries, entities and individuals associated with terrorism, money laundering and other sanctioned activities. Many jurisdictions hold lists of sanctioned people and entities.
- As a result of the Panama Papers and Paradise Papers, the European Union published the first EU list of non-cooperative tax jurisdictions, which contains a black list as well as a grey list.
- Transparency International also provides the Corruption Perception Index which can be an important indicator of jurisdiction risk.

- World FactBook is an open-source resource produced by the United States Central Intelligence Agency.
- The Basel AML index is an annual ranking assessing country risk regarding money laundering/terrorism financing by the International Centre for Asset recovery.
- Finally the credit rating agencies produce reports on jurisdictional risk (for example, Fitch, and Standard & Poor's, Moody's).

New Zealand reporting entities are also advised to regularly read updates on the New Zealand Police website on FATF public statements about locations of concern regarding international money laundering and terrorism risks here, and lists and information on designated terrorist entities here.

## Who should identify suspicious activity?

A suspicion may be raised by frontline staff during on-boarding or ongoing due diligence, or by back-room staff during account monitoring processes. When a suspicion is formed it is important that the basis for this suspicion is recorded and supplied in any subsequent SAR. Regular account monitoring according to risk is a key process for detecting suspicious activity. The relationship between staff and a reporting entity's AML/CFT compliance officer may assist in verifying the basis of suspicion. It is expected that SARs are submitted to the FIU after an internal assessment that the matter satisfies the reasonable grounds element.

## Auditors

In the course of their duties, a person acting in their occupation as an auditor may report suspicious activities. The FIU encourages auditors to do so if they have reasonable grounds to suspect it is relevant to the SAR triggers that are described in section 39A. Despite any other enactment or any rule of law, an auditor may report a SAR to the FIU. This applies to anyone conducting an audit, including auditors of financial statements. As auditing services are not subject to the Act, an auditor's business may not be a reporting entity and may not be registered for goAML. In such cases, auditors should contact the FIU to report a SAR.

## Who must report?

Usually, reporting entities' compliance officers are responsible for submitting SARs, although there is no barrier to other employees submitting SARs. Reports can be made by supervisors, managers, compliance officers or others tasked with submitting SARs to the FIU. If a reporting entity submits a SAR, the person directly involved in the activity does not have to be the person to submit the report to the FIU.

## What must be reported?

To be useful for analysis the SAR information needs to be sufficient to connect a person(s) to a suspicious activity along with any information collected (as permitted by the legislation and regulations) that helps to show the cause for suspicion.

The information requirements for SARs are set out in the AML/CFT (Requirements and Compliance) Amendment Regulations 2017. A SAR submitted to the FIU must, as it relates to the matter giving rise to suspicion, contain:

- a statement of the reasonable grounds on which the reporting entity holds a suspicion;
- an indication of any supporting documents that may help the FIU to analyse the SAR;
- details the reporting entity lawfully holds on the timing, parties and accounts for transactions or services that are sought or provided;
- customer or other party details – names, addresses, business names and addresses – and other supporting identity information (if collected as part of due diligence).

The AML/CFT Act adopts a risk-based framework. In some instances a reporting entity holds detailed and lengthy records of enhanced due diligence information and ongoing due diligence over several years. In such cases, the information in a SAR is likely to be fulsome.

In other situations a reporting entity may have grounds for suspicion following a one-off enquiry as an 'occasional activity' or 'occasional transaction'. However, all SARs must explain why the transaction or activity (or proposed transaction or activity) is suspicious. For example, stating that a personal or business transaction is suspicious because the transaction is large without any supporting information or explanation is not sufficient and does not satisfy the reasonable grounds element.

## When Legal Privilege applies

Section 42 defines and explicitly excludes legally privileged information from reporting. Reporting entities should approach disclosure obligations with rigour and carefully consider where legal privilege applies, and to what information in SARs. Legally privileged information is defined as being information that constitutes a communication that is:

- made or brought about for the purpose of obtaining providing legal advice or assistance; or
- subject to the general law on legal privilege or specified in sections 53-57 of the Evidence Act 2006.

Legal privilege does not remove the requirement to submit a SAR. Most information that relates to a suspicious activity is unlikely to be legally privileged. Legal privilege will likely only impact the reporting of the reason for suspicion and indicators. When the circumstances that trigger a SAR are met, all relevant non-legally privileged information set out in the regulations should be provided. However, care needs to be taken to ensure that privileged communications are not included in some instances.

The FIU may challenge claims of privilege where it is unclear that a careful consideration is made. This determination is also an objective test.

**Maintaining legal privilege example**

*If a communication seeking legal advice indicated that the customer was seeking to set up a trust to disguise identity, elements of the activity that constitute communication relating to advice should not be included in the SAR. In this case, the privileged communication is the query as well as advice given on how to lawfully set up the trust. The existence of such a trust, along with related trust documents and a description of grounds for suspicion may not be privileged communication.*

*An initial SAR may need to be filed within 3 days with minimal information. Further documents may then be provided to the FIU, or ordered by the Commissioner, as they become available. In some instances this initial SAR will be best followed by supplementary SAR reporting.*

Reporting entities in the legal profession may also wish to refer to DIA guidance on the application of legal privilege.

## What happens after reporting?

After a SAR has been submitted, a reporting entity must comply with all relevant provisions of the AML/CFT Act, including the requirement to submit additional SARs where appropriate. Further, several actions under section 37 must be considered in cases where adequate

customer due diligence cannot be conducted; in particular actions such as stopping or terminating a business relationship are key preventative measures.

## What is 'tipping off'?

Section 46 allows reporting entities to disclose information about SARs to the FIU and to specific others in some circumstances. Reporting entities must not disclose SAR information, or the existence of any SARs, to customers. This is for two reasons:

- the identity of staff and reporting entities who make SARs need to be protected for their safety; and
- the subject of a SAR may be part of a criminal investigation and should not be advised of this.

## How to report?

In limited circumstances, SARs may be submitted orally or manually. The vast majority of reports are made electronically online using goAML, which is the system specified by the Commissioner for secure electronic transmission of SARs between reporting entities and the FIU.

Reporting entities must transmit reports utilising this interface, called 'goAML'. Instructions on how to use goAML are set out on the Police website here.

It is feasible for a reporting entity to submit a SAR via email, however, this must be agreed between a reporting entity and the FIU and will only be approved in exceptional circumstances.

## Oral reports

In urgent situations a SAR may be made orally.

Circumstances in which suspicious transactions and activity can be reported orally include:

- Where a reporting entity thinks that a situation requires urgent action; and
- When a reporting entity has more than a reasonable suspicion, rather, knowledge or belief that the transaction is related to serious criminal offending.

Where a suspicious transaction has been reported orally, the reporting entity must submit an electronic version of the report to the FIU as soon as practicable, but no later than three working days after making the oral report.

If reporting entities would like assistance to get started in making online SARs - or to make an oral report - please contact the FIU during office hours on 04-474 9499, and ask for the Manager, Training, Liaison and Compliance, Financial Intelligence Unit.

## Follow-up to SARs

A quality assurance process is in place for SAR submissions; the purpose is to ensure the information provided is both sufficient for analysis and complies with the regulations. Information that is outside the scope of the AML/CFT Act is excluded at that point. The FIU may also make follow-up enquiries to reporting entities to clarify the information in a SAR shortly after submission. Any additional information held by a reporting entity about the grounds for suspicion can be vital in determining whether investigation and prosecution resources are deployed.

If the FIU forms reasonable grounds to suspect offending, there may be a formal request for further information about the matter under section 143 (1) (a). This section permits the Commissioner to ask for records, documents, or information that is relevant to analysing information received by the Commissioner under the AML/CFT Act.

## Feedback about SARs

The FIU's analysis of suspicious matters may occur as the result of a single SAR, or may occur sometime later following analysis of related SARs and/or other reports held by the FIU such as property, border, and prescribed transaction reports. As well, a SAR may directly trigger a criminal investigation. During the analysis and/or investigation the FIU or law enforcement agency may not involve the reporting entity further in respect of a SAR given the nature of criminal investigations.

**Feedback about SARs from the FIU**

*The success of the suspicious activity reporting regime depends on the alertness of reporting entities and high quality SAR reporting. The FIU values the contribution made by reporting entities and the cooperative relationships surrounding SAR submissions. However, the sensitivity of the information means that the FIU is usually unable to give direct feedback to reporting entities about whether a SAR has been useful in detecting criminal activity.*

## What are Prescribed Transaction Reports?

Prescribed Transaction Reports (**PTRs**) are reports that must be made irrespective of risk or suspicion. A prescribed transaction means a transaction conducted through the reporting entity in respect of:

- an international wire transfer of NZD1,000 and over where at least one of the institutions (i.e., ordering, intermediary or beneficiary institution) involved in the transaction is in New Zealand, and at least one is outside New Zealand.
- a domestic physical cash transaction at or over NZD10,000 which are transactions in New Zealand involving the use of physical currency i.e., coin and printed money designated as legal tender, and circulates as, and is customarily used and accepted as a medium of exchange in the country of issue.

Sector supervisors provide more detail on the circumstances in which PTRs must be submitted to the FIU. The FIU analyses PTRs along with other reports such as SARs and border cash reports. PTRs assist in both expanding analysis of SARs and may also independently lead to referrals for investigations.

**Submitting SARS on PTRs**

*PTR information complements other types of reports held by the FIU. The FIU also analyses patterns of suspicious behaviour using PTRs. The fact that a PTR has been submitted does not negate the need to also submit a SAR if there are reasonable grounds for suspicion.*

# *Typologies*

## What are typologies?

The term 'typologies' refers to the various techniques used to launder money or finance terrorism.

Which typologies are relevant for New Zealand?

The following list of common typologies was developed by the APG. These typologies are known to have occurred in the Asia-Pacific region. This list is consistent with the known money laundering and terrorism financing typologies identified in New Zealand. The list should be read in conjunction with the National Risk Assessment and relevant sector risk assessments and industry-specific guidance. Reporting entities should also be aware of the typologies reports and case studies produced by the FIU.

## Common typologies

- **Association with corruption (bribery, proceeds of corruption and instances of corruption undermining AML/CFT measures):** Corruption (bribery of officials) to facilitate money laundering by undermining AML/CFT measures, including the possible influence by politically exposed persons (PEPs): eg investigating officials or private sector compliance staff in banks being bribed or influenced to allow money laundering to take place.
- **Currency exchanges / cash conversion:** used to assist with smuggling to another jurisdiction or to exploit weak reporting requirements on currency exchange houses to minimise risk of detection – eg purchasing of travellers cheques to transport value to another jurisdiction.
- **Cash couriers / currency smuggling:** concealed movement of currency to avoid transaction / cash reporting measures.
- **Structuring (smurfing):** a method involving numerous transactions (deposits, withdrawals, and transfers), often involves various people, high volumes of small transactions and sometimes numerous accounts to avoid detection threshold reporting obligations.
- **Use of credit cards, cheques, promissory notes etc.:** Used as instruments to access funds held in a financial institution, often in another jurisdiction.
- **Purchase of portable valuable commodities (gems, precious metals etc.):** A technique to purchase instruments to conceal ownership or move value without detection and avoid financial sector AML/CFT measures – eg the movement of diamonds to another jurisdiction.
- **Purchase of valuable assets (real estate, race horses, vehicles, etc.):** Criminal proceeds are invested in high-value negotiable goods to take advantage of reduced reporting requirements to obscure the source of proceeds of crime.
- **Commodity exchanges (barter):** Avoiding the use of money or financial instruments in value transactions to avoid financial sector AML/CFT measures – eg a direct exchange of heroin for gold bullion.
- **Use of wire transfers:** to electronically transfer funds between financial institutions and often to another jurisdiction to avoid detection and confiscation.

- **Underground banking / alternative remittance services (hawala / hundi etc.):** informal mechanisms based on networks of trust used to remit monies. Often work in parallel with the traditional banking sector and may be outlawed (underground) in some jurisdictions. Exploited by money launderers and terrorism financiers to move value without detection and to obscure the identity of those controlling funds.
- **Trade-based money laundering and terrorism financing:** usually involves invoice manipulation and uses trade finance routes and commodities to avoid financial transparency laws and regulations.
- **Gaming activities (casinos, horse racing, internet gambling etc.):** Used to obscure the source of funds – eg buying winning tickets from legitimate players; using casino chips as currency for criminal transactions; using online gambling to obscure the source of criminal proceeds.
- **Abuse of non-profit organisations (NPOs):** May be used to raise terrorism funds, obscure the source and nature of funds and to distribute terrorism finances
- **Investment in capital markets:** to obscure the source of proceeds of crime, to further crime (market manipulation or fraud in the securities sector) or to purchase easily negotiable instruments (such as bank drafts and money orders), often exploiting markets with relatively low regulatory and reporting requirements.
- **Mingling (business investment):** a key step in money laundering involves combining proceeds of crime with legitimate business monies to obscure the source of funds.
- **Use of shell companies/corporations:** a technique to obscure the identity of persons controlling funds and exploit jurisdictions with relatively low regulatory and reporting requirements.
- **Use of offshore banks/businesses, including trust company service providers:** to obscure the identity of persons controlling funds and to move monies away from interdiction by domestic authorities.
- **Use of nominees, trusts, family members or third parties etc.:** to obscure the identity of persons controlling illicit funds.
- **Use of foreign bank accounts:** to move funds away from interdiction by domestic authorities and obscure the identity of persons controlling illicit funds.
- **Identity fraud / false identification:** used to obscure identification of those involved in many methods of money laundering and terrorism financing.
- **Use "gatekeepers" professional services (lawyers, accountants, brokers etc.):** to obscure identity of beneficiaries and the source of illicit funds. May also include corrupt professionals who offer 'specialist' money laundering services to criminals.
- **New payment technologies:** use of emerging payment technologies for money laundering and terrorism financing. Examples include cell phone-based remittance and payment systems and cryptocurrencies.

# *Indicators and warnings*

## What are indicators and warnings?

An activity may have certain 'red flag' features that may raise a suspicion that it is linked to criminal offending. These 'red flag' features are described as indicators. It is important that reporting entity staff can recognise indicators, especially indicators relevant to each reporting entity's sector, customer channel and services, as this will help determine if a transaction or activity is suspicious.

The presence of one or more indicators may not provide direct evidence of criminal activity; it may be sufficient to give cause for suspicion depending on circumstances. The presence of multiple indicators should act as a warning sign that additional inquiries may need to be undertaken. Additional inquiries made to a reporting entity's AML/CFT compliance officer may help to dismiss or support the suspicion.

A list of internationally established indicators is provided in this section. This list is divided into general and industry specific indicators. The indicators are based on literature from the FATF, overseas Financial Intelligence Units, and domestic partner agencies. Note that:

- Specific indicators are provided only for major industry groups covered by the AML/CFT Act. If no specific indicators are provided for your particular industry or business, reference should be made to the general indicators provided. Also, indicators provided for other industry groups may also be applicable to your business.
- The following list of indicators is offered as a guide and it is not an exhaustive list of every possible indicator. Staff should be aware that criminals and organised crime groups regularly adapt their behaviour to exploit weaknesses within different industries to launder funds.

## General indicators

### Personal attributes

- Admission of criminal activity.
- You are aware that a customer is the subject of a criminal investigation.
- Admission of an attempt to conceal funds.
- 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.
- Avoidance of face-to-face contact when conducting transactions.
- Reluctance to provide documents usually required and/or the use of counterfeit documentation.
- Transactions involving jurisdictions with weak AML/CFT regimes, particularly, where there is no apparent connection between the jurisdiction and the customer.
- Attempts are made to disguise beneficial owners and/or real parties to the transaction.
- Customer does not want correspondence sent to home address.

- Customer conducts transactions at different physical locations in an apparent attempt to avoid detection.
- Customer is accompanied or observed by a third party.
- Customer shows uncommon curiosity about internal systems, controls and policies and/or demonstrates high level of awareness around customer identification and AML/CFT standards.
- Customer has only vague knowledge of the amount of a deposit.
- Customer appears to informally record large volume transactions, using unconventional bookkeeping methods or "off-the-record" books.
- Normal attempts to verify the background of a new or prospective customer are difficult.
- Customer appears to be acting on behalf of a third party, but does not tell you.
- Customer uses aliases and a variety of similar but different addresses.
- Customer provides false information or information that you believe is unreliable.
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).
- Use of companies to move funds under the guise of legitimate transactions.
- Customer seeks short-cuts or variations from standard procedure and requires unusually quick transactions.
- Customer holds a public position and is conducting an unusual transaction.
- Customer has ties to an individual in a public position and is conducting unusual transactions.

### Identity

- Customer who uses misleading identification, or makes it difficult to verify information.
- Customer only presents copies rather than originals.
- Customer uses foreign, unverifiable identity documents.
- Unusual discrepancies in identification, such as name, address or date of birth.
- Customer alters transaction after being asked for identity documents.

### High risk customer characteristics

- Customer is a Politically Exposed Person (PEP) – or their relatives or associates
- Customer is a person or entity or is a person or entity associated with a country subject to sanctions – or their relatives or associates.
- Non-resident customers, especially those based in a high risk jurisdiction.
- High net worth individuals.
- Firms with silent partners. A silent partner is a person, or a partner in a company, who provides some of the capital for a business but who does not take an active part in managing the business.
- Non face-to-face customers.
- Individuals involved in cash transactions who share addresses, particularly when the addresses are also business locations.
- Customers seemingly acting together simultaneously using separate tellers to conduct large cash transactions or foreign exchange transactions.
- Customer has been the subject of previous suspicious transaction reporting.

### Cash transactions

- Customer frequently exchanges small bill for large ones.

- Customer presents notes that are packed or wrapped in a way that is uncommon for the customer.
- Customer makes cash transactions of consistently rounded-off large amounts.
- Cash deposits or withdrawals that fall consistently just below relevant transaction thresholds.
- Customer asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the customer.
- Large cash deposits using automatic teller machines or drop boxes to avoid direct contact with staff.
- Frequent exchanges of cash into other currencies, where there appears to be no logical explanation for such activity.
- Transfers of large sums of money to or from overseas locations with instructions for payment in cash.
- Several transactions conducted on the same day and at the same branch of a reporting entity with a deliberate attempt to use different tellers.
- High value cash deposits to pay for international funds transfers.

### No economic purpose

- Transaction appears to be out of the ordinary or normal industry practice or does not appear to be economically viable for the customer.
- Transaction is unnecessarily complex.
- Activity is inconsistent with what would be expected from declared business.
- Transaction involves non-profit or charitable organisation for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organisation and the other parties in the transaction.
- Funds invested in a dormant company.
- Frequent small payments to and from jurisdictions of high terrorism risk.
- Payments are structured to avoid thresholds.
- Customer seeks anonymity through third parties, unusual identification.

### Terrorism financing, weapons proliferation and security

- Customer is a person subject to New Zealand sanctions, or is a representative of sanctioned persons or entities.
- Customer accesses accounts, and/or uses debit or credit cards in high risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability, subject to sanctions, or known to support terrorism activities and organisations.
- Customer identified by media or law enforcement as having travelled, attempted/ intended to travel to high risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorism activities and organisations.
- Customer conducted travel-related purchases (for example, purchase of airline tickets, travel visa, passport, etc.) linked to high risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorism activities and organisations.
- The customer mentions that they will be travelling to, are currently in, or have returned from, a high risk jurisdiction (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorism activities and organisations.

- Customer depletes account(s) by way of cash withdrawal.
- Customer or account activity indicates the sale of personal property/ possessions.
- Individual/ Entity's online presence supports violent extremism or radicalisation.
- Customer indicates planned cease date to account activity.
- Customer utters threats of violence that could be of concern to National Security/ Public Safety.
- Sudden settlement of debt(s) or payments of debts by unrelated third party(ies).
- Law enforcement indicates to reporting entity that the individual/ entity may be relevant to a law enforcement and/or national security investigation.
- Customer's transactions involve individual(s)/ entity(ies) identified by media or law enforcement as the subject of a terrorism financing or national security investigation.
- Customer donates to a cause that is subject to derogatory publicly available information (crowdfunding initiative, charity, NPO, non-governmental organisation etc.).
- Customer conducts uncharacteristic purchases (for example, camping/ outdoor equipment, weapons, ammonium nitrate, hydrogen peroxide, acetone, propane, etc.).
- Customer trades in commodities that may also be dually used in missiles, and chemical, biological and nuclear weapons.
- A large number of email transfers between customer and unrelated third party(ies).
- Customer provides multiple variations of name, address, phone number or additional identifiers.
- The sudden conversion of financial assets to a virtual currency exchange or virtual currency intermediary that allows for increased anonymity.

### Use of account(s)

- Use of third parties to deposit funds into account(s).
- Account receives a large number of small cash deposits and a small number of large cash withdrawals.
- Frequent or elaborate movement of funds between related accounts.
- Funds received from or remitted to high risk jurisdictions.
- Cash deposited domestically, with the funds subsequently withdrawn from ATMs offshore.
- Funds are transferred from several accounts and consolidated into one account prior to an international transfer, particularly, to a high risk jurisdiction.
- Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.
- Activity far exceeds activity projected at the time of opening of the account.
- Sudden increase in activity on a dormant account.
- Use of multiple bank accounts or foreign currency accounts without legitimate reason.
- Reluctance to use favourable facilities, for example, avoiding high interest rate facilities for large balances.
- Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using customer accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other customer company and trust accounts.
- Frequent and/or unscheduled cash deposits to loan accounts.
- Frequent deposits of winning gambling cheques followed by immediate withdrawal or transfer of funds.

- Use of internet banking to frequently access New Zealand based accounts internationally.
- Children's accounts (including adult children) being used for the benefit of parents/guardians.

### Use of jurisdictions with weak AML/CFT frameworks

- Transactions going to/from accounts based in locations with weak AML/CFT regimes.
- Investment funds transferred to/from high risk jurisdictions.
- Cross-jurisdictional networks of companies and trusts in high risk jurisdictions.

## Industry specific indicators

The following industry specific indicators may give rise to reasonable grounds for suspicion.

### Registered banks and non-bank deposit takers – Personal transactions

The traditional finance sector continues to be a primary avenue for money laundering.

- Customer makes frequent or large payments to online payment services.
- Customer runs large positive credit card balances.
- Customer visits the safety deposit box area immediately before making cash deposits of sums under the reporting threshold.
- Customer requests to have credit/debit cards sent to locations other than his or her address.
- Customer frequently transfers funds to unknown third parties.
- Unknown third parties frequently transfer funds into customer's account.
- Customer frequently exchanges currencies.
- Customer has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- Customer requests movement of funds that are uneconomical.
- High volume of wire transfers are made or received through the account.
- Immediately after transferred funds have cleared, the customer moves the funds to another account or to another individual or entity.
- International funds transfers from a customer's account to several offshore accounts held in the same name.
- Large foreign exchange transactions.
- Use of counterfeit currency.

### Registered banks and non-bank deposit takers – Business transactions

- Accounts are used to receive or disburse large sums but show virtually no normal business-related activities, such as the payment of payrolls, invoices, etc.
- Accounts have a large volume of deposits in bank drafts, cashier's cheques, money orders or electronic funds transfers, which are inconsistent with the customer's business.
- Accounts have deposits in combinations of cash and monetary instruments not normally associated with the business activity.
- Business does not want to provide complete information regarding its activities.
- Financial statements of the business differ noticeably from those of similar businesses.
- Representatives of the business avoid contact with the branch as much as possible, even when it would be more convenient for them.

- Deposits to or withdrawals from a corporate account are primarily in cash rather than in the form of debit and credit normally associated with commercial operations.
- Customer maintains a number of trustee or customer accounts that are not consistent with that type of business or not in keeping with normal industry practices.
- Customer operates a retail business providing cheque-cashing services but does not make large draws of cash against cheques deposited.
- Customer pays in cash or deposits cash to cover bank drafts, money transfer or other negotiable instruments.
- Customer purchases cashier's cheques and money orders with large amounts of cash.
- Customer makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere.
- Customer makes large volume of cash deposits from a business that is not normally cash-intensive.
- Customer makes large cash withdrawals from a business account not normally associated with cash transactions.
- Customer consistently makes immediate large withdrawals from an account that has just received a large and unexpected credit from abroad.
- Customer makes a single and substantial cash deposit composed of many large bills.
- There is a substantial increase in deposits of cash or negotiable instruments by a company offering professional advisory services, especially if the deposits are promptly transferred.
- There is a sudden change in cash transactions or patterns.
- There is a marked increase in transaction volume on an account with significant changes in an account balance that is inconsistent with or not in keeping with normal business practices of the customer's account.
- Unexplained transactions are repeated between personal and commercial accounts.
- Activity is inconsistent with stated business.
- Account has close connections with other business accounts without any apparent reason for the connection.
- A large number of incoming and outgoing wire transfers take place for which there appears to be no logical business or other economic purpose.

### Registered banks and non-bank deposit takers – NPO sector transactions

- Known or suspected criminal entities establishing trust or bank accounts under charity names.
- Inconsistencies between the pattern or size of financial transactions and the stated purpose and activity of the organisation.
- Sudden increase in the frequency and amounts of financial transactions for the organisation, or the inverse, that is, the organisation seems to hold funds in its account for a very long period.
- Large and unexplained cash transactions by the organisation.
- Absence of contributions from donors located in New Zealand.
- Large number of NPOs with unexplained links.
- The NPO appears to have little or no staff, no suitable offices or no telephone number, which is incompatible with their stated purpose and financial flows.
- The NPO has operations in, or transactions to or from, high risk jurisdictions.

### Money service business (including currency exchange and money remittance) and other businesses involved in electronic funds transfers

- The use of numerous agent locations for no apparent reason to conduct transactions.
- Multiple customers conducting international funds transfers to the same overseas beneficiary.
- Multiple low-value international funds transfers, possibly indicating a large amount of funds broken down into smaller amounts.
- Several customers request transfers either on the same day or over a period of two to three days to the same recipient.
- Customer does not appear to know the recipient to whom they are sending the transfer.
- Customer conducts large transactions to/from countries known as narcotic source countries or as trans-shipment points for narcotics, or that are known for highly secretive banking and corporate law practices.
- Customer sends frequent wire transfers to foreign countries, but does not seem to have connection to such countries.
- Customer exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Customer knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument.
- Customer instructs that funds are to be picked up by a third party on behalf of the payee.
- Customer makes large purchases of traveller's cheques not consistent with known travel plans.
- Customer requests that a large amount of foreign currency be exchanged to another foreign currency.
- Large amounts of currency exchanged for traveller's cheques.
- Customer exchanges small denomination of bills for larger denominations.

### Life insurance

- Large single payments and payouts.
- Customer changes the beneficiary of policies.
- Customer wants to use cash for a large transaction.
- Customer proposes to purchase an insurance product using a cheque drawn on an account other than their personal account.
- Customer requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment.
- Customer who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump sum payment.
- Customer conducts a transaction that results in a conspicuous increase in investment contributions.
- Scale of investment in insurance products is inconsistent with the customer's economic profile.
- Unanticipated and inconsistent modification of customer's contractual conditions, including significant or regular premium top-ups.
- Unforeseen deposit of funds or abrupt withdrawal of funds.
- Involvement of one or more third parties in paying the premiums or in any other matters involving the policy.

- Overpayment of a policy premium with a subsequent request to refund the surplus to a third party.
- Funds used to pay policy premiums or deposits originate from different sources.
- Use of life insurance product in a way that resembles use of a bank account, namely making additional premium payments and frequent partial redemptions.
- Customer cancels investment or insurance soon after purchase.
- Early redemption takes place in the absence of a reasonable explanation or in a significantly uneconomic manner.
- Customer shows more interest in the cancellation or surrender of an insurance contract than in the long-term results of investments or the costs associated with termination of the contract.
- Customer makes payments with small denomination notes, uncommonly wrapped, with postal money orders or with similar means of payment.
- The duration of the life insurance contract is less than three years.
- The first (or single) premium is paid from a bank account outside the country.
- Customer accepts very unfavourable conditions unrelated to their health or age.
- Transaction involves use and payment of a performance bond resulting in a cross-border payment.
- Repeated and unexplained changes in beneficiary.
- Relationship between the policy holder and the beneficiary is not clearly established.

### Investments

- 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, payments requested for no apparent reason to third parties.
- Funds deposited into stockbroker's account followed immediately by request for repayment.
- Limited or no securities transactions recorded before settlement requested.
- Overpayment of stock purchases with the excess amount being sent to a third party instead of being returned to the account holder’s bank account.
- Internal third party transfer requests between securities accounts, for no apparent reason.

### Cash transporters-couriers

- Transactions involving locations with weak AML/CFT regimes or 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.

### Casinos

- Where a customer’s gaming behaviour is unusual for their financial status.
- Customer purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a casino cheque.
- Regular or multiple purchasing and cashing of gaming chips just below the occasional transaction reporting threshold.
- Structuring chip purchases/ cash-outs.

- Third parties involved in depositing and withdrawing funds at casino.
- Transfers from company accounts to private betting accounts.
- Use of third parties to purchase gaming chips.
- Use of third parties to gamble proceeds through a casino.
- Customer requests a winnings cheque in a third party's name.
- Exchange of low denomination for high denomination currency.
- Buying chips for cash or on account then redeeming value by way of casino cheque or money transfer.
- Acquaintances bet against each other in even-money games and it appears that they are intentionally losing to one of the party.
- Customer attempts to avoid the filing of a report for cash by breaking up the transaction.
- Customer requests cheques that are not for gaming winnings.
- Customer puts money into slot machines and claims accumulated credits as a jackpot win.
- Customer exchanges small denomination bank notes for large denomination bank notes, chip purchase vouchers or cheques.
- Customer is known to use multiple names.
- Customer requests the transfer of winnings to the bank account of a third party or a known drug source country or to a country where there is weak AML/CFT system.

### Real estate transactions

- Customer uses third party names on property titles without obvious reason.
- Customer uses trust name on property title without obvious reason.
- Customer appears unconcerned about selling or buying well below or above market value.
- Beneficial ownership of the transactions is obscure.
- Customer arrives at a real estate closing with a significant amount of cash.
- Customer purchases property in someone else's name such as an associate or a relative (other than a spouse).
- Customer does not want to put their name on any document that would connect them with the property or uses different names on Offers to Purchase, closing documents and deposit receipts.
- Customer inadequately explains the last minute substitution of the purchasing party's name.
- Customer negotiates a purchase for the market value or above the asked price, but requests that a lower value be recorded on documents, paying the difference “under the table”.
- Customer pays initial deposit with a cheque from a third party, other than a spouse or a parent.
- Customer pays substantial down payment in cash and balance is financed by an unusual source (for example, a third party or private lender) or offshore bank.
- Customer purchases personal use property through their company when this type of transaction is inconsistent with the ordinary business practice of the customer.
- Customer purchases multiple properties in a short time period, and seems to have few concerns about the location, condition and anticipated repair costs, etc. of each property.
- Customer insists on providing signature on documents by fax only.
- Customer over justifies or over explains the purchase.

- Customer's home or business telephone number has been disconnected or there is no such number.
- Customer uses a post office box or General Delivery address where other options are available.
- Customer wants to build a luxury house in non-prime locations.
- Customer exhibits unusual concerns regarding the firm's compliance with government reporting requirements and the firm's AML policies.
- Customer exhibits a lack of concern regarding risks, commissions or other transaction costs.
- Customer persists in representing their financial situation in a way that is unrealistic or that could not be supported by documents.
- Transactions carried out on behalf of minors, incapacitated persons or other persons who, although not included in these categories, appear to lack the economic capacity to make such purchases.
- A transaction involving legal entities, when there does not seem to be any relationship between the transaction and the activity carried out by the buying company, or when the company has no business activity.
- Transactions in which the parties show a strong interest in completing the transaction quickly, without there being good cause.
- Transactions in which the parties are foreign or non-resident for tax purposes and their only purpose is a capital investment (that is, they do not show any interest in living at the property they are buying).
- Transactions involving payments in cash or in negotiable instruments which do not state the true payer (for example, bank drafts), where the accumulated amount is considered to be significant in relation to the total amount of the transaction.
- Transactions in which the party asks for the payment to be divided in to smaller parts with a short interval between them.
- Transactions in which payment is made in cash, bank notes, bearer cheques or other anonymous instruments.
- Transactions which are not completed in seeming disregard of a contract clause penalising the buyer with loss of the deposit if the sale does not go ahead.
- Recording of the sale of a building plot followed by the recording of the declaration of a completely finished new building at the location at an interval less than the minimum time needed to complete the construction, bearing in mind its characteristics.
- Transaction is completely anonymous – transaction conducted by lawyer – all deposit cheques drawn on lawyer's trust account.

### The following indicators apply to real estate agents and sales representatives

- Customer sells property below market value with an additional “under the table” payment.
- Customer purchases property without inspecting it.
- Customer is known to have paid large remodelling or home improvement invoices with cash, on a property for which property management services are provided.
- Customer buys back a property that they recently sold.
- Frequent change of ownership of same property, particularly between related or acquainted parties.

- If a property is re-sold shortly after purchase at a significantly different purchase price, without corresponding changes in market values in the same area.

### Wholesalers and suppliers

- Customer requests management of invoicing and trade activity from professional to appear legitimate.
- Invoices or payments of invoices are inconsistent with known business or trading behaviour.
- Over or under-invoicing, structured, complex, or multiple invoice requests, and high-dollar shipments that are over or underinsured.
- Unwillingness by a supplier to provide complete or accurate contact information, financial references or business affiliations.

### Loans

- Customer seeks loan without obvious reason.
- Customer makes early, large payments disproportionate to known income (common in real estate).
- Customer makes or receives payments against the loan from unusual sources (cash or funds from foreign jurisdictions).
- Customer makes or receives payment against loans ‘in kind’.
- Customer suddenly repays a problem loan unexpectedly.
- Customer repays a long term loan, such as a mortgage, within a relatively short time period.
- Source of down payment is inconsistent with borrower's background and income.
- Down payment appears to be from an unrelated third party.
- Down payment uses a series of money orders or bank drafts from different financial institutions.
- Customer's employment documentation lacks important details that would make it difficult to contact or locate the employer.
- Customer's documentation to ascertain identification, support income or verify employment is provided by an intermediary who has no apparent reason to be involved.
- Customer has loans with offshore institutions or companies that are outside the ordinary course of business of the customer.
- Customer offers you large dollar deposits or some other form of incentive in return for favourable treatment of loan request.
- Customer asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known.
- The loan transaction does not make economic sense (for example, the customer has significant assets, and there does not appear to be a sound business reason for the transaction).
- Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.
- Customer applies for loans on the strength of a financial statement reflecting major investments in or income from businesses incorporated in countries known for highly secretive banking and corporate law and the application is outside the ordinary course of business for the customer.
- Down payment or other loan payments are made by a party who is not a relative of the customer.

### Trust and company service providers and lawyers and accountants

- Creation and use of complex legal person arrangements for no apparent reason. Especially cross-jurisdictionally.
- Creation of complicated structures where there is no apparent economic reason. Especially cross-jurisdictionally.
- Seeks anonymity. Use of an agent, nominee or intermediary without apparent reason.
- Requests to set up accounts in names of third parties or trusts and companies. Especially cross-jurisdictionally.
- Requests to receive funds from high risk jurisdictions and intermediaries.
- Requests to transfer ownership of legal person arrangements to an unknown third party.
- Customers or intermediaries use nominee directors/ shareholders/ officers.
- Customers or intermediaries address is a virtual office or that of a third party.

### Accountants, lawyers and real estate agents (gatekeeper services)

- Customer seeks use of an agent, nominee or intermediary without obvious reason. Especially cross-jurisdictionally.
- Customer uses professional business or trust account, particularly, where large cash deposits are made.
- Funds are received from a foreign jurisdiction, particularly, where there is no connection between the jurisdiction and the customer.
- Overseas instruction from a customer for no economic reason.
- Customer is not concerned about the level of fees.
- Customer has a fast-growing real estate portfolio.
- Customer is a company or trust with complicated beneficial ownership.
- Purchase amount is unusual compared to the appraised value or the previous purchase amount.
- Customer appears to have access to cash substantially above their means.
- Customer uses a virtual office.
- Customer invoice and trade accounts inconsistent with known business activity.

### Accountants and accounting firms

- Client appears to be living beyond their means.
- Client has cheques inconsistent with sales (i.e., unusual payments from unlikely sources).
- Client has a history of changing bookkeepers or accountants yearly.
- Client is uncertain about location of company records.
- Company carries non-existent or satisfied debt that is continually shown as current on financial statements.
- Company has a number of employees, which is unusual for the type of business.
- Company is paying unusual consultant fees to offshore companies.
- Company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues without reasonable explanation of the continued loss.
- Company shareholder loans are not consistent with business activity.
- Examination of source documents shows misstatements of business activity that cannot be readily traced through the company books.

- Company makes large payments to subsidiaries or similarly controlled companies that are not within the normal course of business.
- Company acquires large personal and consumer assets (i.e., boats, luxury automobiles, personal residences and cottages) when this type of transaction is inconsistent with the ordinary business practice of the client or the practice of that particular industry.
- Company is invoiced by organizations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.

### Dealers in high value goods

- Customer indiscriminately purchases merchandise without regard for value, size, or colour.
- Purchases or sales that are unusual for customer or supplier.
- Unusual payment methods, such as large amounts of cash or payment from third-parties.
- Attempts by customer or supplier to maintain high degree of secrecy with respect to the transaction, such as request that normal business records not be kept.
- Customer is reluctant to provide adequate identification information when making a purchase.
- Transactions that appear to be structured to avoid reporting requirements i.e. multiple transactions below $10,000 in cash.
- A customer orders item, pays for them in cash, cancels the order and then receives a refund.
- A customer asking about the possibility of returning goods and obtaining a cheque (especially if the customer requests that payment be made to a third party).
- A customer paying for high-priced jewellery or precious metal with cash only.
- A customer not asking for the reduced price or haggling over the list price.
- Purchase appears to be beyond the means of the customer based on their stated or known occupation or income.
- Customer may attempt to use a third party cheque or a third party credit card.
- Funds come from an offshore financial centre rather than a local bank.
- Large or frequent payments made in funds other than New Zealand dollars.
- Transaction lacks business sense.
- Purchases or sales that are not in conformity with standard industry practice.

## *Use and disclosure of information by the FIU*

The FIU uses SAR information to prevent, dismantle and disrupt serious and organised crime and to assist with protecting national security.

### Investigations and prosecutions

The FIU uses the information it lawfully collects under the AML/CFT Act and regulations for analysis. The primary use of the intelligence developed by the FIU is for the investigation and prosecution of financially motivated crime. Typically, New Zealand Police is the biggest FIU customer in terms of the dissemination of intelligence. The Police have various specialist investigation teams which receive FIU products, such as the Money Laundering Investigations Team, the Cybercrime Unit, the Asset Recovery Unit, and the National Organised Crime Group, as well as Criminal Investigation Branches in each of the Police Districts. These Police units are responsible for the investigation of offences such as money laundering, drug dealing, certain fraud, theft, online child exploitation and terrorism financing.

The FIU also contributes to other law enforcement agencies such as New Zealand Customs for customs offending and importation of illicit goods and trade-based money laundering, Inland Revenue for tax evasion cases, Immigration New Zealand for labour and immigration fraud, migrant exploitation and people trafficking matters, and the Serious Fraud Office for complex fraud and corruption cases.

The FIU discloses information to the appropriate agencies for the purposes of national security, counter-terrorism, countering weapons proliferation, and transnational and serious organised crime.

As previously discussed, there are many other offences that generate illicit profit that is subsequently laundered; this means that there are many other government agencies that may receive intelligence from the FIU on a case-by-case basis. FIU publishes quarterly statistics which shows the distribution of the financial intelligence it produces.

### International cooperation

A key function of the FIU is to receive and analyse financial intelligence from international counterparts and other enforcement agencies.

The New Zealand FIU is a member of the Egmont Group which is a large global network of FIUs. Egmont Group was created to provide FIUs around the world a forum to exchange information confidentially to combat money laundering, the financing of terrorism and other predicate offences. It currently has 156 member FIUs. Given the transnational nature of money laundering and terrorism financing, information sharing is an effective way to disrupt money laundering. Each member of the Egmont Group assists with intelligence products and requests for information from other countries. The New Zealand FIU contributes information to the Egmont Group for law enforcement purposes under the AML/CFT Act. The security of information within the Egmont Group is governed by international convention. There are reputational repercussions for any member country that discloses information inappropriately, especially with respect to ongoing access to Egmont Group information. Further, the New Zealand FIU has formal information sharing agreements with a number of other FIUs; those agreements mutually reinforce the security of each country's information.

On a case-by-case basis, the FIU shares financial intelligence internationally through the Police Liaison Officers who are Police employees hosted in other countries and through Interpol.

## Prevention and disruption

The FIU has a role in preventing and disrupting crime. Usually, if investigation and prosecution is not appropriate or not possible, the FIU may disclose information to agencies with regulatory responsibilities. In these cases the FIU is seeking to prevent or disrupt further criminal activity. An example is the referral of a reporting entity to an AML/CFT supervisor for cases in which early regulatory action is preferable to law enforcement action. Regulatory prevention and disruption can be applied effectively where there is offshore offending. An example is the referral to the RBNZ of intelligence on an offshore company claiming to be a registered New Zealand bank. The RBNZ may undertake a range of enquiries and there are several options for regulatory action.

## *Protections*

Under the AML/CFT Act a number of protections exist for persons reporting suspicious activity.

Note that the following section provides a summary of the protections related to SARs. It does not constitute legal advice. For full details on these and other protections reference should be made to the AML/CFT Act.

### Protection of a person reporting suspicious activity

Where a person reports a suspicious activity (section 44) or supplies any information in connection with a SAR, they will not be held criminally or civilly liable for any action taken in order to comply with the AML/CFT Act or regulations is the action –

(a) Was taken in good faith; and
(b) Was reasonable in the circumstances.

### Immunity from liability for disclosure of information

Immunity from liability for disclosure of information (section 45) applies where:

- A person does any act that constitutes an offence against section 243 of the Crimes Act 1961; and
- In respect of doing that act, that person would have a defence to a charge under that section by virtue of section s244(a) of the Crimes Act 1961; and
- That person discloses, to any Police employee, any information relating to the money laundering transaction or suspected money laundering transaction; and
- That information is disclosed in good faith for the enforcement of criminal law; and
- That person is otherwise under an obligation to maintain secrecy in relation to, or not to disclose, that information.

If the above immunity applies, then, notwithstanding that the disclosure would otherwise constitute a breach of that obligation of secrecy or non-disclosure, the disclosure by that person, to that member of the Police, of that information is not a breach of that obligation of secrecy or non-disclosure or (where applicable) of any enactment by which that obligation is imposed.

### Disclosure of information in judicial proceedings

Protection against disclosure in judicial proceedings (section 47) applies to:

- SARs,
- Any information that would identify a person who prepared, handled, or reported a SAR,
- Other information that would infer the existence of an SAR.

This information can only be disclosed in judicial proceedings where a Judge (or person presiding) is satisfied that the disclosure is necessary in the interests of justice.

### Acting in compliance with the AML/CFT Act

Section 77 offers a broad protection for actions undertaken by reporting entities and their staff.

No reporting entity is criminally or civilly liable for any action taken in order to comply with the AML/CFT Act if the action was taken in good faith and was reasonable in the circumstances.

## *Offences and penalties*

The AML/CFT regime fosters cooperative relationships between reporting entities, supervisors and the FIU. The FIU relies on close relationships with reporting entities. Should a reporting entity's customer be the subject of further enquiries reporting entities can expect a cooperative and supportive relationship with the FIU. The expectation on reporting entities is one of effective risk management with the aim of preventing and detecting money laundering and terrorism financing. To help reporting entities comply with the legislation many offences are termed 'civil liability acts' and the associated penalties are either administrative or pecuniary. However, some offences fall in the criminal jurisdiction. For example, it is an offence to knowingly or recklessly engage in conduct that constitutes a civil liability act. Reporting entities should familiarise themselves with the offences and penalties set out in the AML/CFT Act.

**Note:** The following section provides a generalised list of the offences and penalties related to reporting suspicious activities. It does not constitute legal advice. For full details on these and other offences and penalties, reference should be made to the AML/CFT Act**.**

### Offences relating to suspicious activity reporting

Section 92: It is an offence to fail to report suspicious activity (including, but not limited to transactions). A reporting entity commits an offence if an activity is conducted or is sought to be conducted through the reporting entity; and the reporting entity has reasonable grounds to suspect that the activity or the proposed activity is or may be relevant to a money laundering offence or an offence that gives rise to money laundering or terrorism financing.

Section 93: It is an offence to provide false or misleading information. A person commits an offence who, in making a SAR or a prescribed transaction report (**PTR**), or in supplying information in connection with a SAR or PTR:

- Makes any statement that the person knows is false or misleading in a material particular; or
- Omits from any statement any matter or thing without which the person knows that the statement is false or misleading in a material particular.

Section 94: It is an offence to unlawfully disclose SARs or PTRs. Section 46 sets out the colloquially termed 'tipping off' provisions. Reporting entities cannot disclose reports made to the FIU to either help the customer or themselves or it may prejudice money laundering or terrorism financing investigations.

Section 95: Records must be retained. The FIU is reliant on accurate and timely information. It is an offence to fail to keep or retain adequate records relating to suspicious activity or prescribed transactions for 5 years.

Section 96: It is an offence to obstruct an investigation relating to SARs and PTRs.

Section 97: Section 47 also protects SARs, any information that would identify a person who prepared, handled or reported a SAR, and any other information that would infer the existence of a SAR. A person commits an offence if they disclose information protected under section 47 without lawful excuse.

Section 101: Avoiding detection by making transactions just below prescribed transaction thresholds is a common money laundering method. It is an offence to structure transactions, or to help a person structure transactions, in this way.

## Penalties

A reporting entity or person who commits an offence under any of sections 91 to 97 and section 101 is liable, on conviction to –

(a) In the case of an individual, either or both of the following:
    (i). A term of imprisonment of not more than two years:
    (ii). A fine of up to NZD $300,000; and
(b) In the case of a body corporate, a fine of up to NZD $5 million.