Practice Guidelines for the Financial Transactions Reporting Act 2017

Issued by the Financial Intelligence Unit

Pursuant to section 65 of the Financial Transactions Reporting Act 2017

August 2017

Table of Contents

What are these guidelines for?

The Financial Transactions Reporting Practice Guidelines are issued by the Financial Intelligence Unit in conjunction with the Financial Supervisory Commission. The guidelines are designed to assist you with the obligations under the Financial Transactions Reporting Act 2017 (the Act). It includes guidance on:

- Financial misconduct;
- Compliance Programmes and Risk Assessments;
- Customer Due Diligence;
- Record Keeping;
- Financial transaction reports; and
- The reporting of suspicious activity to the FIU.

As a reporting institution you must give high priority to establishing and maintaining an effective compliance regime and culture. It is recognised that effective regimes can only be delivered through partnership with industry, and accordingly the FIU encourages all reporting institutions to ensure that they establish an open and positive approach to compliance issues amongst all employees.

Failure to comply with an obligation under the Act can constitute an offence which carries penalties up to **$250,000 or to imprisonment for a term not exceeding 5 years for an individual or up to $1,000,000 for a company.**

You must comply with the Act despite any obligation as to secrecy or other restrictions on the disclosure of information imposed by any other enactment or law.

These guidelines are provided for information only and should not be relied on as evidence of complying with the requirements of the Act. They do not constitute legal advice and should not be relied on as such.

If, after reading these guidelines, you are still unclear about your any of your obligations please seek legal advice or contact the FIU.

Additional guidelines may issued by the the FIU from time to time under section 65 of the Act and these guidelines may be updated as required.

Phil Hunkin

Head

Financial Intelligence Unit

1. Introduction

The Cook Islands has a reputation as a sound and well regulated jurisdiction. This was confirmed by the 2009 APG Mutual Evaluation. It is essential for the country to maintain this reputation in order to continue attracting legitimate investors with funds and assets that are untainted by criminality.

Anyone in the Cook Islands that assists with facilitating financial misconduct, whether knowingly, unintentionally or without regard to what they may be facilitating, could face law enforcement action as well as the loss of reputation and customers. This kind of conduct by a reporting institution also damages the reputation of the Cook Islands as a whole.

The Financial Transactions Reporting Act 2017 (the Act) replaces the Financial Transactions Reporting Act 2004 and along with the Financial Transaction Reporting Regulations 2017 (the Regulations), provide the legal framework in which reporting institutions must have in place compliance systems to assist with the prevention, detection and prosecution of financial misconduct.

The Financial Action Task Force (FATF) 2012 revised recommendations that state compliance systems should adopt a risk-based approach. The Act (and subsidiary legislation) requires that the risks posed by customers, products and systems are identified, mitigated and the mitigating measures are documented and reviewed periodically.

Systems and controls may not always prevent and detect financial misconduct but it is envisaged the risk-based approach will serve to balance the cost burden placed on reporting institutions and their customers with a realistic assessment of the threat of a business being used in connection with financial misconduct.

2. Financial misconduct – what is it?

The vast majority of criminals would not be in the business of crime if it were not for the tremendous profits to be made. There is a direct relationship between the profitability of most types of crimes and their prevalence. The Act is aimed at reducing that profitability by ensuring reporting institutions assist in the detecting and preventing of financial misconduct, as well as other serious offences. Financial misconduct is defined in the Financial Intelligence Unit Act 2015 and includes:

- Money laundering
- Fraud involving cross-border transactions
- The financing of terrorism
- The financing of the proliferation of weapons of mass destruction
- The financing or facilitation of bribery, and other corrupt practices
- Tax evasion.

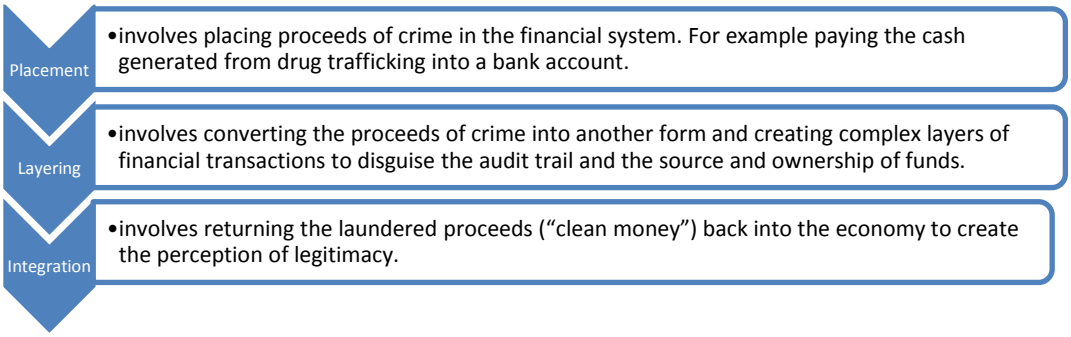
The types of financial misconduct (as listed above) are interrelated in many aspects, particularly in relation to money laundering, and consideration of each type of misconduct should take into account how that type may relate to others.

The National Money Laundering and Terrorism Financing Risk Assessment 2015[1] sets out the risks to the Cook Islands as a jurisdiction. It is a useful tool for reporting institutions to understand and recognise the risks of financial misconduct to the Cook Islands and how they may fit into that picture.

2.1 Money laundering

Money laundering is any act or attempted act to disguise the source of money or assets derived from criminal activity, which is generally known as the proceeds of crime. Money laundering is a criminal offence in the Cook Islands under the Crimes Act 1969. Money laundering enables criminals such as drug dealers, terrorists, fraudsters, to amass wealth and operate and expand their criminal empires. The economic and political influence of criminal organisations weakens the social fabric, collective ethical standards, and ultimately the democratic institutions of societies such as the Cook Islands. The FATF list of designated categories of predicate offences can be found at **Appendix 8**.

There are three recognised stages in the money laundering process:



Some common methods of laundering money or assets are:

- **Nominees**
  This is one of the most common methods of laundering and hiding assets. A money launderer uses family members, friends or associates who are trusted by them, and who will not attract attention, to conduct transactions on their behalf. The use of nominees facilitates the concealment of the source and ownership of assets.
- **Structuring**
  Many individuals deposit cash or buy bank drafts at various institutions, or one individual carries out transactions for amounts less than the amount that must be reported to the authorities (usually the FIU), and the cash is subsequently transferred to a central account. These transactions normally do not attract attention as they deal in funds that are below reporting thresholds and they appear to be conducting ordinary transactions.

[1] www.fsc.gov.ck/cookIslandsFscApp/content/fiu/aboutus/nationalriskassessment

- **Asset purchases with bulk cash**
  Individuals purchase high-value items such as cars, boats, and real estate with cash. In many cases, launderers use the assets but distance themselves from them by having them registered in a friend's or relative's name. The assets may also be resold to further launder the proceeds. Individuals often use proceeds of crime to buy foreign currency that can then be transferred to offshore bank accounts anywhere in the world.
- **Currency smuggling**
  Funds are moved across borders to disguise their source and ownership, and to avoid being exposed to the law enforcement and reporting systems that record money entering into the financial system. Funds are smuggled in various ways (such as by mail, courier and body-packing) often to countries with strict bank secrecy laws.

2.2 Fraud involving cross border transactions

Fraud is the deliberate conduct by a person to deceive another person in order to a gain a benefit. There is no limit as to the types of fraudulent schemes or their complexity and sophistication. Fraud involving cross border transactions involves schemes which transfer funds or assets from one jurisdiction to another. Examples may include:

- Fraud schemes such as securities fraud, in which a perpetrator transfers illegal funds from one jurisdiction to another in order to hide the funds;
- Scams through emails in which victims transfer funds to a person in another country;
- Internet scams in which a victim's financial details are hacked and can be used to steal funds from the victim or to be on sold.

While the incidence of the domestic fraud is low, the risk of fraud involving cross border transactions is high[2] and the associated risk of money laundering to the Cook Islands is mainly through fraud committed outside of the Cook Islands.

Fraud is a criminal offence in the Cook Islands under the Crimes Act 1969.

2.3 Terrorism Financing

Terrorism financing involves the collecting and providing of funds for terrorist activity. Terrorist activity has as its main objectives the intimidation of a population, or compelling a government to do something or not to do something, and this is normally achieved through violent and destructive means.

The fundamental aim of terrorism financing is to obtain resources to support terrorist activities. The sums needed to mount terrorist attacks are not always large and the associated transactions are not necessarily complex.

Terrorism financing is a criminal offence in the Cook Islands under the Terrorism Suppression Act 2004.

[2] Page 12 paragraph 1.8 of the Cook Islands National Risk Assessment 2015.

There are two primary sources of financing for terrorist activities. The first involves getting financial support from countries, organisations or individuals. The other involves revenue-generating activities.

- **Financial support**: Terrorism could be sponsored by a country or government and other sources such as individuals and non-profit organisations.
- **Revenue generating activities:** The revenue generating activities of terrorist groups may include criminal acts, and therefore may appear similar to other criminal organisations. Kidnapping and extortion can serve a dual purpose of providing needed financial resources while furthering the main terrorist objective of intimidating the target population. In addition, terrorist groups may use smuggling, fraud, theft, robbery, and narcotics trafficking to generate funds. Financing for terrorist groups may also include legitimately earned income, which might include collection of membership dues/subscriptions, sale of publications, speaking tours, cultural and social events as well as solicitation and appeals within the community. This fundraising might be in the name of organisations with charitable or relief status, so that donors are led to believe they are giving to a legitimate cause. This type of legitimately earned financing might also include donations of personal earnings by terrorist group members.

Transactions related to terrorism financing may look a lot like those related to money laundering. Therefore, strong, comprehensive anti-money laundering regimes are essential to tracking terrorist financial activities.

2.4 Financing of Proliferation of weapons of mass destruction

Proliferation of weapons of mass destruction (WMD) can be in many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long range missiles). Proliferation of WMD financing is an important element and, as withinternational criminal networks, proliferation support networks use the international financial system tocarry out transactions and business deals. Financial support provided to terrorist organisations thatwant to acquire and/or use WMD is also by its nature contributing to the proliferation of WMD.

Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities; or particular sectors, industries interests, or jurisdictions.

Under the Act the Head of FIU (“the Head”) may issue sanctions list(s) which reflect sanctions on individuals, entities or jurisdictions by the United Nations or FATF or both. A reporting institution must be satisfied a customer is not a sanctioned person (natural, legal or legal arrangement). If a customer is resident, located or operating from a sanctioned jurisdiction enhanced due diligence must be applied.

2.5 The financing and facilitating of bribery and other corrupt practices

Criminal proceeds are generated from corruption offences such as bribery, embezzlement, trading in influence, and abuse of functions. Corruption offences are generally committed for the purpose of

obtaining private gain and the proceeds of corruption are often laundered so that they can be enjoyed without fear of detection or confiscation.

Accordingly, corrupt officials and individuals take great pains to disguise their identity and the original source of the funds in order to place funds derived from corruption in the financial system without detection and to purchase assets. Likewise, often in corruption cases, bribe payers tend to disguise the financial link between them and the corrupt officials, including the destination of the funds, using money laundering schemes.

While traditionally the focus of the FATF Recommendations has always been on combating money laundering and terrorist financing, they do also include specific measures which recognise corruption risks, for example, requiring reporting institutions to take action to mitigate the risks posed by politically exposed persons (PEPs).

2.6 Tax evasion

Tax evasion is where a person through illegal or fraudulent means, intentionally avoids paying their true tax liability. Tax evasion often involves the same routes and players as money laundering and enforcement efforts against them are closely interlinked.

The mechanisms by which tax evasion operates can include mechanisms of anonymity which are consistent with those that operate on behalf of traditional organised crime or other forms of financial misconduct.

3. Reporting institutions

3.1 Are you a reporting institution?

An organisation is a reporting institution if it, as a business undertakes specified activities listed in the Regulations. This includes all licensed financial institutions in the Cook Islands such as banks, insurance providers, trustee and corporate service providers and money-changing and remittance business. It also includes other businesses that deal in high value items, such as real estate agents, motor vehicle dealers, jewelers and pearl dealers as well as professionals that provide services such as incorporating entities or managing funds such as lawyers and accountants.

Being a reporting institution does not mean every part of your business must comply with the Act, the obligations only relate to your dealings with a customer if:

- you have an ongoing business relationship with that customer; or
- your customer wants to undertake a one-off transaction of $10,000 New Zealand dollars (or equivalent in foreign currency) or more[3]

[3] If you are a bank or money transfer business you also have obligations in respect of customers sending electronic funds transfers. Please refer to paragraph 5.3 for further detail.

4. Compliance and Risk Assessments

4.1. Internal compliance policies, procedures and controls

4.1.1 Compliance programme

Each reporting institution[4] must have internal policies, procedures and controls (referred to as the "compliance programme") in place necessary to detect financial misconduct and to manage and mitigate the risk of it occurring. For the purposes of this guideline:

- *policies* set out expectations, standards and behaviours in a business;
- *procedures* are more detailed and apply to day to day operations; and
- *controls* are tools that management use to ensure the business complies with policies and procedures.

The policies, procedures and controls you implement must be adequate and effective for your business. They must be sufficiently robust to reasonably address the risks outlined in your risk assessments. The Money Laundering Reporting Officer (MLRO) is responsible for managing the compliance programme.

Your compliance programme may, depending on the size of your organization, cover the following matters:

- An overview of how your business will address the risks identified in your risk assessments and its approach to CDD;
- What customer information/documents you require to conduct CDD and how you will verify this information;
- How your CDD procedures will identify your customers' ultimate principals.
- How you will carry out enhanced due diligence for higher risk customers or transactions, including how you will obtain information related to source of wealth of the customer.
- How you manage the retention of your records, e.g how and where your records will be stored and whether there is a digital retention and disposal schedule to readily identify records to be retained or destroyed;
- How staff should determine if there are grounds for submitting suspicious activity reports, and which positions have responsibility for authorising and submitting suspicious activity reports to the FIU.
- Designating and vetting senior management positions;
- The scope and nature of staff training, e.g identifying certain tasks or duties that may only carried by staff who have had appropriate compliance training, frequency and delivery of that training, etc.

The list above is not exhaustive and you must consider your obligations under the Act and Regulations and how they relate to your business.

[4] A reporting institution may be exempted from this requirement in certain circumstances.

Under section 15 you must (unless the FIU has undertaken an onsite compliance visit in the previous 12 months or you have been exempted from the requirement) review and test your compliance programme to ensure it remains up to date, to identify anydeficiencies and make changes to address them. This should be done on a periodic basis and it is recommended for most reporting institutions this should be conducted every two years.

This review and testing should be undertaken by a person who has experience in anti-money laundering or countering the financing of terrorism or has relevant financial experience in your sector. This could be a person or firm external to your organisation or could be someone internal or from within your group provided they have not been involved in the development, implementation or maintenance of any aspect of your compliance programme.

4.1.2 Money Laundering Reporting Officer (MLRO)

As previously stated the MLRO is responsible for your organisation's compliance programme. Duties of the MLRO will typically include:

- developing, implementing and maintaining internal policies, procedures and controls that comply with the obligations of this Act or managing that process;
- overseeing or facilitating training for staff on financial misconduct
- liaising with the FIU and participating in any enquiries in relation to detection, prevention and prosecution of financial misconduct; and
- providing reports, guidance and other information to the board and senior management on your organisations compliance programme, financial misconduct risks, reports made to the FIU (or other law enforcement or regulatory agency).

A person appointed by your MLRO must be in a senior management position or must have appropriate work experience. The regulations provide that appropriate work experience is having at worked for at least 3 years in your organisation (or in a similar type of organisation) in a role that is appropriate for the duties of the MLRO and accordingly they should have a good degree of familiarity and understanding of your reporting institution's activities, particularly the products and services being offered.

The person appointed as MLRO must be approved by the Head.

You may appoint 1 or more people to be deputy MLRO's to act in the MLRO's absence or to assist the MLRO in their duties.

4.1.3 Staff appointments and training

Under section 16 you must establish policies, procedures and controls for vetting directors, senior managers and any other employee whose role involves duties to ensure compliance with obligations of this Act. Directors and senior managers are in positions where they may be able to influence or override decisions such as taking on new business that may pose financial misconduct risks. Employees can also be sources of risk.

Vetting involves checking someone's background to determine their suitability for the position, making sure the information they have provided you is correct.

In addition under section 17 you must also have policies and procedures in place to train senior managers and employees This training must be focused on all senior management and other key staff whose duties include responsibilities under the Act. This may include independent contractors and frontline staff who deal with or on behalf of customers. This training should relate to:

- understanding the risks of financial misconduct faced by your organisation and your compliance programme;
- their obligations under that compliance programme;
- recognition and handling of activity or information that may give rise to a suspicious activity report;
- their personal liability for failing to report suspicious activity in accordance with internal policies and procedures, including the offence of tipping off; and
- new developments including information on current techniques, methods and trends in financial misconduct.

The method of training may depend on the size of your organisation and its operations but it should include formal sessions, on the job training and if possible external training. New staff should be trained before they begin to deal with customers.

All staff should be periodically informed of any changes to the compliance policies and procedures particular to their jobs. Those who change jobs within the organisation should be given training as is necessary to be up to date with the policies and procedures associated with their new role.

You may want to consider the follow as methods of monitoring staff training and awareness:

- providing employees and other relevant people with a document consolidating information outlining your organisation's compliance programme or policies and procedures relevant to their role;
- requiring employees and other relevant people to acknowledge that they have received and understood the information detailed above;
- recording the training sessions provided, to whom, and the topics covered.

4.1.4 Group policy

You may have overseas branches or subsidiaries. You are required to ensure that any branch or subsidiary outside the Cook Islands takes measures consistent with the Act in that branch or subsidiary.

This is not intended to mean that measures must mirror those in the Act in every detail, rather that the measures should be of equivalent or consistent with those in the Act. In such cases it may be advisable for a reporting institution to consider establishing a group strategy to protect its global reputation and business.

If the law of the jurisdiction in which the branch or subsidiary is carrying on business imposes requirements lower than those set by the Act, that branch or subsidiary should apply the higher

standard. Reporting procedures and the offences to which the host country relates must be adhered to in accordance with local laws and procedures. However if you unable to take any measures in order for your branch or subsidiary to be in compliance with the Act because it is prohibited by the laws of host jurisdiction, you must inform the FIU.

4.2. Risk Assessments

The Act provides that you must assess the risks of financial misconduct for:

- your business;
- a customer with which you are establishing an ongoing business relationship, or undertaking an isolated transaction with; and
- implementing new technologies.

Assessing the risk involves:

- identifying aspects of your business, or customer or new technology that may be susceptible to financial misconduct; and
- considering each of the at-risk areas you have identified and evaluating the likelihood that your business, or technology, will be used for financial misconduct or in relation to a customer will undertake financial misconduct.

4.2.1 Business risk assessment

You understand your business better than anyone else and therefore you are best placed to identify the risks your business faces from financial misconduct, the likelihood of it occurring through your business and to develop appropriate ways to manage and control these risks. When undertaking a risk assessment for your business, you should consider the following:

- nature, scale and complexity of your business's activities;
- your products and services you offer and the way you deliver those products and services;
- the types of customers you deal with; and
- whether you rely on third parties for elements of CDD process.

You should take into consideration typology reports for your business sector and your own experience and knowledge of the risks in your sector.

4.2.2 The nature, scale and complexity of your business activities

- Consider the nature and complexity of your business's activities, for example a large business is less likely to know its customers personally and it could offer a greater degree of anonymity than a smaller business.
- Consider any vulnerabilities in the level of compliance resources available within your organisation.

- Consider any factors that may increase your exposure to the risk of financial misconduct, eg. business volumes, outsourcing aspects of compliance functions, the other professional services or organisations you deal with.
- Consider the jurisdictions your business operates if it conducts activities outside of the Cook Islands and any particular threats or vulnerabilities from those jurisdictions.
- Actively involve all members of senior management in determining risks (threats and vulnerabilities) posed by financial misconduct within their respective areas of responsibility.

4.2.3 Your products and services you offer and the way you deliver those products and services

- Consider the products and services provided by your business, and how those services might be abused for financial misconduct, for example a product or service that allows or favours customer anonymity.
- Consider the characteristics of your products and services and whether there are any increased vulnerabilities such as providing for high volumes of cash to be transacted, bearer instruments, virtual currencies or other untraceable medium.
- Consider how your products and services are delivered to your customers and the extent to which this might increase the risk. Risks are likely to be greater when relationships can be established remotely (non face to face) or when they may be controlled remotely by the customer or whether you have indirect relationships with customers (via intermediaries, pooled accounts, etc).
- The type of product should be considered, higher risk products or services are more likely to be those with high volumes and values; where unlimited third party funds can be freely received and those where funds can be regularly paid to third parties without due diligence on the third parties being obtained.

4.2.4 The types of customers you deal with

- Consider the types of customers your business markets to. For example higher risk customers may include:
    - customers involved in cash-intensive businesses;
    - customers who are politically exposed persons (PEP's), or high net worth individuals;
    - customers that are from, or operate in, a higher risk jurisdiction,
    - customers that use complex business structures that offer no apparent financial benefits;
    - customers whose source of wealth or source of funds cannot be easily verified or where the audit trail seems unnecessarily layered;
    - customers who conduct business through or are introduced by third parties such as laywers, accountants or other professionals those who conduct non face to face business.
- Consider the countries or other jurisdictions from which your customers operate from and whether they are high or low risk in terms of organised crime, corruption and terrorism and

whether they have inadequate frameworks to prevent and detect financial misconduct in jurisdictions where it may have customers.

- Consider customers who may indicate a lower risk, for example customers who are employed and receive a regular source of income from a known source (eg. salaried persons, pensioners, state benefit recipients), customers with whom you have a long term and active ongoing business relationship.

4.2.5 The reliance which is placed on any third party for elements of customer due diligence

- Consider the extent and type of any reliance your business may place on third parties for customer due diligence,
- Consider the quality of the provider for any outsourced functions including reputational issues, previous experiences with the provider, issues with the jurisdictions in which they operate, the results of any audits, assessments or inspections undertaken on them.

Business risk assessments should be reviewed any time there is material change in the operation or activities of your organisation. They should be performed annually if your organisation operates in sector assessed as higher risk in the most recent National Risk Assessment or at least every 3 years for any other reporting institution.

4.3 New technologies

Prior to the launch or implementation of new technology such as products, business practices or delivery methods including new delivery systems, you must assess the risk of financial misconduct in relation to that new technology and take appropriate action to manage the risks. The factors to consider include:

- whether the new technology favours customer anonymity or allows for financial transactions to be undertaken with limited auditability;
- consider any vulnerabilities the new technology may have in relation to criminals or malicious persons accessing or modifying the technology for criminal or malicious purposes;
- where the new technology relies on outside service providers or external experts to implement, operate and support, consider the quality and resourcing of the provider or expert(s).

You should also consider the extent a new technology may impact on your business risk assessment and consider whether it needs to be reviewed and updated.

It is important to note if you are part of a group structure, new products, systems or procedures maybe implemented without material input from the Cook Islands based organisation the obligation under the Act requires you to identify and mitigate any risks arising from the proposed new technology rather than placing a moratorium on new technologies.

4.4 Customer risk assessments

You must also assess the risk of financial misconduct:

- Before or as soon as reasonably practicable after the establishment of an ongoing business relationship; and
- Then on a regular basis after that to ensure the customer's risk profile is up to date; and
- when carrying out an isolated transaction for a customer who has not otherwise established an ongoing business relationship with the reporting institution.

In order to complete a meaningful risk assessment, it is recommended that information should be gathered prior to the assessment, although this is not always possible. Upon completion of the risk assessment any additional information or clarifications should be sought in the event that circumstances remain unclear.

The initial risk assessment of a customer will help determine:

- whether enhanced due diligence (EDD) under section 29 needs to be undertaken; and
- if the customer is establishing an ongoing business relationship the extent to which ongoing monitoring under section 32 may need to undertaken.

You should have regard to all risk factors in relation to the customer including:

- the nature, scale, complexity and location of the customers activities;
- the manner in which you deal with the customer.

4.4.1 The nature, scale, complexity and location of the customer's activities

You should understand and consider risks inherent in the type of customer you are dealing with and the nature of the activities of your customer. This includes the customer's activities outside of your ongoing business relationship, for example if your customer is a domestic PEP whether the nature of their position puts them at higher risk of bribery, corruption or other criminal activity.

You will also need to consider the types of products or services being sought by the customer and whether they are consistent with your knowledge of their activities. You should consider the jurisdictions from which your customer may operate from or reside in.

4.4.2 The manner in which you deal with a customer

You should consider whether your dealings with a customer involves providing any product or service on a non-face to face basis or is able to be controlled by a customer remotely; for example where significant or unlimited funds can be freely received; or where significant or unlimited funds can regularly be paid to third parties without CDD on the third parties being obtained.

Where you rely on a third party for customer due diligence you must still undertake a customer risk assessment on that customer.

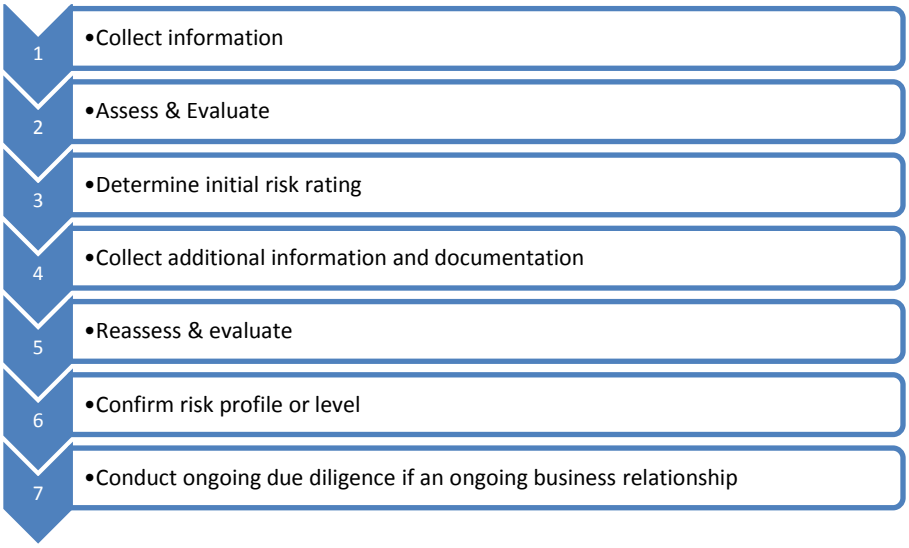
4.4.3 Assessing risk level/profile for customers

It is considered best practice to assess each customer and their risks on a case by case basis and that a "tick box" approach be avoided. While there is no objection to templates or forms being used during the risk assessment, it should be carefully considered how these work, what the "scoring" system is and how the score is reviewed.

As with business risk assessments, customer risk assessments should be reviewed on a regular basis to ensure they remain up to date and assess any changes of the risk profile/level due to changes in a customer's circumstances. Customer risk assessments should be reviewed:

- At least annually for higher risk customers;
- At least every 3 years for other customers; and
- At the point of a material change in a customer's circumstances, eg. establishing connections with a higher risk business or jurisdiction.

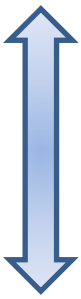
The following diagram sets out a basis customer risk assessment process:



When assessing the risks posed by a customer, the relevant person should consider all risk factors that are known and ensure that all of these factors are included into the customer's risk profile taking care that any mitigating factors are fully documented. An institution must be able to objectively and reasonably justify a risk assessment classification or profile and document those justifications.

4.4.4 Suggested risk profiles or levels

You may use your own categories of risk level or profile provided you can demonstrate a correlation between your categories and those listed below:



Unacceptable risk:	If an institution is not satisfied that the risks identified can be effectively managed the business should be declined.
Higher risk:	CDD must be undertaken and also EDD applies to all higher risk customers. You should also have in place high levels of ongoing monitoring for higher risk customers with which you have an ongoing business relationship .
Standard risk:	CDD must be undertaken and in some cases there may be limited exemption for verification before a transaction is undertaken. There may be further requirements where the customer is a PEP.
Lower risk:	Lower risk customers face the same CDD as standard risk customers or simplified CDD may be undertaken. In addition verification exemptions may apply in some cases where prescribed. Lower risk should be limited to customers who do not present any high risk factors (whether mitigated or not). You must be able to objectively justify that a customer presents a lower than the standard risk. This should be considered on a case by case basis and should not be applied on a general basis (eg. blanket risk assessing on all children's accounts as lower risk).

It is important to remember that if you identify a customer as being of a higher risk of financial misconduct this **does not** automatically mean that a customer is a money launderer or is financing terrorism. Conversely identifying a customer as carrying a lower risk of financial misconduct **does not** mean that the customer presents no risk at all.

If you identify a customer as a higher risk and you are not satisfied that you will be able to effectively manage and mitigate those risks, you should consider the prospective customer to be of "unacceptable risk" and decline from entering into an ongoing business relationship with them or undertaking an isolated transaction. It is important however that you make a decision on "unacceptable risk" customers on a case by case basis rather than wholesale de-risking of business segments or categories of customers.

A reporting institution should consider its own findings from its own business risk assessment and any risk factors identified by the institution should be applied to the profile of the customer.

5. Customer due diligence and record keeping

5.1 Customer due diligence (CDD)

Customer due diligence or CDD encompasses knowing who your customer is. It involves obtaining, documenting and using a broad range of information to know who your customer is and whether they are legitimate. Under the Act there are three types of CDD depending on your customer and the types of transactions they undertake. They are standard CDD, simplified CDD and enhanced CDD.

5.1.1 Who should CDD be conducted on?

CDD must be conducted on:

- a customer; and
- an ultimate principal of a customer; and
- any person acting on behalf of a customer

It is important to remember a customer can be a natural person (individual) or a legal person or a legal arrangement. A customer may be more than 1 person, particularly in relation to legal persons. For example if a reporting institution knows that person A is conducting a transaction on behalf of person B, then person A and B should be identified and verified along with any ultimate principals

You are also required to conduct CDD on a person acting on behalf of a customer. Acting on behalf of a customer is when a person is authorised to carry out transactions or activities on behalf of the customer, examples may include:

- A person with authority to sign, amend account holder details, transfer or spend in the customers name
- A person granted authority because they are the legal guardian of a minor
- An employee of the customer who undertakes daily banking duties for the customer
- A person who is authorised to use a password (or similar) to log in to an account or facility held by the customer (e.g. internet or mobile banking)

A person making a deposit into the account of an unrelated customer (e.g. paying for goods provided by the customer) would not be considered to be acting on behalf of the customer however a person making a deposit of the customer's funds under instruction from the customer is acting on behalf of the customer.

5.1.2 What is an ultimate principal?

An ultimate principal (also known as the beneficial owner) is a natural person who:

- has effective control of a customer or on whose behalf a transaction is conducted:
- ultimately owns or controls 25% or more of the shares or voting rights of customer.

Ultimate principals apply primarily to customers who are legal persons or legal arrangments. A customer's ultimate principal is not necessarily one individual, there may be several ultimate principals in a structure. Your task is to identify and verify the identity of all the ultimate principals of your customer.

To do this you will need to understand the ownership and control structure of your customer. Your customer may have complex ownership or control structures, for example it is possible for ownership to be split into parcels of 25% of less, but relationships between parties may give an individual aggregated ownership of amounts greater than 25%.

In other customers for example a co-operative you may find there are a large number of natural persons with less than 25% ownership, but you still need to identify the ultimate principals whom have effective control of the customer.

Also understanding the management and governance structure of your customer will assist you to establish those persons with effective control, for example

- Those individuals with the ability to control the customer and/or dismiss or appoint those in senior management positions;
- Individuals holding 25% or more of the customers voting rights
- Individuals like the CEO who hold senior management positions
- Trustees or foundation council members

Identifying ultimate principals of a customer is an obligation that must be satisfied regardless of the level of risk associated with that customer, however you make a risk based approach in verifying ultimate principals to determine what reasonable steps to take to satisfy yourself that the customers identity and information is correct.

For example a well known local family business wants to become your customer. You must first identify the customer and the ultimate principals and obtain standard identification documents such as passports. Your risk assessment may lead you to treat this customer as low risk. You may decide that a check in the local business directories, combined with your local knowledge are reasonable steps. Alternatively you could treat the customer as higher risk in which case you should apply enhanced CDD.

If a customer is a legal arrangement or similar (for example a foundation), the ultimate principals are the trustees and any other person who exercises effective control over the legal arrangement including through a chain of control or ownership. Depending on the trust this may include any individual who has influence over the management of the trust, specific trust property or with the power to amend the trust's deeds, or remove or appoint trustees. This might include a protector or special trustee (if there are any).

Where a blind trust or a dummy settlor is used, this places an obligation on the relevant person to identify the individual who gave the instructions to form the legal arrangement and any person funding the establishment of the arrangement

It is important that reporting institutions take a purposive approach in identifying ultimate principals, that is remembering what the Act is trying to achieve and that the fundamental obligation is knowing who your customer is and understanding a person's role and powers in relation to a customer is the more important factor to consider rather than a person's title or position.

5.1.3 When should CDD be conducted?

All CDD procedures must be conducted before or during the formation of the ongoing business relationship or isolated transaction (this includes a series of transactions that appear linked), or if you consider there is a suspicion of financial misconduct or aserious offence. Only in the circumstances as set out in section 28, can the verification of identity be undertaken following formation of the ongoing business relationship.

If you cannot satisfy the relevant CDD requirements or you identify the customer (or any of the customer's ultimate principals) as being a person or entity listed by the UN Security Council[5], you must not proceed with the ongoing business relationship or isolated transaction and you must consider making a suspicious activity report to the FIU.

If you consider that undertaking CDD procedures or terminating the business will tip off the customer you are not required to do so but you must make a suspicious activity report to the FIU within 24 hours.

5.1.4 Standard CDD

Standard CDD involves the collection of identity information of the customer (including any ultimate principals of the customer) or any person acting on behalf of the customer. The regulations set out the kinds of identity information that you must obtain.

It also involves obtaining information on the intended nature and purpose of the ongoing business relationship or isolated transaction, taking steps to identify the source of funds, ensuring any person purporting to act on behalf of a customer has the authority to do so and confirming the customer is not a person or entity sanctioned by the UN Security Council.

In addition if your customer is a legal entity or a legal arrangement you must be satisfied that you know or understand:

- who the ultimate principals of the customer are[6],
- what is its legal status, for example it is a corporation or a partnership, do you have proof of existence?;
- the nature of the customers activities, for example what it is that their business does and jurisdictions they operate;
- the ownership and control structure of the customer, including any group ownership or connected entities where applicable,for example, whether the customer is a subsidiary of another entity and the organisation and management structure of the customer, and
- the powers that regulate and bind the customer which may include, but are not limited to:
    - the memorandum and articles of association (or similar type of documents) for a company
    - in the case of a partnership, a copy of the partnership agreement
    - in the case of a trust, the trust deed
    - in the case of a foundation, the foundation rules

[5] The UN Security Council Resolutions on sanctioned persons and entities are published by the FIU on their website or otherwise circulated by the FIU.
[6] Ultimate principals are discussed further at paragraph 5.1.2

- the constitution of an incorporated association,

The Financial Transactions Reporting Regulations set out additional requirements that must be undertaken in relation to legal arrangements or foundations (Regulation 6). A reporting institution must identify and take reasonable steps to verify trustees (if not already done so), any other person with the power to direct the customers activities, the settlor or such other person on whose instructions the legal arrangement was formed and known beneficiaries[7].

Further requirements relating to life insurance beneficiaries are also prescribed.

5.1.5 Simplified CDD

Simplified CDD can be conducted on customers you have identified as low risk. Any time you identify a customer as low risk you must document how you reached that risk rating. You must still obtain identity information as set out in the regulations and verify that information as well as obtain information on the intended nature and purpose of the ongoing business relationship or isolated transaction. Generally simplified CDD relates to customers that are already subject to transparency and public disclosure. For example simplified CDD may be undertaken on customers listed on a recognized stock exchange.

5.1.6 Enhanced CDD

Enhanced CDD must be conducted in a number of specific situations as set out in section 29 of the Act. Enhanced CDD requires the collection and verification of the same information as standard CDD as well as taking reasonable steps to establish the source of wealth of the customer (and any ultimate principal of that customer). You must also consider whether additional identity information should be obtained.

Source of wealth is concerned with the origins of a customers financial standing or net worth, that is those activities which have generated a customer's funds and property as opposed to source of funds as being concerned with the funding of the business relationship or transaction. An institution must take reasonable steps to obtain sufficient information about the source of wealth or income for all foreign PEPs and higher risk domestic PEPs.

5.1.7 Politically exposed persons (PEPs)

You must assess all customers to identify whether they are a PEP. A PEP is the term given to the risk associated with providing financial and business services to those with a high political profile or who hold public office. Being a PEP does not automatically mean the person is of high risk profile/level. However being entrusted with a prominent public function does mean that the person is likely to have a greater exposure to bribery and corruption.

Additional obligations are required for foreign PEPs and high risk domestic PEPs, such as enhanced CDD being conducted as well as senior management approving the establishment or continuation of any ongoing business relationship or isolated transaction.

[7] Known beneficiaries do not include beneficiaries of a discretionary trust, charitable trust or a trust with 10 or more beneficiaries (or similar types of foundations). In dealing with these types of trusts a reporting institution must obtain sufficient information on the class or characteristics of the beneficiary to ensure CDD can be taken before a distribution is made. The object of a charitable trust must also be obtained by a reporting institution,

It should be noted the Act provides a PEP is a natural person who is or has been in the previous 12 month period entrusted with a prominent public function.

5.2 Ongoing customer due diligence and monitoring

Reporting institutions are required to conduct ongoing customer due diligence and monitoring of any ongoing business relationship it has with a customer. This covers the entire relationship including information held and transactions undertaken by a customer.

5.2.1 Transaction monitoring

A reporting institution should know the expected type, volume and value of activities[8] prior to establishing an ongoing relationship in order to monitor for differences and fluctuations.

Possible areas to monitor include:

- The nature and type of the transactions;
- The frequency and nature of a series or patterns of transactions;
- The amount of any transactions, paying further attention to large transactions;
- The geographical origin/destination of a transaction; or
- The parties concerned with a view to ensuring that there are no payments to or from a person or entity listed as sanctioned by the UN Security Council .

You should pay particular attention to transactions which may be considered unusual activity in the circumstances of the customer, making appropriate enquiries to investigate these transactions to identify whether there may be a suspicion of financial misconduct.

You should take note of any changes in the nature of the relationship with the customer over time. This may be where:

- New products or services are entered into;
- New corporate or trust structures are created;
- A change in a customer's employment or other circumstances takes place;
- The stated activity or turnover of a customer increases; or
- The nature, volume or size of transactions increases.

Where the basis of the business relationship changes significantly, you should reassess the customer's risk profile to ensure that the revised risk is accurate and you understand the basis of the ongoing business relationship with the customer.

[8] This forms part of your obligation to understand the nature and intended purpose of the ongoing business relationship.

5.2.2 Due diligence monitoring

Ongoing collection of CDD information is important. You must ensure that any updated CDD information obtained through meetings, discussions or other methods of communication with your customer is recorded and retained with the customers records. The information must also be available to the MLRO.

While reporting institutions are not automatically required to replace identification documents simply because they have expired, it is expected that identification information be accurate, relevant and up to date. Therefore institutions must be satisfied that the information on file meets these criteria. Where identification information previously obtained has changed, for example change in name or address, the revised information must be obtained and according to level of risk be verified.

5.2.3 Frequency of ongoing due diligence

CDD information in respect of ongoing business relationships must be reviewed periodically. The extent of the due diligence should be linked to the risk profile of the customer. To meet the requirements of ongoing due diligence, the following monitoring frequencies are suggested:

- Standard risk customers' CDD information should be reviewed at least every 3 years.
- High risk customers require more frequent intensive monitoring. CDD information should be reviewed at least annually.

All reviews should be completed in a timely manner.

For higher risk customers (including foreign PEPs and high risk domestic PEPs) an institution must consider:

- whether it has adequate procedures or management information systems in place to provide the MLRO and management with timely information, including information on any connected accounts or relationships;
- how it will monitor the sources of funds, wealth and income and how any changes in circumstances will be recorded; and
- conduct an annual independent review of CDD information, activity and transactions.

The use of cash, monetary instruments or bearer negotiable instruments ("BNIs") as a means of payment or method to transfer funds can pose a higher risk of financial misconduct than other means like electronic funds transfers or cheque. Where cash, monetary instruments or BNI transactions are being proposed by a customer and such requests are not in accordance with the customers known practice, you should make further enquiries.

It is important to remember if you consider activity as suspicious, or you have knowledge of financial misconduct, you must not unquestioningly carry out instructions as issued by the customer. When faced with unreasonable customer instructions that lead an institution to know or suspect financial misconduct, that institution must make a suspicious activity report to the FIU.

5.2.4 Verification of information

A reporting entity is required to verify the identity information obtained by standard CDD, simplified CDD and enhanced CDD. Verification must be done on the basis of documents, data or information issued by a reliable and independent source.

In a standard CDD situation you must, according to the level of risk involved, take **reasonable steps** to verify the information obtained so that you are satisfied you know who the customer is (at all levels) and where a person acts on behalf of a customer, that the person has authority to act on behalf of the customer. Methods to verify information for different customer types include:

For a natural person[9]:

- a certified copy of a valid and current photographic identification document (such as a passport or driving licence) issued by a government agency; and
- a copy of a recent rates, tax or utility bill (except a mobile telephone bill) that shows the person's name and permanent residential address; or
- a copy of a bank statement showing the person's name and address where the customer has maintained a relationship for at least 12 months; or
- a copy of other independent source document that shows the person's name and residential address.

For a legal person:

- a certified copy of the certificate of incorporation, or registration, or organisation, or other similar type document; and
- a copy of the register of directors, or council members, or member or partners; and
- a copy of the memorandum and articles of association; articles of organisation, limited liability company reports, partnership agreement, or other similar type documents; and
- a copy of recent rates, tax or utility bill that shows the legal person's name and mailing address or place of business; or
- a copy of the legal person's most recent annual return
- copies of audited financial statements which shows the legal person's name, directors and registered address; and

For a trust:

- a certified copy of the trust deed (or relevant extracts of trust deed) registration or instrument evidencing or by which the trust was established; and
- a certified copy of a recent bank statement which shows the trustees mailing address (if applicable); and

For a foundation:

- a certified copy of the certificate of registration, the register of council members and the register of ultimate principals, and the foundation instrument and foundation rules; and
- verification documents for the founder, council members and ultimate principals; and
- verification document in respect of each beneficiary upon making a payment from the foundation where the foundation does not have a charitable purpose.

[9] This includes ultimate principals and a person acting on behalf of a customer.

In a simplified CDD situation you must, according to the level of risk involved, verify the identity of the customer and where a person acts on behalf of a customer, that the person has authority to act on behalf of the customer so that you are satisfied you know who the person is and that the person has authority to act on behalf of the customer.

There is no 'reasonable steps' requirement for simplified CDD. When performing simplified CDD, as compared with standard CDD, a reporting entity must still reach the threshold of being 'satisfied' that you know who the customer is and where a person acts on behalf of a customer, that the person has authority to act on behalf of the customer.

5.2.5 Certification of documents

Use of an independent suitable certifier guards against the risk that a hard copy document is not a genuine copy and in the case of identity documents that it corresponds to the customer whose identity is being verified. However for certification to be effective, the certifier will need to have sighted the original documentation and have met the individual face to face. Where a staff member meets a customer face to face they can certify the document otherwise for non face to face business suitable certifiers include:

- a member of the judiciary, justice of the peace, or court registrar;
- an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity;
- a lawyer or notary public, who is a member of a recognised professional body;
- an accountant who is a member of a recognised professional body;
- a serving police officer, or principal of a school;
- a manager or other senior officer within the reporting institution's financial services group.

The certifier should sign and date the copy document (printing his/her name clearly underneath), clearly indicate his/her position or capacity and provide contact details. The certifier should check any photograph on the basis that it represents a good likeness of the customer and state that it is a true copy of the original.

A scanned copy of a certified document (i.e where a document has been certified in hard copy and is then scanned and emailed to the relevant person) is acceptable, however a reporting institution should take a risk based approach to satisfy itself that the documents received adequately verify that the customer is who they say they are and that the institution is comfortable with the authenticity of the documents. A reporting institution should check the type of file and ensure it is tamper resistant, it should check the email address it is being received from to ensure it appears legitimate and relates to the customer sending the document.

5.2.6 Use of electronic documents

Independent data sources can be used to electronically verify a customer's identity and address - by being used to verify that the documents are authentic, however they will not necessarily verify that the customer says who they are.

Independent electronic data sources can provide a wide range of confirmatory material without involving a customer. You should have an understanding of the depth, breath and quality of the data accessed. The sources that are often used by electronic systems include the passport issuing office, driving licence issuing authority, companies registry, the electoral roll and other electronic databases. If an institution intends to use electronic data sources supplied by commercial agencies it should satisfy themselves that the agency:

- Uses a range of positive information sources that can be called upon to link a customer to both current and historical information;
- Accesses negative information sources such as databases relating to fraud and deceased persons;
- Accesses a wide range of alert data sources; and
- Has transparent processes that enable a reporting institution to know what checks have been carried out, and what the results of the checks are.

5.3 Electronic funds transfers and correspondent banking due diligence

(The requirements under subpart 2 of Part 3 of the Act only apply to reporting institution that undertake banking business, or money or value transfer services, or other similar arrangements)

5.3.1 Electronic funds transfers

The definition of electronic funds transfers (EFT) covers all transactions to transfer funds by electronic means. Electronic transactions made on behalf of customers that are accompanied by payment instructions are EFT's where the payment is to be made to an account, facility or other arrangement at another institution. Under the Act transactions that involve the use of debit cards or credit cards are not EFTs if the debit or credit card number accompanies the transaction, transfers and settlements between financial institutions (if both are originator and the beneficiary acting on their behalf) are not EFTs.

If you undertake banking business or money transfer services you are required to develop and implement policies and procedures for your respective capacity as an ordering institution, intermediary (if applicable) and beneficiary institution. These procedures should ensure that reporting institutions include required originator and beneficiary information in payment messages.

Customer due diligence requirements for EFTs are designed to enable information on parties to an EFT be immediately available so as to hinder anonymous use and misuse of EFTs.

As an ordering institution you must identify and verify an originator before conducting an EFT greater than $1500 or undertake CDD procedures in accordance with section 25 if not already done so. You must also ensure cross-border EFTs are accompanied by the required originator and beneficiary information, dependent on the value of the EFTs.

Domestic EFTs may only include the account number or unique transaction reference if it permits audibility back to the originator and beneficiary and this information can be obtained within 3 working days.

For intermediary institutions you must ensure that all information that accompanies an EFT is retained and take reasonable measures which are consistent with straight-through processing, to identity cross-border electronic funds transfers that lack the required originator or beneficiary information.

As a beneficiary institution you must identify and verify beneficiaries for EFTs more than $1500 if you have not already done so. In addition you must also take reasonable measures, including post-event monitoring or real time monitoring where feasible, to identify electronic funds transfers that lack originator or beneficiary information

Both intermediary and beneficiary institutions are required to have policies, procedures and controls in place for determining controls for determining—

- when to execute, reject or suspend an electronic funds transfer lacking required originator or beneficiary information; and
- the appropriate follow-up action.

5.3.2 Correspondent banking due diligence

Correspondent services is the provision of banking or money transfer services by one institution in one jurisdiction to another institution in another jurisdiction. Used throughout the world, correspondent accounts enable banks providers to conduct business and services that the institution does not directly offer.

Before entering into an ongoing business relationship or an isolated transaction involving correspondent services, you must ensure:

- you have assessed the suitability of the respondent institution, including obtaining sufficient information about the nature of its business, its reputation, quality of supervision and whether it has been subject to regulatory action[10]; and
- you have assessed the respondent institution procedures and controls in respect of financial misconduct and determined that they are adequate and effective; and
- ensured that senior management considers and approves an ongoing business relationship with the institution; and
- understood and documented the responsibilities of each institution in their ongoing business relationship.

If you open an account for use by a customer from a respondent institution (payable-through account), you must be satisfied that the respondent institution has customer due diligence procedures in place which are consistent with the requirements of this Act with respect to each person having direct access to the account and that it will provide the relevant evidence of the customers identity upon your request.

You must also ensure that your accounts cannot be utilised by shell banks through the relationship.

[10] From publicly available sources

5.4. Record Keeping

Record keeping is an essential component of the audit trail procedures under the Act. To comply with the requirements of the Act, the records you are required to prepare and maintain should be such that the following can be ascertained:

- The requirements of the Act have been met including:
  - Compliance programme including staff training, review and assessment of your compliance programme;
  - Documentation of risk assessments and the basis for risk profiles;
  - Customer due diligence, including ongoing due diligence and monitoring;
  - Reporting on financial transactions; and
  - Reports made to the FIU in relation to suspicious activity.
- Supervisors, auditors and law enforcement agencies are able to assess the effectiveness of the institutions compliance regime;
- Any transactions or instructions effected via the reporting institution can be reconstructed;
- The trail for funds entering and leaving the Cook Islands is clear;
- The details and records of any customers can be properly identified and located;
- A CDD profile can be established for all customers for whom there is an ongoing business relationship;
- A reporting institution can satisfy, within a reasonable time frame, any enquiries or directions from the appropriate authorities as to disclosure of information;
- Disaster recovery procedures relating to retrieval of records are established and periodically reviewed.

5.4.1 Customer and transaction records

The Act require reporting institutions to keep a copy of documents obtained in relation to customer due diligence and transactions.

CDD records include any customer files and correspondence relating to the ongoing business relationship or an isolated transaction.

Records relating to verification of identity must comprise the evidence itself or a copy of it and if that is not readily available, information about where to obtain a copy must be retained. If an institution relies on an intermediary for CDD, the institution must ensure the intermediary is aware of the record keeping requirements.

Records for isolated transactions must comprise of copies of the CDD and the transaction details (including originator information) that allows the reconstruction of:

- identification information;
- account files;
- business correspondence;
- results of any analysis undertaken.

To satisfy this requirement reporting institutions should consider keeping records of the following transaction details:

- The volume of funds through the account/turnover of client/entity;
- The origin of the funds;
- The form in which the funds were offered or withdrawn, i.e cash, cheque, etc
- The identity of the person undertaking the transaction;
- The destination of the funds;
- The form of instruction and authority;
- The name and address (or identification code) of the counter party;
- The property dealt in, including price and size;
- Whether the transaction was a purchase or a sale;
- The account details from which the funds were paid (including, in the case of cheques, bank name, sort code, account number and name of account holder);
- The form and destination of payment made by the business to the customer;
- Whether the investments were held in custody by the business or sent to the customer or to his/her order and, if so, to what name and address;
- Activities of the client entity;
- Any large item/exception reports created in the course of transaction monitoring.

All records relating to customers and transactions must be kept for at least 6 years (from the transaction date or end of ongoing business relationship), and if those records are subject to an investigation until such time as FIU authorises their disposal.

Records may be kept electronically with the appropriate security, back-up and recovery procedures and must be in English (or be able to be translated into English) and they may be kept outside the Cook Islands as long as those records can be produced in the Cook Islands without significant delay (and in all cases within 3 days) after a request has been made by a competent authority.

5.4.2 Other records

A reporting institution must also establish a register which contains a copy of:

- every report to FIU of suspicious activity; and
- any other report required to be made to FIU; and
- a copy of every enquiry made of it by a competent authority (in the Cook Islands or elsewhere) or law enforcement body that relates to financial misconduct.

These records must be kept for at least 6 years after the date on which the reports were made.

6. Financial Transaction Reporting

6.1 Financial Transaction Reporting

You must report to the FIU certain financial transactions. They are:

- any transactions of cash valued at $10,000 NZD or over; and
- all electronic funds into and out of the Cook Islands regardless of amount[11].

Cash transactions must be reported within 3 working days after the transaction has been made.

Electronic funds transactions are to be reported electronically in batches within 5 working days after the transaction has been made, at the end of that period. The reporting obligations in respect of electronic funds transfer only relate to reporting institutions that undertake banking business or money transfer services business.

The manual reporting form in respect of cash transactions is at **Appendix 1.**

The manual reporting form in respect of electronic funds transfer (or similar) is at **Appendix 2.**

The batch reporting form in respect of cash transactions is at **Appendix 3.**

The batch reporting form in respect of electronic funds transfers (or similar) is at **Appendix 4.**

6.2 Suspicious Activity Reports

6.2.1 Who must report suspicious activity?

Suspicious activity in the course of an ongoing business relationship, transaction or intended transaction must be reported to the FIU. You are required to report suspicious activity within **2 working days** of the suspicion arising unless the activity involves a person of interest in which case you must report within **24 hours.**

A supervisory body or auditor of a reporting institution is also required to report suspicious activity it identifies in their dealings with a reporting institution, if that reporting institution has not reported it. It is important to document any reasons why you may not have made a suspicious activity report.

A suspicious activity report may be made in person or by telephone to the FIU however you must still submit a written report within 24 hours of the oral report.

The reporting form in respect of suspicious activity is at **Appendix 5.**

You may be required to conduct further reporting of any subsequent activity by the customer as well as providing additional information to the FIU when requested.

6.2.2 What is suspicious activity?

The Act defines suspicious activity as meaning any activity or information that:

- relates to 1 or more of the following:
    - an intended transaction:
    - a transaction, whether or not complete:

[11] However it does not include transactions between reporting institutions.

- an ongoing business relationship; and
- is something that cause the reporting institution to:
  - know or suspect that financial misconduct or a serious offence is intended or has occurred; or
  - have reasonable grounds to suspect that financial misconduct or a serious offence is intended or has occurred

Knowledge of financial misconduct is when actual knowledge is possessed by the reporting institution.

Suspicion is the subjective test a reporting institution should apply. It is something more than a fanciful possibility – it is more than a vague unease. However concerns should be justified by the existence of facts even if those facts do not prove that financial misconduct is occurring or has occurred. Typically suspicion will arise when something unusual is noticed and subsequent investigation continues to produce unusual or contradictory facts.

Reasonable grounds for suspicion of financial misconduct are facts which if presented to a reasonable person, that person would reach the conclusion that financial misconduct could be occurring or has occurred. “reasonable grounds to suspect” is determined by what is objectively reasonable in the reporting institutions circumstances, including normal business practices and systems within the institution.

6.2.3 Identifying suspicious activity

It is important to note that there is no monetary threshold for making a report for suspicious activity. An activity may not necessarily involve a transaction. Suspicious activity may involve several factors that may on their own seem insignificant, but together may give reasonable grounds for knowing or suspecting.

The context in which the activity occurs is a significant factor in giving rise to suspicion. This will vary from business to business and from one customer to another. A reporting institution should evaluate the activity in terms of their risk assessments, including normal business practices and knowledge of the customer.

An assessment of suspicion should be based on reasonable evaluation of relevant factors, including the customer risk profile/level, knowledge of customers business, their financial history, previous behavior, adverse press or publicity. All circumstances surrounding the activity should be reviewed.

Indicators are provided in the appendices to help assess whether or not transactions might give rise to reasonable grounds for suspicion. They are examples of common and industry-specific circumstances that may be helpful in evaluating activity. They include indicators based on certain characteristics that have been linked to financial misconduct in the past.

The indicators were compiled in consultation with international financial intelligence organisations and are not intended to cover every possible situation. A single indicator is not necessarily indicative of reasonable grounds to know or suspect, however if a number of indicators are present during the activity then a reporting institution will need to scrutinise the activity with determining whether the activity should be reported. Taken together, the presence of one or more indicators as well as knowledge of the customers business affairs may help in identifying suspicious activity.

Indicators to help establish a suspicion of activity that is related to the commission of terrorist financing offences most resemble those that relate to money laundering although the amounts related to terrorist financing may be of smaller amounts.

As part of the international effort to combat terrorism, the United Nations Security Council publishes lists of organisations and individuals suspected of involvement in terrorist activities. The updated list for use by anyone is available on the FSC website or can be obtained from the Head.

If a reporting institution suspects that activity by a customer relates to terrorist financing then a suspicious activity report should be made to the FIU.

A reporting institution is required to maintain enhanced due diligence and scrutinise the activity of persons of interest and immediately make suspicious activity reports when required

Examples of common indicators are at **Appendix 6.**

Examples of industry specific indicators are at **Appendix 7**.

6.2.4 Tipping Off

Tipping off occurs when a person working within a reporting institution or in connection with a reporting institution discloses that there is suspected activity, or that report has been, or an investigation is underway following a report. Section 38 provides that a monitor or a person connected to a monitor must not tip off in the circumstances which include:

- that knowledge or suspicion;
- that a report under this Act has been, or may be made to the FIU;
- that other information required under this Act has been, or may be given to the FIU;
- the contents or likely contents of any report under this Act relating to that suspicious activity;
- information that might identify any person who has:
  - handled that suspicious activity:
  - prepared any report regarding that suspicious activity:
  - provided any information to the FIU regarding that suspicious activity.

7. Other legislative requirements

7.1 Prohibitions

7.1.1 Opening accounts in false names

You must not open or operate an account for any person that is anonymous (which includes numbered accounts) or is in a name that you know or has reasonable cause to suspect is fictitious.

7.1.2 Shell banks

A shell bank is a bank incorporated in a jurisdiction in which it has no physical presence and which is not affiliated with a financial services group which is subject to effective consolidated supervision.

You must not have dealings, enter a transaction, or have or continue relationships with a shell bank. If you conduct banking business the prohibition on correspondent relationships with shell banks under section 46 of the Banking Act 2011 also applies to you.

7.1.3 Concealing identity through nominee arrangements

All persons are required to disclose to a reporting institution if they are acting in a nominee or trustee capacity when dealing with that institution. It is an offence for any person to deal with a reporting institution in a way that conceals any other persons identity that is required under this Act to under CDD, or to allow a person to undertake a financial transaction to facilitate financial misconduct.

If you consider any person is acting in breach of this, you must conduct enhanced CDD in accordance with section 29. If you still have suspicion you must terminate the business and consider making a suspicious activity report.

7.1.4 Structuring

It is an offence for any person to structure their financial transactions in a way that avoids the requirements of this Act in terms of reporting or CDD.

7.1.5 False or misleading information

It is an offence under the Act for any person to make a false or misleading statement (including omissions) when making a suspicious activity report.

_____

END

Cook
Islands
Financial
Intelligence
Unit

CASH TRANSACTION REPORT (CTR) $10,000 NZD OR MORE

Please complete in **INK** and in **CAPITAL LETTERS**

Reporting of cash transactions of $10,000 NZD or more is required by law under Section 45 of the Financial Transactions Reporting Act 2017. Penalties exist for failure to report or to supply full and correct information.

PART A - IDENTITY OF PERSON CONDUCTING

1 Full name (title, given names and surname)

_____

_____

Also known as: _____

2 Date of birth: _____

3 Country of birth: _____

4 Occupation, business or principal activity

_____

5 Business address (physical and PO Box)

_____ PO Box: _____

_____

Country: _____ Phone: _____

6 Residential address (cannot be a PO Box)

_____

_____

Country: _____ Phone: _____

7 NON RESIDENT - Cook Islands contact address

_____

_____

Country: _____ Phone: _____

8 Give details if this person is a signatory to account affected by this transaction

Account Title/Name: _____

Account No. _____ Branch: _____

Financial Institution: _____

9 How was the identity of this person confirmed?

ID Type: _____

ID Number: _____

Issuer: _____

10 Is a photocopy of ID document/s attached?

Yes ☐ No ☐

If more than one person involved please provide same details contained in Sections 1 - 11 for each person, where appropriate, and attach.

PART B - DETAILS OF PERSON/ORGANISATION ON WHOSE BEHALF THE TRANSACTION WAS CONDUCTED (if applicable)

11 Full name of person/organization

_____

12 Business address (physical and PO Box)

_____ PO Box: _____

_____

Country: _____ Phone: _____

13 Occupation, business or principal activity

_____

14 Give details if this person is a signatory to account affected by this transaction

Account Title/Name: _____

Account No. _____ Branch: _____

Financial Institution: _____

PART C - DETAILS OF THE TRANSACTION

15 Date of transaction

☐☐ ☐☐ ☐☐☐☐

DAY **MONTH** **YEAR**

16 Total amount of this transaction (include cash and any other components of the transaction - If a foreign currency is involved, convert the amount to New Zealand dollars)

NZ$ _____ ____

17 If a foreign currency was involved in this transaction, specify:

Foreign Currency _____

Foreign Currency Amount _____

18 Cash paid IN ☐ **19 Cash paid OUT** ☐

Rarotonga Printing 031007B

20 Type of transaction(s) involved

Transfer to another Financial Institution: _____

Travellers cheques _____

Foreign currency _____

Bank cheque _____

Account deposit / withdrawal _____

Bank draft _____

Securities _____

Precious stones/metals/pearls etc _____

Other _____

21 If a cheque / bank draft / money order / telegraphic transfer / transfer of currency or purchase or sale of any security was involved in this transaction, please specify:

Drawer/Ordering Customer: _____

Payee/Favouree/Beneficiary: _____

22 If another financial institution was involved in this transaction, please specify:

Name of financial institution: _____

Branch: _____

Country: _____

PART D - DETAILS OF THE RECIPIENT PERSON/ORGANISATION (if applicable)

23 Full name of person/organization

24 Business address (physical and PO Box)

_____ PO Box: _____

Country: _____ Phone: _____

25 Occupation, business or principal activity

26 Reason for transaction (eg payment for imports)

27 Details of recipient account (if not already provided)

Account Title/Name: _____

Account No. _____ Branch: _____

Financial Institution: _____

PART E - EXPLANATORY NOTES

28 Give details of the nature and circumstances surrounding the transaction if required. PLEASE PRINT IN BLOCK LETTERS.

29 Is additional information attached to this report?

Yes ☐ **No** ☐

Please specify: _____

PART F - REPORTING FINANCIAL INSTITUTION

30 Type of Financial Institution (eg bank)

31 Name of Financial Institution

32 Name of branch or office where transaction was conducted

33 Business address (physical and PO Box)

_____ PO Box: _____

Country: _____ Phone: _____

PART G - FINANCIAL INSTITUTION'S STATEMENT

34 Details of authorised person:

Given names and surname: _____

Job title: _____

Phone: _____ Fax: _____

35 This statement is made pursuant to the requirement to report "significant" cash transactions under Cook Islands laws on the grounds detailed in this report.

Signature of authorised person:

Sign here

Date: ☐☐ ☐☐ ☐☐☐☐ **DAY MONTH YEAR**

36 Financial Institutions internal reference number (if applicable)

Send completed forms to:	For assistance contact:
Head of FIU PO Box 594 Rarotonga	Financial Intelligence Unit Phone: (+682)29182 Fax: (+682)21798 intel@cifiu.gov.ck

Cook Islands Financial Intelligence Unit

ELECTRONIC FUNDS TRANSFER REPORT (EFTR)

Please complete in **INK** and in **CAPITAL LETTERS**

Reporting of electronic funds transfers is required by law under section 46 of the Financial Transactions Reporting Act 2017. Penalties exist for failure to report or to supply full and correct information.

PART A - DETAILS OF THE TRANSACTION

1 Initiating office/branch

2 Date of transmission/receipt

DAY MONTH YEAR

3 Direction of transmission

Into Cook Islands ☐ Out of Cook Islands ☐

4 Transaction reference number

5 Sending institutions details

BIC (where applicable or)

Name of Bank:

City: Country:

6 Receiving institutions details

BIC (where applicable or)

Name of Bank:

City: Country:

7 Date funds available

DAY MONTH YEAR

8 If a foreign currency was involved in this transaction, specify:

Currency

Amount of transaction

PART B - INVOLVED PARTY AND INSTITUTION DETAILS

9 Ordering customer/organisation (SWIFT field 50)

Name:

Occupation, business or principal activity:

Business / Residential address: (physical and PO Box)

PO Box:

Country: Phone:

Account details:

Account Title/Name:

Bank: Branch:

Account Number:

Person who authorised transfer:

Title:

Name:

Position with organisation:

10 Beneficiary customer/organisation (SWIFT field 59)

Name:

Occupation, business or principal activity:

Business / Residential address: (physical and PO Box)

PO Box:

Country: Phone:

Account details: (SWIFT field 57)

Account Title/Name:

Bank: Branch:

Account Number:

Person identified to receive payment (if applicable)

Title:

Name:

Position with organisation:

11 Sender's Correspondent (SWIFT field 53)

Name of Bank:

City: Country:

12 Reciever's Correspondent (SWIFT field 54)

Name of Bank:

City: Country:

Rarotonga Printing 031007C

PART C - ADDITIONAL PAYMENT DETAILS

13 Details of payment

(SWIFT field 70 - Information for the beneficiary customer)

14 Sender to Receiver information

(SWIFT field 72 - Additional information for the receiving institution)

15 Additional information (include Intermediary bank details, related reference number, ordering and beneficiary institutions

(SWIFT field references - related reference number -21, ordering institution)

16 Any other information deemed relevant

17 Is additional information attached to this report?

No ☐ ☐

Please specify: _____

PART D - REPORTING FINANCIAL INSTITUTIONS

18 Type of Financial Institution (eg bank)

19 Name of Financial Institution

20 Name of branch or office where transaction was conducted

21 Business address (physical and PO Box)

_____ PO Box: _____

Country: _____ Phone: _____

PART E - FINANCIAL INSTITUTION'S STATEMENT

22 Details of authorised person:

Given names and surname: _____

Job title: _____

Phone: _____ Fax: _____

23 This statement is made pursuant to the requirement to report suspicious transactions under Cook Islands laws on the grounds detailed in Part E.

Signature of authorised person:

Sign here

Date: ☐☐ ☐☐ ☐☐☐☐

DAY **MONTH** **YEAR**

24 Financial Institutions internal reference number (if applicable)

Send completed forms to:	For assistance contact:
Head of FIU PO Box 594 Rarotonga	Financial Intelligence Unit Phone: (+682)29182 Fax: (+682)21798 intel@cifiu.gov.ck

APPENDIX 3

Batch Reporting Form for Cash Transactions

Section 45 of the Financial Transactions Reporting Act 2017

Enquiries about this Batch Reporting Form

All enquiries regarding this document are to be made to the following:

- Senior Intelligence Officer – intel@cifiu.gov.ck ; or telephone 29 182.

Reporting mode statement

The mode of reporting to the FIU will be by electronic email to the intel@cifiu.gov.ck Each reporting entity will be issued a secure password to allow all batch files to be password protected before being emailed to the FIU for processing anduploading to the database.

1. CTR Reporting

1.1. Report File

A batch of CTRs to be supplied to FIU via EDDSWEB will be composed of a number of logical records organised into a single file. The structure of this file, and of the logical records within it, is discussed in the next sections.

Files containing CTR data should be named according to the following convention:

Syymmdd.nnn

where:

S indicates the type of data in

the file.

yymmdd is the date the file

was created.

nnn sequence number for the specified date starting from 001 each day.

1.1.1. Field Tags

Special alphanumeric tags will be used to denote the starting point of each additional FIU field. All tags are followed by the colon character (:) before the actual field data begins.

1.1.2. Field and Component Separators

Within the CTR batch/flat file, the following set of field and component separators will be used.

Value	Meaning
=<tag field>:	Start of a new tag group e.g. **=P01:**P
:<tag field>:	Start of a tag field value e.g. **:P03:**James Brown
=B01:	Start of a new transaction in the file e.g. **=B01:**SC
=	End of file

1.1.3. Fields to be Provided

M	Mandatory data. Must be supplied.
MI	Mandatory If. Mandatory - if the data is known to, or available to the reporting financial institution at time of reporting. This is also referred to as optional data.

Note that optional tag groups may contain mandatory tags. The intention is that if the group is provided then any mandatory tags within it must be provided.

1.1.4. Field Formats

Field formats will be expressed using the following symbols. These are best shown by the use of examples, as follows.

20x	x stands for a character or a digit. At least one and up to 20 printable characters or digits (including punctuation characters).
4*35x	Up to four lines of up to 35 printable characters each, separated by CS2 separators (see above). It is expected that words would "wrap" (i.e. start on a new line if they cannot fit on the previous), but this is not mandatory.
yyyymmdd	A date expressed as year(y), month(m), day(d).

1.2. CTR File header record

The File header record is mandatory.

M/MI	Tag	Field	Format
M	A01	Header code	HR
M	A02	Financial Institution code	4x
M	A03	Report file id	10x

Notes

A02 Financial Institution code

Contact the FIU for the financial institution code.

A03 Report file id

The value of this code must be unique amongst all files provided by the Financial Institution. In the header record of an Electronic Input File (from a Financial Institution) the code will have the format xyymmddnnn, where:

x is S (i.e. a CTR file)

yymmdd is the date of extraction of the data

nnn is the sequence number for that date (starting with 001).

1.3. CTR Report Header Details

This mandatory block describes the CTR it precedes, and has the format described below.

M/MI	Tag	Field	Format
M	B01	Report origin code	2x
M	B02	Financial institution report reference	20x

Notes

B01 Report origin code

Code indicating the type and origin (i.e. electronic or manual entry) of the report.

Value	Meaning
SC	Electronic CTR

B02 Financial Institution report reference

Reference number allocated to the report by the financial institution. This reference should be unique within the financial institution.

1.4. Branch Details

M/MI	Tag	Field	Format
M	M03	Branch BRN Code	20x

Notes

M03 Branch BRN Code

Contact FIU for the Branch BRN Code.

1.5. Transaction Details

M/MI	Tag	Field	Format
M	M07	Transaction Type	2x
M	M09	Transaction Date	yyyymmdd

M	M10	Transaction Amount	18x
MI	M20	Transaction Reason	5*60x
MI	M21	Transaction Explanation	5*60x
MI	N04	Foreign Currency Amount	15x

Notes

M07 Transaction Type

If Cash Paid IN

Use the following code values for transaction type.

Value	Meaning
AD	Account deposit
AT	Transfer to domestic Bank
IP	International purchase foreign Currency
IT	International money transfer
OI	Other cash in
RP	Repatriation of local Currency
SF	Foreign Currency

If Cash Paid OUT

Use the following code values for transaction type.

Value	Meaning

AF	Transfer from domestic Bank
CD	Bank draft
CW	Withdrawal
EP	Expatriation of local Currency
IF	International money transfer
IS	International sale of foreign Currency
OO	Other cash out
PF	Foreign Currency

1.6. Party Details

At least one occurrence of this group is **mandatory**. The party details record gives details of customers involved in the transaction. Although most tags are marked as optional as many details as practical should be provided.

M/MI	Tag	Field	Format
M	P01	Party Code	1x
M	P03	Name	2*70x
M	P04	Business Address	4*35x
M	P08	Business Country	35x
MI	P11	Business Occupation	30x
M	P12	Date of Birth	yyyymmdd
M	P13	Account Branch Number	20x
M	P14	Account Number	20x
M	P16	Account Title	70x
M	P17	Identification Number	20x
M	P18	ID Issuer	30x
M	P19	ID Type	1x
M	P23	Business Address Phone	20x
M	P24	Country of Birth	35x
M	P30	Residential Address Street	4*35x
M	P34	Residential Address Country	35x
M	P35	Residential Address Phone	20x
M	P40	Postal Address Street	4*35x
MI	P50	Temporary Domestic Address Street	4*35x
MI	P54	Temporary Domestic Address Country	35x

MI	P55	Temporary Domestic Address Phone	20x

Notes

P01 Party Code

Use the following code values for party code.

Value	Meaning
P	Person conducting the transaction (Agent).
Q	Person on whose behalf transaction is being conducted (Owner).
W	Other person mentioned on a CTR .
T	Recipient person who receives the Cash.

P13 Account Branch Number

Contact FIU for the Branch BRN Code.

P19 ID Type

Use the following code values for ID type.

Value	Meaning
A	Account
B	Date of Birth
C	Credit/Debit card
D	Driver's License
E	Country of Birth
K	Institution Branch
L	Other Branch
M	Miscellaneous
N	Company Number
O	Other ID
P	Passport

T	Telephone/Fax Number
Z	Bank Identification Code

1.7. Instrument Details

This group is optional. This record describes the cheques, money orders, telegraphic transfer, transfer of currency or purchase (or sale of securities) etc that were used in the transaction. If no instruments are used (i.e. it was a notes and coins transaction), then there will be no instrument detail records.

M/MI	Tag	Field	Format
MI	Q01	Instrument type code	1x
MI	Q02	Drawer name	2*70x
MI	Q03	Payee name	2*70x
MI	Q04	Financial institution name	30x
MI	Q05	Branch name	30x
MI	Q06	Country name	20x

Notes

Q01 Instrument type code

Use the following code values for party code.

Value	Meaning
C	Instrument

1.8. Free Format Text Details (V)

This group is optional. The financial institution can use it to enter any other details relevant to the transaction, or persons involved.

M/MI	Tag	Field	Format
MI	V02	Additional Financial institution text	72x

1.9. CTR File Trailer Record

The File trailer record is mandatory and has the following structure. Each field in the Trailer record is preceded by a tag and each is followed by the separator FS3, except for the last which is followed by BS1.

M/MI	Tag	Field	Format
M	Z01	Header code	TR
M	Z01	No of CTR Reports in this file	6x

2. CTR File Example

A01:HR
:A02:0002
:A03:S140826002
=B01:SC
:B02:FIUTRANS0001
=M03:4-3
:M07:AD
:M09:20140909
:M10:20000
:M20:Cash Deposit
:M21:Salary deposit
=N01:NZD
:N04:15000
=P01:P
:P03:Walter Smith
:P04:123 West Main Road
:P08:New Zealand
:P11:Team Leader Accounts
:P12:19730908
:P13:6-1
:P14:123456
:P16:Walter Smith
:P17:12346
:P18:Land Transport Authority
:P19:D
:P23:679123456
:P24:New Zealand
:P30:123 South Main Road
:P34:New Zealand
:P35:679123456
:P40:P O Box 1234, North Main
:P50:123 Seas Main Road
:P54:New Zealand
:P55:679123456
=P01:Q
:P03:Walter Smith
:P04:123 Main Road
:P05:Auckland

:P08:New Zealand
:P11:Team Leader
:P13:6-1
:P14:123341
:P16:Walter Smith
:P23:21212313
:P30:123 North Road
:P31:Auckland
:P34:New Zealand
:P35:12312313
:P40:123 North Road
=P01:T
:P03:Jane Smith
:P04:564 Main Road
:P05:Auckland
:P08:New Zealand
:P11:Manager HR
:P13:10-1
:P14:131231231
:P16:Jane Smith
:P23:12121331
:P40:PO Box 12132 South Road
=Q01:C
:Q02:Walter Smith
:Q03:Walter Smith
:Q04:ANZ
:Q05:Auckland
:Q06:New Zealand
=V02:Cheque Deposit
=Z01:TR
:Z02:1
=

APPENDIX 4

Batch Reporting Form for Electronic funds transfers

Section 46 of the Financial Transactions Reporting Act 2017

Enquiries about this Batch Reporting Form

All enquiries regarding this document are to be made to the following:

- Senior Intelligence Officer – intel@cifiu.gov.ck ; or telephone 29 182.

Reporting mode statement

The mode of reporting to the FIU will be by electronic email to intel@cifiu.gov.ck. Each reporting entity will be issued a secure password to allow all batch files to be password protected before being emailed to the FIU for processing anduploading to the database.

1. EFTR Reporting

1.1. Report File

A batch of EFTRs to be supplied to FIU via EDDSWEB will be composed of a number of logical records organized into a single file. The structure of this file, and of the logical records within it, is discussed in the next sections.

Files containing EFTR data should be named according to the following convention:

Eyymmdd.nnn

where:

E indicates the type of data in

the file.

yymmdd is the date the file was

created.

nnn sequence number for the specified date starting from 001 each day.

1.1.1. Field Tags

Special alphanumeric tags will be used to denote the starting point of each additional FIU field. All tags are followed by the colon character (:) before the actual field data begins.

1.1.2. Field and Component Separators

Within the EFTR batch/flat file, the following set of field and component separators will be used.

Value	Meaning
=<tag field>:	Start of a new tag group e.g. **=P01:**P
:<tag field>:	Start of a tag field value e.g. **:P03:**James Brown
=B01:	Start of a new transaction in the file e.g. **=B01:**SO
=	End of file

APPENDIX 4

1.1.3. Fields to be Provided

M **Mandatory data**. Must be supplied.

MI **Mandatory If.** Mandatory - if the data is known to, or available to the reporting financial institution at time of reporting. This is also referred to as optional data.

Note that optional tag groups may contain mandatory tags. The intention is that if the group is provided then any mandatory tags within it must be provided.

1.1.4. Field Formats

Field formats will be expressed using the following symbols. These are best shown by the use of examples, as follows.

20x x stands for a character or a digit. At least one and up to 20 printable characters or digits (including punctuation characters).

4*35x Up to four lines of up to 35 printable characters each, separated by CS2 separators (see above). It is expected that words would "wrap" (i.e. start on a new line if they cannot fit on the previous), but this is not mandatory.

yyyymmdd A date expressed as year(y), month(m), day(d).

APPENDIX 4

1.2. EFTR File header record

The File header record is **mandatory**.

M/MI	Tag	Field	Format
M	**A01**	Header code	HR
M	**A02**	Financial Institution code	4x
M	**A03**	Report file id	10x

Notes

A02 Financial Institution code

Contact the FIU for the financial institution code.

A03 Report file id

The value of this code must be unique amongst all files provided by the Financial Institution. In the header record of an Electronic Input File (from a Financial Institution) the code will have the format **xyymmddnnn**, where:

x is E (i.e. a EFTR file)

yymmdd is the date of extraction of the data

nnn is the sequence number for that date (000 to 999).

APPENDIX 4

1.3. EFTR Report Header Details

This mandatory block describes the CTR it precedes, and has the format described below.

M/MI	Tag	Field	Format
M	**B01**	Report origin code	2x
M	**B02**	Financial institution report reference	20x

Notes

B01 Report origin code

Code indicating the type and origin (i.e. electronic or manual entry) of the report.

Value	Meaning
SO	Electronic EFTR

B02 Financial Institution report reference

Reference number allocated to the report by the financial institution. This reference should be unique within the financial institution.

APPENDIX 4

1.4. Transmission Details

M/MI	Tag	Field	Format
M	**C01**	Date of transmission/receipt	yyyymmdd
M	**C03**	Sending Institution Code /BIC Or (C04,C05 and C06 tags (all))	24x
M	**C04**	Sending Institution Name	2*35x
M	**C05**	Sending Institution City/Location	35x
M	**C06**	Sending Institution Country	35x
M	**C07**	Receiving Institution Code /BIC Or (C08,C09 and C10 tags (all))	24x
M	**C08**	Receiving Institution Name	2*35x
M	**C09**	Receiving Institution City/Location	35x
M	**C10**	Receiving Institution Country	35x
M	**C11**	Into/out of Cook Islands flag	1x
MI	**D03**	Additional Information	72x
MI	**D05**	Transaction Reference Number	16x
M	**D07**	Date Funds Available	yyyymmdd
M	**D08**	Currency Code	3x
M	**D09**	Transaction Amount	15x
M	**D10**	Details of Payment	4*35x
M	**D12**	Sender to Receiver Information	6*35x
M	**D13**	Initiating Branch BRN Code	20x

Notes

If you do not provide a Sending institution code (BIC), you need to provide a Sending institution

name, Sending institution city/location and a Sending institution country details.

Similarly, if you do not provide a Receiving institution code (BIC), you need to provide a Receiving institution name, Receiving institution city/location and Receiving institution country.

C11 Into/out of Cook Islands flag

Use the following code values for transaction type.

Value	Meaning
O	EFTR transmitted out of Cook Islands
I	EFTR transmitted into Cook Islands

D13 Initiating Branch BRN Code

Contact FIU for the branch BRN code.

APPENDIX 4

1.5. Ordering Customer Details

M/MI	Tag	Field	Format
M	**E01**	Ordering Customer	70x
M	**E02**	Ordering Customer Business Address	3*35x
M	**E06**	Ordering Customer Business Country	35x
M	**E08**	Ordering Customer Account BRN Code	20x
M	**E09**	Ordering Customer Account Number	34x
M	**E13**	Ordering Customer Business Phone	20x
M	**E14**	Ordering Customer Account Title	2*35x
MI	**E22**	Ordering Customer Occupation	30x
MI	**E30**	Ordering Customer Residential Address	3*35x
MI	**E34**	Ordering Customer Residential Country	35x
MI	**E35**	Ordering Customer Residential Phone	20x
MI	**E40**	Ordering Customer Postal Address	3*35x
MI	**E60**	Authorized Ordering Customer	70x
MI	**E61**	Authorized Ordering Customer Position	30x

Notes

E08 Ordering Customer Account BRN Code

Contact FIU for the branch BRN code.

APPENDIX 4

1.6. Sender's Correspondent Institution Details

M/MI	Tag	Field	Format
M	**G01**	Sender's Institution Code (BIC)	24x
Or			
M	**G02**	Sender's Institution Name and Address	4*35x

Notes

Either the sender's correspondent code (e.g. BIC) or the name and address of the sender's correspondent should be included.

G02 Sender's Institution Name and Address

Separate the following as below:

G02 - Line 1: Name of Bank

G02 - Line 2: City

G02 - Line 3: Country

1.7. Receiver's Correspondent Institution Details

M/MI	Tag	Field	Format
M	**H01**	Receiver's Institution Code (BIC)	24x
Or			
M	**H02**	Receiver's Institution Name and Address	4*35x

Notes

Either the receiver's correspondent code (e.g. BIC), or the name and address of the receiver's correspondent should be included.

H02 Sender's Institution Name and Address

Separate the following as below:

H02 - Line 1: Name of Bank

H02 - Line 2: City

H02 - Line 3: Country

1.8. Beneficiary Customer Details

M/MI	Tag	Field	Format

APPENDIX 4

M	**L02**	Beneficiary Account BRN Code	20x
M	**L03**	Beneficiary Account Number	35x
M	**L04**	Beneficiary Name	70x
M	**L05**	Beneficiary Business Address	3*35x
M	**L09**	Beneficiary Business Country	35x
M	**L11**	Beneficiary Business Phone	20x
M	**L12**	Beneficiary Account Title	2*35x
M	**L22**	Beneficiary Occupation	30x
MI	**L30**	Beneficiary Residential Address	3*35x
MI	**L34**	Beneficiary Residential Country	35x
MI	**L35**	Beneficiary Residential Phone	20x
MI	**L40**	Beneficiary Postal Address	3*35x
M	**L60**	Final Recipient Name	70x
M	**L61**	Final Recipient Position	30x

Notes

L02 Beneficiary Account BRN Code

Contact FIU for the branch BRN code.

APPENDIX 4

1.9. EFTR File Trailer Record

The File trailer record is mandatory and has the following structure. Each field in the Trailer record is preceded by a tag and each is followed by the separator FS3, except for the last which is followed by BS1.

M/MI	Tag	Field	Format
M	**Z01**	Header code	TR
M	**Z01**	No of CTR Reports in this file	6x

APPENDIX 4

2. EFTR File Example

A01:HR
:A02:0003
:A03:E140825009
=B01:SO
:B02:WestEFTR0001
=C01:20140924
:C04:ANZ
:C05:Auckland
:C06:New Zealand
:C08:Westpac
:C09:Avarua
:C10:Cook Islands
:C11:I
=D03:Advise when payment complete
:D05:FIUEFTR001
:D07:20140925
:D08:NZD
:D09:12000
:D10:School Fees
:D12:Pay full amount
:D13:7-1
=E01:John Doe
:E02:1234 West Main Rd
:E06:New Zealand
:E08:3-6
:E09:12345678
:E13:64112345
:E14:James Doe
:E22:Consultant
:E30:1234 South Main Rd
:E34:New Zealand
:E35:64118762
:E40:P O Box 12345 North Rd
:E60:James Doe
:E61:Consultant
=G02:ANZ
=H02:Westpac
=L02:2-1

APPENDIX 4

:L03:125432
:L04:Jane Doe
:L05:1234 Main St
:L09:Cook Islands
:L11:12345
:L12:Jane Doe
:L22:Sales Agent
:L30:14567 Mahi Rd
:L34:Cook Islands
:L35:12353
:L40:P O Box 12345 Main
:L60:Jane Doe
:L61:Sales Agent
=Z01:TR
:Z02:1
=

Cook
Islands
Financial
Intelligence
Unit

SUSPICIOUS ACTIVITY REPORT (SAR)

Please complete in **INK** and in **CAPITAL LETTERS**

Reporting of suspicious activity is required by law under sections 47, 48 and 49 of the Financial Transactions Reporting Act 2017. Penalties exist for failure to report or to supply full and correct information.

PART A - IDENTITY OF PERSON CONDUCTING

1 Full name (title, given names and surname)

_____

_____

Also known as: _____

2 Date of birth:

_____
Day/Month/Year

3 Country of birth:

_____

4 Occupation, business or principal activity

_____

5 Business address (physical and PO Box)

_____ PO Box: _____

_____

Country: _____ Phone: _____

6 Residential address (cannot be a PO Box)

_____

_____

Country: _____ Phone: _____

7 NON RESIDENT - Cook Islands contact address

_____

_____

COOK ISLANDS Phone: _____

8 Give details if this person is a signatory to account affected by this transaction

Account Title/Name: _____

Account No. _____ Branch: _____

Financial Institution: _____

9 How was the identity of this person confirmed?

ID Type: _____

ID Number: _____

Issuer: _____

10 Is a photocopy of ID document/s attached?

Yes ☐ No ☐

If more than one person involved please provide same details contained in Sections 1 - 11 for each person, where appropriate, and attach.

PART B - DETAILS OF PERSON/ORGANISATION ON WHOSE BEHALF THE TRANSACTION WAS CONDUCTED (if applicable)

11 Full name of person/organisation

_____

12 Business address (physical and PO Box)

_____ PO Box: _____

_____

Country: _____ Phone: _____

13 Occupation, business or principal activity

_____

14 Give details if this person is a signatory to account affected by this transaction

Account Title/Name: _____

Account No. _____ Branch: _____

Financial Institution: _____

PART C - DETAILS OF THE TRANSACTION

15 Type of transaction (eg deposit)

_____

16 Date of transaction

☐☐ ☐☐ ☐☐☐☐
DAY **MONTH** **YEAR**

17 Total amount of this transaction (include cash and any other components of the transaction - If a foreign currency is involved, convert the amount to New Zealand dollars)

NZ$ _____ . ____

18 If a foreign currency was involved in this transaction, specify:

Foreign Currency _____
(eg Hong Kong Dollars)

Foreign Currency Amount _____
(eg HKD$400,000)

19 If a cheque / bank draft / money order / telegraphic transfer / transfer of currency or purchase or sale of any security was involved in this transaction, please specify:

Drawer/Ordering Customer: _____

Payee/Favouree/Beneficiary: _____

Rarotonga Printing 070619D

20 If another financial institution was involved in this transaction, please specify:

Name of financial institution: _____

_____

Branch: _____ Country: _____

21 Give details of accounts of any OTHER person(s) / organisation(s) affected by this transaction

Account title: _____

Account type: _____

Bank/Financial Institution: _____

Branch: _____

Account Number: _____

PART D - DETAILS OF THE RECIPIENT

22 Full name of person/organisation

_____

_____

23 Business address (physical and PO Box)

_____ PO Box: _____

_____

Country: _____ Phone: _____

24 Occupation, business or principal activity

_____

25 Reason for transaction (eg payment for imports)

_____

_____

_____

26 Details of recipient account (if not already provided)

Account Title/Name: _____

Account No. _____ Branch: _____

Financial Institution: _____

PART E - GROUNDS FOR SUSPICION

27 Give details of the nature and circumstances surrounding the transaction and the reason for suspicion. (If there is insufficient space, attach a separate sheet). PLEASE PRINT IN BLOCK LETTERS.

_____

_____

_____

_____

_____

28 Is additional information attached to this report?

Yes ☐ **No** ☐

Please specify: _____

PART F - REPORTING FINANCIAL INSTITUTION

29 Type of Financial Institution (eg bank)

_____

30 Name of Financial Institution

_____

31 Name of branch or office where transaction was conducted

_____

32 Business address (physical and PO Box)

_____ PO Box: _____

_____

Country: _____ Phone: _____

PART G - FINANCIAL INSTITUTION'S STATEMENT

33 Details of authorised person:

Given names and surname: _____

_____

Job title: _____

Phone: _____ Fax: _____

34 This statement is made pursuant to the requirement to report suspicious transactions under Cook Islands laws on the grounds detailed in Part E.

Signature of authorised person:

Sign here

Date: ☐☐ **DAY** ☐☐ **MONTH** ☐☐☐☐ **YEAR**

35 Financial Institutions internal reference number (if applicable)

_____

Send completed forms to:	
Head of FIU PO Box 594 Rarotonga COOK ISLANDS	Financial Intelligence Unit Phone: (+682)29182 Fax: (+682)29183 email: intel@cifiu.gov.ck

APPENDIX 6

Examples of Common Indicators

The following are examples of common indicators that **may** point to a suspicious transaction. Please read the guidelines for general information about identifying suspicious transactions and how to use these indicators.

1. **General**

- Client admits or makes statements about involvement in criminal activities.
- Client does not want correspondence sent to their home address.
- Client appears to have accounts with several financial institutions in one area for no apparent reason.
- Client repeatedly uses an address but frequently changes the names involved.
- Client is accompanied and watched.
- Client shows uncommon curiosity about internal systems, controls and policies.
- Client has only vague knowledge of the amount of a deposit.
- Client presents confusing details about the transaction.
- Client over justifies or explains the transaction.
- Client is secretive and reluctant to meet in person.
- Client is nervous, not in keeping with the transaction.
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Client's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after opening account.
- Client is involved in activity out-of-keeping for that individual or business.
- Client insists that a transaction be done quickly.
- Inconsistencies appear in the client's presentation of the transaction.
- Client appears to have recently established a series of new relationships with different financial entities.
- Client attempts to develop close rapport with staff.
- Client uses aliases and a variety of similar but different addresses.
- Client uses a post office box or General Delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
- Client offers you money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious.
- You are aware that a client is the subject of a money laundering or terrorist financing investigation.

2. Knowledge of Reporting or Record Keeping Requirements

- Client attempts to convince employee not to complete any documentation required for the transaction.
- Client makes inquiries that would indicate a desire to avoid reporting.
- Client has unusual knowledge of the law in relation to suspicious transaction reporting.
- Client seems very conversant with money laundering or terrorist financing issues.
- Client is quick to volunteer that funds are clean or not being laundered.

3. Identity Documents

- Client provides doubtful or vague information.
- Client produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Client refuses to produce personal identification documents.
- Client only submits copies of personal identification documents.
- Client wants to establish identity using something other than his or her personal identification documents.
- Client's supporting documentation lacks important details such as a phone number.
- Client inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be checked for some reason.
- All identification documents presented appear new or have recent issue dates.

4. Cash Transactions

- Client starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the client in the past.
- Client frequently exchanges small bills for large ones.
- Client uses notes in denominations that are unusual for the client, when the norm in that business is much smaller or much larger denominations.
- Client presents notes that are packed or wrapped in a way that is uncommon for the client.
- Client deposits musty or extremely dirty bills.
- Client makes cash transactions of consistently rounded-off large amounts (e.g., $9,900, $8,500, etc.).
- Client consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Client consistently makes cash transactions that are significantly below the reporting threshold amount in an apparent attempt to avoid triggering the identification and reporting requirements.
- Client presents uncounted funds for a transaction. Upon counting, the transaction totals an amount just below that which could trigger reporting requirements.

- Client conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Client frequently purchases travellers cheques, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity for the client.
- Client asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.)
- Stated occupation of the client is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

5. Economic Purpose

- Transaction seems to be inconsistent with the client's apparent financial standing or usual pattern of activities.
- Transaction appears to be out of the ordinary course for industry practice or does not appear to be economically viable for the client.
- Transaction is unnecessarily complex for its stated purpose.
- 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.

6. Transactions Involving Accounts

- Opening accounts when the client's address is outside the local service area.
- Opening accounts with names very close to other established business entities.
- Attempting to open or operating accounts under a false name.
- Account with a large number of small cash deposits and a small number of large cash withdrawals.
- Funds are being deposited into several accounts, consolidated into one and transferred outside the country.
- Client frequently uses many deposit locations outside of the home branch location.
- 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.
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.

- Account that was reactivated from inactive or dormant status suddenly sees significant activity.
- Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.
- Unexplained transfers between the client's products and accounts.
- Multiple deposits are made to a client's account by third parties.
- Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.
- Multiple personal and business accounts are used to collect and then funnel funds to a small number of foreign beneficiaries, particularly when they are in locations of concern, such as countries known or suspected to facilitate money laundering activities. More information on which countries these characteristics may apply to, please refer to the Web sites provided in this guideline

7. Transactions Involving Areas Outside the Cook Islands

- Client and other parties to the transaction have no apparent ties to the Cook Islands.
- Transaction crosses many international lines.
- Use of a credit card issued by a foreign bank that does not operate in the Cook Islands by a client that does not live and work in the country of issue.
- Transactions involving countries deemed by the Financial Action Task Force as requiring enhanced surveillance.
- Foreign currency exchanges that are associated with subsequent wire transfers to locations of concern, such as countries known or suspected to facilitate money laundering activities and the financing of terrorism activities.
- Deposits followed within a short time by wire transfer of funds to or through locations of concern, such as countries known or suspected to facilitate money laundering activities and the financing of terrorism activities.
- Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money-laundering system.
- Transaction involves a country known for highly secretive banking and corporate law.
- Transaction involves a country known or suspected to facilitate money laundering activities.

8. Transactions Related to Offshore Business Activity

Any person or entity that conducts transactions internationally should consider the following indicators:

- Accumulation of large balances, inconsistent with the known turnover of the client's business, and subsequent transfers to overseas account(s).
- Frequent requests for travellers cheques, foreign currency drafts or other negotiable instruments.

- Loans secured by obligations from offshore banks.
- Loans to or from offshore companies.
- Offers of multimillion-dollar deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore shell bank whose name may be very similar to the name of a major legitimate institution.
- Unexplained electronic funds transfers by a client on an in-and-out basis.
- Use of letter-of-credit and other methods of trade financing to move money between countries when such trade is inconsistent with the clients business.
- Use of a credit card issued by an offshore bank.

_____

END

APPENDIX 7

Examples of Industry-Specific Indicators

Industry-Specific Indicators

In addition to the common indicators outlined, the following industry-specific indicators may point to a suspicious transaction. Remember that **behaviour** is suspicious, not people. Also, it is the consideration of many factors not any one factor that will lead to a conclusion that there are reasonable grounds to suspect that a transaction is related to financial misconduct.

All circumstances surrounding a transaction should be reviewed, within the context of your knowledge of your client. Taken together, the general and industry-specific indicators that apply to your business may help you identify suspicious activity.

Depending on the services you provide, you may need information about indicators in more than one of the following sections.

1. Financial Entities

Please read general information about identifying suspicious transactions and how to use these indicators.

The following indicators are for your consideration if you are an institution that opens accounts and holds deposits on behalf of individuals or companies. This includes banks, credit unions, trust and loan companies.

<u>Personal Transactions</u>

- Client appears to have accounts with several financial institutions in one geographical area.
- Client has no employment history but makes frequent large transactions or maintains a large account balance.
- Client makes one or more cash deposits to general account of foreign correspondent bank (i.e., flow-through account).
- Client runs large credit card balances.
- Client visits the safety deposit box area immediately before making cash deposits.
- Client wishes to have credit and debit cards sent to international or domestic destinations other than his or her address.
- Client has numerous accounts and deposits cash into each of them with the total credits being a large amount.
- Client deposits large endorsed cheques in the name of a third-party.
- Client frequently makes deposits to the account of another person who is not an employee or family member.
- Client frequently exchanges currencies.
- Client frequently makes automatic banking machine deposits just below the reporting threshold.
- Clients access to the safety deposit facilities increases substantially or is unusual in light of their past usage.
- Many unrelated individuals make payments to one account without rational explanation.
- Third parties make cash payments or deposit cheques to a client's credit card.

- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- Client acquires significant assets and liquidates them quickly with no explanation.
- Client acquires significant assets and encumbers them with security interests that do not make economic sense.

Corporate and Business Transactions

Some businesses may be susceptible to the mixing of illicit funds with legitimate income. This is a very common method of money laundering. These businesses include those that conduct the majority of their business in cash on opening accounts with the various businesses in your area, you would be aware of those that are mainly cash based. Unusual or unexplained increases in cash deposits made by those entities may be indicative of suspicious activity.

- 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, cashiers cheques, money orders or electronic funds transfers, which is inconsistent with the clients business.
- Accounts have deposits in combinations of monetary instruments that are atypical of legitimate business activity (for example, deposits that include a mix of business, payroll, and social security cheques).
- Accounts have deposits in combinations of cash and monetary instruments not normally associated with 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.
- Client maintains a number of trustee or client accounts that are not consistent with that type of business or not in keeping with normal industry practices.
- Client operates a retail business providing cheque-cashing services but does not make large draws of cash against cheques deposited.
- Client pays in cash or deposits cash to cover bank drafts, money transfers or other negotiable and marketable money instruments.
- Client purchases cashiers cheques and money orders with large amounts of cash.
- Client deposits large amounts of currency wrapped in currency straps.
- Client 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.
- Client makes a large volume of cash deposits from a business that is not normally cash-intensive.
- Client makes large cash withdrawals from a business account not normally associated with cash transactions.
- Client consistently makes immediate large withdrawals from an account that has just received a large and unexpected credit from abroad.
- Client makes a single and substantial cash deposit composed of many large bills.
- Small, one-location business makes deposits on the same day at different branches across a broad geographic area that does not appear practical for the business.

- 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.
- Client wishes to have credit and debit cards sent to international or domestic destinations other than his or her place of business.
- 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 client's account.
- Asset acquisition is accompanied by security arrangements that are not consistent with normal practice.
- Unexplained transactions are repeated between personal and commercial accounts.
- Account activity is inconsistent with stated business.
- Account has close connections with other business accounts without any apparent reason for the connection.
- Activity suggests that transactions may offend securities regulations or the business prospectus is not within the requirements.
- A large number of incoming and outgoing wire transfers take place for which there appears to be no logical business or other economic purpose, particularly when this is through or from locations of concern, such as countries known or suspected to facilitate money laundering activities.

2. Businesses who Send or Receive Electronic Funds Transfers

Please read the general information about identifying suspicious transactions and how to use these indicators. If you are involved in the business of electronic funds transfers, consider the following indicators:

- Client orders wire transfers in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Client transfers large sums of money to overseas locations with instructions to the foreign entity for payment in cash.
- Client receives large sums of money from an overseas location via electronic funds transfer that includes instructions for payment in cash.
- Client makes frequent or large electronic funds transfers for persons who have no account relationship with the institution.
- Client receives electronic funds transfers and immediately purchases monetary instruments prepared for payment to a third party which is inconsistent with or outside the normal course of business for the client.
- Client requests payment in cash immediately upon receipt of a large electronic funds transfer.
- Client instructs you to transfer funds abroad and to expect an equal incoming transfer.
- Client shows unusual interest in electronic funds systems and questions limit of what amount can be transferred.
- Client transfers funds to another country without changing the form of currency.
- Large incoming wire transfers from foreign jurisdictions are removed immediately by company principals.
- Client sends frequent wire transfers to foreign countries, but business does not seem to have connection to destination country.

- Wire transfers are received from entities having no apparent business connection with client.
- Size of electronic transfers is out-of-keeping with normal business transactions for that client.
- Wire transfers do not have information about the beneficial owner or originator when the inclusion of this information would be expected.
- Stated occupation of the client is not in keeping with the level or type of activity (for example a student or an unemployed individual who receives or sends large numbers of wire transfers).
- Beneficiaries of wire transfers involve a large group of nationals of countries associated with terrorist activity.
- Client conducts transactions involving 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.
- Client makes electronic funds transfers to free trade zones that are not in line with the clients business or from countries known to have ML or TF problems.

3. Businesses who Provide Loans

Please the general information about identifying suspicious transactions and how to use these indicators. If you are involved in the business of providing loans or extending credit to individuals or corporations, consider the following indicators:

- Client suddenly repays a problem loan unexpectedly.
- Client's employment documentation lacks important details that would make it difficult for you to contact or locate the employer.
- Client has loans to or from offshore companies that are outside the ordinary course of business of the client.
- Client offers you large dollar deposits or some other form of incentive in return for favourable treatment on loan request.
- Client asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known.
- Loan transactions are entered into in situations where the client has significant assets and the loan transaction does not make economic sense.
- Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.
- Client 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 client.

4. Life Insurance Companies, Brokers and Agents

Please read the general information about identifying suspicious transactions and how to use these indicators. If you provide life insurance as your main occupation or as one of the many services that you offer, consider the following indicators.

- Client proposes to purchase an insurance product using a cheque drawn on an account other than his or her personal account.
- Client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment.

- Client 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 payment.
- Client conducts a transaction that results in a conspicuous increase in investment contributions.
- Client cancels investment or insurance soon after purchase.
- Client shows more interest in the cancellation or surrender than in the long-term results of investments.
- Client 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.
- Client accepts very unfavourable conditions unrelated to his or her health or age.

5. Securities Dealers

Please read the general information about identifying suspicious transactions and how to use these indicators. If you are involved in any aspect of the business of dealing in securities or segregated fund products, including portfolio managers and investment advisors, consider the following indicators.

- Normal attempts to verify the background of a new or prospective client are difficult.
- Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the client or their financial ability.
- Any dealing with a third party when the identity of the beneficiary or counter-party is undisclosed.
- Client attempts to purchase investments with cash.
- Client wishes to purchase a number of investments with money orders, travellers cheques, cashiers cheques, bank drafts or other bank instruments, especially in amounts that are slightly less than $10,000, where the transaction is inconsistent with the normal investment practice of the client or their financial ability.
- Client uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the client or their financial ability.
- Client wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the client.
- Client frequently makes large investments in shares, bonds, investment trusts or the like in cash or by cheque within a short time period, which is inconsistent with the normal practice of the client.
- Client makes large or unusual settlements of securities in cash.
- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
- Transfers of funds or securities between accounts not known to be related to the client.
- Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity.
- Transactions of very large dollar size.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.
- All principals of client are located outside of the Cook Islands.
- Client attempts to purchase investments with instruments in the name of a third party.

- Payments made by way of third party cheques are payable to, or endorsed over to, the client.
- Transactions made by your employees, or that you know are made by a relative of your employee, to benefit unknown parties.
- Third-party purchases of shares in other names (i.e., nominee accounts).
- Transactions in which clients make settlements with cheques drawn by, or remittances from, third parties.
- Unusually large amounts of securities or share certificates in the names of persons other than the client.
- Proposed transactions are to be funded by international wire payments, particularly if from countries where there is no effective anti-money-laundering system.

6. Foreign Exchange Dealers, Money Remittance and Services Businesses

Please read the general information about identifying suspicious transactions and how to use these indicators. If you are involved in the money services business, including foreign exchange dealers, money remitters and issuers of travellers cheques consider the following indicators:

- Client requests a transaction at a foreign exchange rate that exceeds the advertised rate.
- Client wants to pay transaction fees that exceed the advertised fees.
- Client exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Client knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument.
- Client wants a cheque issued in the same currency to replace the one being cashed.
- Client wants cash converted to a cheque and you are not normally involved in issuing cheques.
- Client wants to exchange cash for numerous postal money orders or similar in small amounts for numerous other parties.
- Client enters into transactions with counter parties in locations that are unusual for the client.
- Client instructs that funds are to be picked up by a third party on behalf of the payee.
- Client makes large purchases of travellers cheques not consistent with known travel plans.
- Client requests numerous cheques in small amounts and various names, which total the amount of the exchange.
- Client requests that a cheque or money order be made out to the bearer.
- Client requests that a large amount of foreign currency be exchanged to another foreign currency.

7. Accountants

Please read the general information about identifying suspicious transactions and how to use these indicators. If you are an accountant, consider the following indicators when you are carrying out certain activities on behalf of your client, as explained above.

- Client appears to be living beyond his or her means.
- Client has business activity inconsistent with industry averages or financial ratios.
- Client receives 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 no 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 organisations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.

8. Real Estate Brokers or Sales Representatives

Please read the general information about identifying suspicious transactions and how to use these indicators. If you are in the real estate industry, consider the following indicators when carrying out certain activities on behalf of your clients, as explained above.

- Client arrives at a real estate closing with a significant amount of cash.
- Client purchases property in the name of a nominee such as an associate or a relative (other than a spouse).
- Client does not want to put his or her name on any document that would connect him or her with the property or uses different names on Offers to Purchase, closing documents and deposit receipts.
- Client inadequately explains the last minute substitution of the purchasing party's name.
- Client negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference under the table.
- Client sells property below market value with an additional under the table payment.
- Client pays initial deposit with a cheque from a third party, other than a spouse or a parent.
- Client pays substantial down payment in cash and balance is financed by an unusual source or offshore bank.
- Client purchases personal use property under corporate veil when this type of transaction is inconsistent with the ordinary business practice of the client.
- Client purchases property without inspecting it.
- Client 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.
- Client pays rent or the amount of a lease in advance using a large amount of cash.
- Client is known to have paid large remodeling or home improvement invoices with cash, on a property for which property management services are provided

Designated categories of offences

Designated categories of offences means:

- participation in an organised criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;
- robbery or theft;
- smuggling; (including in relation to customs and excise duties and taxes);
- tax crimes (related to direct taxes and indirect taxes);
- extortion;
- forgery;
- piracy; and
- insider trading and market manipulation.

When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.

Source: Glossary of the FATF Recommendations

END