TRANSACTION REPORTING AUTHORITY

ANTI-MONEY LAUNDERING/ COUNTER TERRORIST FINANCING GUIDELINES FOR FINANCIAL INSTITUTIONS & CASH DEALERS

Contents

Foreword

This Guideline is issued by the Transaction Reporting Authority (TRA) to outline the requirements of the Money Laundering and Proceeds of Crime Act 2000, Money Laundering and Proceeds of Crime (Amendment) Act 2010 (the "MLPCA") and the Money Laundering and Proceeds of Crime Regulations 2010 (the "Regulations"), to provide a practical interpretation of the MLPCA and Regulations, to give examples of good practice, and to assist management in developing policies and procedures appropriate to their business. The Guideline is issued pursuant to section 11A(o) of the MLPCA.

The MLPCA and Regulations were introduced to help detect, prevent and deter money laundering. Financial institutions and cash dealers are required by the MLPCA and Regulations to report suspicious transactions and establish record-keeping and compliance regimes. The MLPCA also established a Transactions Reporting Authority (TRA) and by order dated 5 July 2001 the Attorney-General, with the approval of Cabinet, appointed the National Reserve Bank of Tonga (NRBT) as the TRA.

Reporting institutions[1] are expected to be aware of and implement the requirements of the MLPCA and Regulations. The role of the TRA and other supervisory agencies in Tonga is to ensure compliance with the requirements of these legislations through on-site compliance examinations. It is intended that such examinations will be conducted by the TRA pursuant to section 11A(e) of the MLPCA.

Reporting institutions' reporting of suspicious transactions is a cornerstone of the Financial Action Task Force (FATF) recommendations. Law enforcement agencies throughout the world acknowledge that the successful investigation of money laundering offences depends largely on information received from the financial community. Reporting institutions are not being asked or expected to assume the role of law enforcers of money laundering. A positive approach to legislative requirements, however, will greatly improve the efforts of those agencies responsible for enforcement.

This Guideline will be reviewed periodically to reflect changing circumstances and experiences and to provide additional clarification concerning matters where queries arise. More generally, the TRA will work closely with other authorities in Tonga to ensure that Tonga's system to combat money laundering and terrorist financing meets international requirements.

The **scope** of this Guideline covers "reporting institutions" which are defined under Section 2 of the MLPCA. The **terminology** used in this Guideline is consistent with the MLPCA.

---

[1] For the purposes of this Guideline, "reporting institutions" are "cash dealers" and "financial institutions" as defined in section 2(1) of the MLPCA.

This Guideline has been written in five sections:

- Part I General information: gives an overview of money laundering and terrorist financing.
- Part II Developing an effective system: describes key obligations placed on reporting institutions by the MLPCA and Regulations.
- Part III Banks, fiduciary service providers and insurers: summarises the potential risks of money laundering and terrorist financing for fiduciary service providers and insurers.
- Part IV Specific Guidelines for reporting institutions: includes a series of appendices outlining additional requirements for each class of reporting institution including examples of suspicious transactions.
- Part V STR Form: includes an example of the suspicious transaction reporting (STR) form that reporting institutions are required to complete pursuant to the MLPCA.

Reporting institutions should contact the TRA to discuss aspects of these guidelines and any problems or questions arising from the legislations.

Working together is the key.

Transaction Reporting Authority
Phone: (676) 24-057
Facsimile: (676) 24-201
Email: nrbt@reservebank.to
Postal address: Transaction Reporting Authority, National Reserve Bank of Tonga, Private Bag 25, Nuku'alofa, Tonga

PART I – GENERAL INFORMATION

1.1 Money Laundering

What is money laundering?

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of money or other assets gained from crime. If undertaken successfully, money laundering also allows criminals to maintain control over those proceeds of crime and, ultimately, disguise the true criminal source of this income.

Money laundering is a global problem that affects all countries. By its nature, it is a hidden activity and therefore the scale of the problem and the amount of criminal money being generated either locally or globally each year is impossible to measure accurately, but it has been estimated at between USD1.3 trillion to USD3.3 trillion per year[2]. Failure to prevent the laundering of the proceeds of crime permits criminals to benefit from their actions, thus making crime more attractive.

Stages of Money Laundering

There is no one method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a car or jewellery), to passing money through a complex international web of legitimate businesses and "shell companies" (i.e. those companies that primarily exist only as named legal entities without any trading or business activities). Initially, however, in the case of drug trafficking and some other serious crimes such as robbery, the proceeds usually take the form of cash, which needs to enter the financial system by some means. Likewise, street level purchases of drugs are almost always made with cash. Despite the variety of methods employed, the laundering process is accomplished in three stages, which may comprise numerous transactions, by the launderers that could alert a reporting institution to criminal activity:

a) **Placement** - the physical disposal of the money or assets gained from crime. This may include:

i) Placing cash on deposit at a bank (often intermingled with a legitimate money to obscure the audit trail), thus converting cash into readily recoverable funds;

[2] In the 1996, the International Monetary Fund (IMF) estimated the global volume of money laundering to be between two to five per cent of world GDP (Source: US National Money Laundering Strategy 2002). This estimate of the global volume of money laundering is based on the 1996 study and 2007 IMF world GDP data.

ii) Physically moving cash between countries;

iii) Making loans in tainted cash to businesses which seem legitimate or are connected with legitimate businesses, thus also converting cash into debt;

iv) Purchasing high value goods for personal use or expensive presents to reward existing or potential colleagues;

v) Purchasing negotiable assets in one-off transactions; or

vi) Placing cash in the client account of a professional intermediary.

b) **Layering** - separating criminal proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. This may include:

i) Rapid switches of funds between banks and/or countries;

ii) Use of cash deposits as collateral to support legitimate transactions;

iii) Switching cash through a network of legitimate business and "shell companies" across several jurisdictions; or

iv) Resale of goods or assets.

c) **Integration** - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as legitimate or 'clean' funds.

The three basic steps may occur as separate and distinct phases. They may occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering options and the requirements of the criminal individual or criminal organisation(s) involved.

Although placement, layering and integration are common strategies in laundering, the MLPCA[3] further defines money laundering to include (i) the acquisition, possession and use of property by a person, knowing or having reasonable grounds to believe or suspect that it is derived directly or indirectly from the commission of a serious offence; and (ii) the acquisition,

[3] *MLPC Act* section 2 & section 17

possession and use of property by a person, knowing or having reasonable grounds to believe or suspect that it is derived directly or indirectly from the commission of a serious offence by:

- conversion or transfer of property that the person knows to be proceeds of crime with the aim of concealing or disguising the illicit origin of that property; or
- concealing or disguising the true nature, source location, disposition, movement, or ownership of, or right with respect to, property that the person knows to be the proceeds of crime.

Vulnerability of Reporting Institutions to Money Laundering

Historically, efforts to combat money laundering have concentrated on the deposit-taking procedures of reporting institutions where it is easier to discover the launderer's activities.

However, criminals have learnt that unusual or large cash payments made into reporting institutions can create suspicion and lead to additional enquiries. Criminals have therefore sought other means to convert the illegally cash or to mix it with legitimate cash earnings before it enters the financial system, thus making it harder to detect at the placement stage. Equally, there are many crimes (particularly the more sophisticated ones) where cash is not involved.

The need to combat money laundering

The ability to launder the proceeds of crime through the financial system is vital to the success of criminal operations. The unchecked use of financial systems for this purpose has the potential to undermine individual reporting institutions and ultimately the entire financial sector. The increased integration of the world's financial systems and the removal of barriers to the free movement of capital have made money laundering easier and complicated the tracing process.

Reporting institutions that become involved in a money laundering scandal, even unwittingly, will risk prosecution, the loss of their good market reputation, and damage the reputation of Tonga as a safe and reliable country for investors.

Money laundering is often thought to be associated solely with banks, other credit institutions and bureaux de change. Whilst the traditional banking processes of deposit taking, money transfer and lending do offer a vital laundering mechanism, particularly in the initial conversion from cash, products and services offered by other types of financial and non-financial sector businesses are also attractive to the launderer.

The sophisticated launderer often involves many other unwitting accomplices such as:

- Stockbrokers and securities houses;

- Insurance companies and insurance brokers;

- Financial intermediaries;
- Accountants and solicitors;
- Real estate agents;
- Casinos and other gambling games such as lotteries;
- Company formation agents;
- Dealers in precious metals and bullion;
- Antique dealers, car dealers and others selling; and
- High value commodities and luxury goods.

Vulnerability points for money launderers

Money launderers' transactions are more vulnerable to detection at certain points in the financial system, specifically:

i) Entry of cash into the financial system;

ii) Cross-border flows of cash;

iii) Transfers within and from the financial system;

iv) Purchasing investments and other assets;

v) Incorporation of companies; and

vi) Formation of trusts.

Through the analysis of suspicious transactions reports submitted to the TRA by reporting institutions, the following methods and trends have been identified in Tonga:

i) Large cash transactions (deposits/withdrawals) involving newly opened accounts;

ii) Large cash transactions (deposits/withdrawals) inconsistent with the customer's account history;

iii) Large telegraphic transfers inconsistent with customer's profile and history;

iv) Using of personal accounts for business transactions; and

v) Failure to provide identification documents.

1.2 The Financing of Terrorism

What is Terrorist Financing?

Terrorist financing involves collecting and providing funds for terrorist activity. Terrorist activity has as its main objective intimidation of a population or compelling a government to do something or not do something. This is done by intentionally killing, seriously harming or endangering a person, causing substantial property damage likely to seriously harm people or by seriously interfering with or disrupting essential services, facilities or systems.

Terrorists need financial support to carry out terrorist activities and achieve their goals. In this respect, there is little difference between terrorists and other criminals in their use of the financial system. A successful terrorist group, much like a criminal organization, is one that is able to build and maintain an effective financial infrastructure. For this, it must develop sources of funding and means of obscuring the links between those sources and the activities the funds support. It needs to find a way to make sure that the funds are available and can be used to get whatever goods or services are needed to commit terrorist acts. The money needed to mount terrorist attacks can be small and the associated transactions are not necessarily complex.

Methods of Terrorist Financing

There are two primary sources of financing for terrorist activities. The first involves getting financial support from countries, organizations or individuals. The other involves revenue-generating activities. These are explained in further detail below.

Financial Support

Terrorism could be sponsored by a country or government, although this is believed to have declined in recent years. State support may be replaced by support from other sources, such as individuals with sufficient financial means.

Revenue-Generating Activities

The revenue-generating activities of terrorist groups may resemble other criminal organizations. 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 and 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 organizations with charitable or relief status, so that donors are led to believe they are giving to a legitimate cause.

Only a few non-profit organizations or supposedly charitable organizations have been implicated in terrorist financing. In these cases, the organizations may in fact have carried out some of the charitable or relief work. Members or donors may have had no idea that a portion of funds raised by the charity was being diverted to terrorist activities. This type of legitimately earned financing might also include donations by terrorist group members of a portion of their personal earnings.

Laundering of Terrorist-Related Funds

Like criminal organizations, terrorists must find ways to launder or transfer illicit funds without drawing the attention of the authorities. For this reason, transactions related to terrorist 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.

Importance of Combating Terrorist Financing

Acts of terrorism pose a significant threat to the safety and security of people all around the world. Tonga continues to work with other nations to confront terrorism and bring those who support, plan and carry out acts of terrorism to justice.

Business relationships with terrorist groups could expose reporting institutions or financial intermediaries to significant reputational and operational risk, as well as legal repercussions. The risk is even more serious if the terrorist group is subsequently shown to have benefited from the lack of effective monitoring or wilful blindness of a particular institution or intermediary that enabled them to carry out the terrorist activities.

International Efforts to Combat Terrorist Financing

At an extraordinary Plenary on the Financing of Terrorism held in October 2001, the Financial Actions Task Force (FATF)[4] expanded its mission beyond money laundering. During the extraordinary Plenary, the FATF agree to a set of special recommendations which committed members to:

- Ratify and implement relevant United Nations instruments.
- Criminalize the financing of terrorism, terrorist acts and terrorist organisations.
- Freeze and confiscate terrorist assets.

[4] The Financial Actions Task Force (FATF) is the international standard setter and has issued guidance to jurisdictions in relation to money laundering and terrorist financing.

- Report suspicious transactions linked to terrorism.
- Provide the widest possible range of assistance to other countries' law enforcement and regulatory authorities for terrorist financing investigations.
- Impose anti-money laundering requirements on alternative remittance systems.
- Strengthen customer identification measures in international and domestic wire transfers.
- Ensure that non-profit organizations cannot be misused to finance terrorism.

Tonga is committed to contributing to the fight against terrorism. Reporting institutions should seek to prevent terrorist organizations from using their financial services, and assist the Government and the TRA in their efforts to detect suspected terrorist financing, and promptly respond to enquiries from the TRA.

The systems reporting institutions need to detect transactions potentially related to terrorism closely resemble those designed to detect money laundering. In fact, the indicators in this guideline are combined for both money laundering and terrorist financing.

Should a reporting institution become aware that a transaction or attempted transaction is related to the financing of terrorism or involves an individual or entity named as a terrorist pursuant to United Nations Security Council resolutions, the reporting institution should immediately notify the TRA and submit a suspicious transactions report, even if the reporting institution declines the transaction as a result of its own due diligence.

.

PART II – DEVELOPING AN EFFECTIVE SYSTEM

2.1 Introduction

The MLPCA and Regulations impose requirements on reporting institutions related to reporting of transactions, record keeping, staff awareness and customer identification. These statutory requirements are briefly outlined in this section of the Guideline. In addition, to assist reporting institutions develop internal policies and procedures to establish an effective system to combat money laundering and terrorist financing, this section provides guidance on the practical implementation of the requirements and intent of these legislation.

The Duty of Vigilance

Reporting institutions are required to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the institution from being used, intentionally or unintentionally, by criminal elements. The MLPCA[5] requires reporting institutions to establish and maintain procedures to combat money laundering and terrorist financing.

The duty of vigilance is necessary to avoid assisting the process of laundering and to react to possible attempts at being used for that purpose. Thus the duty of vigilance consists mainly of the following five elements:

i) Verification;

ii) Recognition of suspicious transactions;

iii) Reporting of transactions as required by the MLPCA and Regulations;

iv) Keeping records; and

v) Training

Institutions perform their duty of vigilance by having in place systems which enable them to:

i) Determine the true identity of customers requesting their services;

ii) Recognise and report suspicious transactions to the TRA;

---

[5] *Money Laundering and Proceeds of Crime Act* section 16(a); and Part V of the *Money Laundering and Proceeds of Crime Regulations*

iii) Keep records for the prescribed period of time;

iv) Train key staff to ensure that they understand their obligations under the MLPCA and Regulations;

v) Liaise closely with the TRA on matters concerning policy and systems to detect money laundering and the financing of terrorism; and

vi) Ensure that internal audit and compliance functions regularly monitor the implementation and operation of the institution's anti-money laundering and counter terrorist financing (AML/CFT) policies and procedures.

The nature and scope of the policies and procedures will vary depending on its size, structure and the nature of the business. However, irrespective of size and structure, all institutions should establish policies and procedures which in effect measure up to this Guideline and the requirements of the MLPCA and Regulations.

The system should enable key staff to react effectively to suspicious occasions and circumstances by reporting them to the relevant personnel in-house and to receive training from time to time, whether from the institution or externally.

Responsibilities of Reporting Institutions

To ensure that Tonga is not used as a channel for criminal funds, all reporting institutions should:

a) Comply with TRA policies, regulations, directives and the MLPCA and Regulations. The Board of Directors and Management of reporting institutions should ensure that TRA policies and all relevant Acts are adhered to and that a service is not provided where there are reasonable grounds to believe that transactions are associated with money laundering offence or an offence of the financing of terrorism activities;

b) Appoint a compliance officer to be responsible for ensuring the institution's compliance with the requirements of the MLPCA and Regulations;

c) Establish an audit function to test its anti-money laundering and combating financing of terrorism procedures and systems;

d) Co-operate with law enforcement agencies such as the TRA on any limits imposed by legislation on customer confidentiality or where there are reasonable grounds for suspecting money laundering;

e) Implement effective procedures for customer identification, record keeping and reporting suspicious transactions. These procedures should be in line with Part 2 of the MLPCA and Part 5 of the Regulations;

f) Screen potential employees to ensure that they are fit and proper and to be re-screen on an ongoing basis;

g) Ensure that its officers and employees are:

- aware of the laws relating to money laundering and financing of terrorism; and
- aware of the procedures and policies for compliance with anti-money laundering and combating the financing of terrorism standards
- trained to recognise suspicious transactions.

Money Laundering Compliance Officer

The MLPCA[6] requires reporting institutions to appoint an officer who is responsible for reviewing and submitting STRs. It is recommended that this officer be designated as the Money Laundering Compliance Officer. In addition to meeting the STR obligations of the MLCPA, the Money Laundering Compliance Officer would also be responsible for ensuring the institution's compliance with the requirements of the MLPCA and Regulations. For example, the officer would also be responsible for staff training.

The TRA expects that the Money Laundering Compliance Officer should be a senior staff member with the necessary powers to ensure the effective management of the system.

Identification procedures

An important objective of obtaining and verifying the identity of customers through reliable documents and sources is to ensure that any person(s) or body corporate found to be conducting or attempting to conduct any serious offence, money laundering offence or an offence of the financing of terrorism, is easily detected, traced and dealt with by the TRA, and relevant law enforcement and regulatory authorities.

Regulation 6 requires reporting institutions to undertake customer due diligence measures, including identifying and verifying the identity of customers, when:

- establishing business relations;

[6] *Money Laundering and Proceeds of Crime Act* section 15(a)

- carrying out occasional transactions when the total value of the transactions equals or exceeds $10,000;
- carrying out wire transfers as provided in Regulation 17; and
- engaged in any business or transaction in any instance where there is a suspicion of money laundering or terrorist financing;
- the reporting institution has doubts about the adequacy of previously obtained customer identification data.

Reporting institutions are, as a matter of best practice and prudent management, encouraged to conduct continuous due diligence on its customers in the course of its business.

It is a statutory requirement[7] that reporting institutions to take reasonable measures to identify a customer on the basis of any official or other identifying document and verify the identity of the customer on the basis of reliable and independent source documents, data or information or other evidence. Furthermore, in the case of a body corporate the MLPCA requires verification of the legal existence of the body corporate by obtaining copies of the entity's certificate of incorporation together with a copy of the latest annual return submitted to the Registrar of Companies.

For customers who are legal persons or legal arrangements, reporting institutions[8] are required shall obtain and verify the following information:

- the customer's name, legal form addresses of controlling body members;
- proof of incorporation or similar evidence of establishment or existence:
- the principal owners, beneficiaries and control structure;
- provisions that set out the power to bind the customer; and
- provisions for authorisation of any person purporting to act on behalf of the customer and the identity of the person.

[7] *Money Laundering and Proceeds of Crime Act* section 12; and *Money Laundering and Proceeds of Crime Regulations* Regulation 6
[8] *Money Laundering and Proceeds of Crime Regulations* Regulation 6

Know your Customer (KYC)

The need for reporting institutions to know their customers is vital for the prevention of money laundering and to counter the financing of terrorism. If a customer has established an account under a false identity, he/she may be doing so for the purpose of defrauding the reporting institution itself or merely to ensure that he/she cannot be traced or linked to the proceeds of the crime that the institution is being used to launder. A false name, address or date of birth will usually mean that the law enforcement agencies cannot trace the customer if needed for interview in connection with an investigation.

When a business relationship is being established, the nature of the business that the customer expects to conduct with the reporting institution should be ascertained at the outset to show what might be expected as normal activity. In order to be able to judge whether a transaction is or is not suspicious, reporting institutions need to have a clear understanding of the legitimate business of their customers.

The procedures which reporting institutions adopt to comply with money laundering legislation will inevitably overlap with the prudential fraud prevention measures which they would undertake in order to protect themselves and their genuine customers. So far as lending is concerned, a bank or non-bank financial institution engaged in lending will naturally want to make specific checks on an applicant's true identity, credit-worthiness, employment and other income details. Such checks will often be very similar to identity checks undertaken for money laundering purposes.

Reporting institutions[9] are required to maintain accounts in the true name of the account holder. Reporting institutions should not open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. Nor should confidential numbered accounts function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to perform proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from a bank's compliance function or from supervisory authorities.

[9] *Money Laundering and Proceeds of Crime Act* section 13(2); and *Money Laundering and Proceeds of Crime Regulations* Regulation 6(2)

2.2 Components of an Effective System

Essential Elements of Know-Your-Customer Requirements

All reporting institutions should have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the institution from being used, intentionally or unintentionally, by criminal elements. The design of these policies should reflect the nature of the services offered by the institution. Essential elements should start from the institutions' risk management and control procedures and should include:

a) customer acceptance policy,

b) customer identification,

c) on-going monitoring of high risk accounts, and

d) risk management.

Institutions should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account.

Customer acceptance policy

Reporting institutions should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to the institution. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Reporting institutions should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers.

2.3 Identification verification

This Guideline, in line with the MLPCA and Regulations, sets out what might reasonably be expected as a minimum adequate evidence of identity of reporting institutions. However, the overriding requirement is for the reporting institution itself to be satisfied that it has established the true identity of the prospective customer as far as it is reasonably possible.

A reporting institution should establish to its satisfaction that it is dealing with a real person or organisation (natural, corporate or legal), and verify the identity of those persons who have power to operate an account. If funds to be deposited or invested are being supplied by or on behalf of a third party, the identity of the third party (i.e. the underlying beneficiary) should also be established and verified.

Where face to face contact is normal procedure and it is expected that face to face contact will take place early in the business relationship, wherever possible, the prospective customer should be seen personally and photographic evidence of identity obtained.

The verification procedures necessary to establish the identity of the prospective customer should basically be the same whatever type of account or service is required (e.g. current, deposit, lending or mortgage accounts).

The evidence of identity required should be obtained from documents issued by reputable sources. Copies of the supporting evidence and every transaction that is conducted through the reporting institution should be retained for a minimum period of five years after the completion of the transaction[10].

Any subsequent changes to the customer's name, address, or employment details of which the reporting institution becomes aware should be recorded as part of the "know your customer" process. Generally this would be undertaken as part of good practice for the reporting institution's own protection against fraud and bad debts.

Once identification procedures have been satisfactorily completed, then the business relationship has been established and, as long as records concerning that customer are maintained in line with Section 13 of the MLPCA, no further evidence of identity is needed when transactions are subsequently undertaken for that customer as long as regular contact is maintained. When an existing customer closes one account and opens another, there is no need to re-verify identity, although good practice would be to obtain any missing or additional information at this time. This is particularly important if there has been no recent contact with the customer e.g. within the past twelve months.

Evidence of Identity

Reporting institutions must obtain satisfactory evidence of identity of a prospective customer at the time of opening an account or entering into a business relationship. Unless satisfactory evidence of identity is obtained as soon as is reasonably practicable, the reporting institution must not proceed any further with the business relationship or carry out a one-off transaction with the applicant for business, unless directed to do so by the TRA.

Some people will not have official documents, such as a passport or birth certificate. Some may not know their exact date of birth. In such cases, a risk-based approach should be taken and alternative means of identification may be acceptable, such as a letter from a reputable and identifiable party.

---

[10] *Money Laundering and Proceeds of Crime Act* section 13(4)

Reporting institutions should take into consideration the need to balance verification requirements against access to financial services.

What is Identity?

As a guide, a list of documents that are acceptable for verifying a person or corporation's identification is provided below. Reporting institutions should include in their internal policies and procedures a list of documents that it is prepared to accept from a customer to verify identity. This list establishes minimum requirements that the TRA would expect reporting institutions to obtain from customers.

Natural Persons

The following combinations of documents from the list below are acceptable as identification for a person:

a) Two 'Category A' documents, or

b) One 'Category A' document and two 'Category B' letters, or

c) Three 'Category B' letters.

Reporting institutions should ensure that customers provide at least one document capable of serving as photo identification. This may include a photo that is signed and verified by a person listed in 'Category B'. Reporting institutions may waive this photo requirement for customers where they are satisfied the person's identity can be adequately verified through other means.

A risk-based approach should again be adopted. 'Category A' documents are more robust than 'Category B' documents. When verifying an individual's identity, a 'top-down' approach should be used by asking individuals to provide 'Category A' documents first, before drawing on 'Category B' documents. The process of identification should be documented and the reporting institution should state in writing why the decision was made to accept Category B documents to verify an individual's identity.

- **Category A – Official Documents:** Current passport (all countries)
- Current driver's license (all countries)
- Government identification documents
- Certificate of Christening/Baptism
- Citizenship certificate
- Birth certificate
- Employment identification
- Employment records
- Employment pay slips
- Marriage certificate
- Educational institution certificates
- Student card or registration document for an educational institution (such as a primary or high school)
- Government health card
- License or permit issued by the Government of Tonga
- Public utilities record (such as an electricity or telephone bill)
- Current records of membership of

- Other official records from the Government of Tonga
- An existing customer who is known favourably to the reporting institution (verified by a reporting institution signature)
- An existing customer with a bank who has held an account with the bank for more than two years
- Foreign pensioner's card
- Tonga work permit
- professional or trade organisation
- Records from a bank (including bank or credit cards such as Visa, Diners Club, Mastercard, American Express; or statements for an account or credit card)
- Superannuation or provident fund membership card
- Fire arms license
- Mortgage or other security document over the customer's property

Category B Documents:

A written reference confirming the customer's full name, date of birth and occupation, from one of the following acceptable referees:

- A bank employee
- An officer in charge of a bank agency
- A bank manager
- A lawyer or legal practitioner
- A registered medical practitioner or dentist
- A qualified pharmacist
- A Magistrate of a District Court
- A landlord of a rented premises where the person lives
- A public servant
- A Customs or Immigration officer
- A Minister of Religion
- A Church leader
- A Magistrate
- A local level Government Councillor
- A Notary
- A Headmaster of a primary or secondary school
- A serving Member of Parliament
- A Police officer or commander
- An accountant who is a member of an association of accountants
- An employee of a reporting institution or cash dealer
- A statutory declaration from a person who has known the customer for one year or more
- A village leader

The identity of unincorporated businesses or associations (e.g. self employed persons who own a business) should be verified by establishing the identity of the partner, proprietor or owner. This should be done using the same documents that are used to identify a natural person.

Reporting institutions should conduct on-going due diligence on relationships with each customer and scrutiny of any transactions undertaken by customers to ensure that the transaction being conducted is consistent with the reporting institution's knowledge of the customer, the customer's business and risk profile. Where necessary, for example in the case of Politically Exposed Persons, reporting institutions should obtain information as to the source of funds.

Direct Clients - Partnerships

Where an application for business is made by a partnership, the identity of each individual partner who is an account signatory or who is authorised to give instructions to the reporting institution, should be verified as if he or she is a prospective direct personal client. In the case of a limited partnership, the identity of a limited partner need not be verified unless he or she is a significant investor (i.e. has contributed more than 10% of the total capital of the partnership).

Direct Corporate Clients

A reporting institution should obtain the following information and documentation concerning all prospective direct company clients:

- Certificate of incorporation and any change of name certificates; where the corporate body is incorporated outside Tonga, such certificates should be certified or, where the certificates form part of a business transaction record, such certificates should be notarized.

- Where a business transaction record must be kept, a copy of the most recent annual return, if any, filed at the Registrar of Companies; such return must be notarized where the corporate body is incorporated outside Tonga.

- Address of the registered office and the name and address of the registered agent, if applicable;

- The address of the principal place of business;

- The verified identity of each of the beneficial owners of the company who hold an interest of 10% or more in the company and/or the persons on whose instructions the directors, the signatories on the account or the individuals authorised to deal with the reporting institution are empowered to act;

- In the case of a bank account, the verified identity of the account signatories or the persons authorised to deal with the reporting institution;

- A resolution or bank mandate, signed application or other form of authority, signed by no fewer than the number of directors required for a quorum, containing details of the persons authorised to give instructions to the reporting institution concerning the account, together with their specimen signatures;

- In the case of a bank account, copies of any Powers of Attorney or other similar instruments or documents given by the directors in relation to the company; and

- A statement signed by a director setting out the nature of the business of the company, the reason for the account being opened, the expected turnover of volume of business and the source of funds.

Reporting institutions should also obtain a copy of the memorandum and articles of association or by-laws of the company or a copy of the company's last available financial statements.

Reporting institutions should exercise care in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Satisfactory evidence of the identity of beneficial owners of all such companies should be obtained. In the case of entities that have a significant proportion of capital in the form of bearer shares, extra vigilance is required. A reporting institution may be completely unaware that the bearer shares have changed hands. Therefore, reporting institutions should put in place satisfactory procedures to monitor identity of material beneficial owners. This may require the reporting institution to immobilise the shares, e.g. by holding the bearer shares in custody.

Direct Clients - Trusts

The identification of trustees, settlors, protectors, any person having power to appoint or remove trustees and any person (other than the settlor) who has provided funds to the settlement should be verified as direct prospective clients (individual or corporate, as appropriate). In addition, the following should be obtained:

- Evidence verifying proper appointment of trustees, e.g. copy extracts from the Deed of Trust or a letter from a lawyer verifying the appointment;

- Details of the nature and purpose of the trust; and

- Details of the source of funds.

Reporting institutions should also obtain and verify the identity of the beneficiaries or the principal beneficiaries of a trust. If the trust is complex, it is accepted that this will not always be possible or necessary depending on the reporting institution's judgement of the money laundering risk involved. However if such a situation arises, the reporting institution should take appropriate steps to satisfactorily identify the beneficiaries of the trust.

Certification of Documents

Suitable Certifiers

A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated bank, trust company or trustee company, notary public or member of the judiciary. The certifier should sign the copy document (printing his or her name clearly

underneath) and clearly indicate his position or capacity on it together with a contact address and telephone number.

The list of suitable certifiers is not intended to be exhaustive and reporting institutions should exercise due caution when considering certified copy documents, especially where such documents originate from a country perceived to represent a high risk of financial crime or money laundering or from unregulated entities in any jurisdiction.

Where certified copy documents are accepted, it is the reporting institution's responsibility to satisfy itself that the certifier is appropriate. In all cases, the reporting institution should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate or other document.

Reliance on Other Institutions to Verify Identity

Verifying identity is often time consuming and expensive and can cause inconvenience for prospective customers. It is therefore important that as far as possible reporting institutions standardise and simplify their procedures and avoid duplicating the identification requirements where it is reasonable and practicable to do so.

Although the responsibility to obtain satisfactory evidence of identity cannot be avoided by the reporting institution that is performing a service for customer, there are occasions when it is reasonable to rely on another institution to undertake the procedures or to confirm identity; intermediaries or third parties. Relying on due diligence conducted by another reporting institution, however reputable, does not in any way remove the ultimate responsibility of the recipient reporting institution to know its customers and their business. Reporting institutions should not rely on financial institutions that are subject to weaker standards than those governing the banks' own KYC procedures or those applicable to Tonga.

Exceptions from Identification Requirements

The MLPCA[11] provides limited exemptions to the prescribed identification requirements. Specifically, documentary evidence of identity will not normally be required if:

- the person conducting the transaction is a financial institution or cash dealer that is subject to the provisions of the MLPC legislations; or

[11] *Money Laundering and Proceeds of Crime Act* section 12(5)

- the transaction is part of an established business relationship with person and the person has already produced satisfactory evidence of identity, unless the reporting institution suspects the transaction is suspicious or unusual.

Higher Risk Customers, Jurisdictions and Business Relationships

Reporting institutions are required[12] to perform enhanced customer due diligence measures for categories of customer, business relationships or transactions with a higher risk of money laundering.

In cases where a customer is regarded as higher risk, reporting institutions must take reasonable steps to:

- establish the source of that customer's wealth and funds; and
- conduct regular and ongoing monitoring of the customer's transactions.

Part B of the Schedule of the Regulations outlines factors for determining if a customer is higher risk. International experience identifies the following examples of higher risk customers:

- Non face-to-face customers
- Politically Exposed Persons (PEPs) – individuals entrusted with prominent public functions or persons linked to a PEP.
- Non-resident customers – especially customers who are from or work in countries or regions or industries where risk of money laundering and terrorist financing is high.
- Customers that are connected with jurisdictions that lack proper standards in the prevention of money laundering and terrorist financing

Reporting institutions must make judgements about which industries are higher risk. Industries at higher risk of being associated with money laundering include:

- those with high earning potential and which are subject to controls and permits – e.g. fishing and logging
- dealers in precious metals or stones; and
- legal professionals and accountants who carry out transactions for their clients.

[12] *Money Laundering and Proceeds of Crime Regulations* Regulation 15

- Non face-to-face customers – e.g. those which operate accounts via electronic means

- Legal persons or arrangements, such as trusts that act as asset holding vehicles.

It is a statutory requirement13 that no higher risk customer shall be accepted as a customer unless a senior member of the financial institution's management has verified and approved the application.

Financial Institutions shall have policies in place and take such measures as are needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.

Non face-to-face Verification

Reporting institutions should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview.

Clearly, in such situations, photographic evidence of identity is inappropriate and it is therefore important to undertake not only address verification but also to put in place additional procedures to establish personal verification. For example, there are three main areas of information (i.e. address details, employment details and the name and date of birth of the applicant), which could be checked to establish beyond reasonable doubt that a prospective new customer is genuine and that the named applicant is not the victim of an identity theft.

In accepting business from non-face-to-face customers:

- Reporting institutions should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview; and

- There must be specific and adequate measures to mitigate the higher risk.

Examples of measures to mitigate risk include:

- Certification of documents presented;

- Requisition of additional documents to complement those which are required for face-to-face customers;

- Independent contact with the customer by the reporting institution;

[13] *Money Laundering and Proceeds of Crime Regulations* Regulation 15(4)

- Seeking verification of the source of funds for the initial deposit, including sighting documentary evidence confirming the source of the funds.

Non-Resident Customers

For those prospective customers who are not normally resident in Tonga, but who make face to face contact, passports or national identity cards must always be available and the relevant reference numbers should be recorded. It is impractical to set out detailed descriptions of the various identity cards and passports that might be offered as evidence of identity by foreign nationals. However, if necessary, reporting institutions should seek to verify identity and permanent address with a reputable reporting institution in the applicant's home country or country of residence.

Record Keeping Requirements

An important objective of record keeping is for reporting institutions, at all stages in a transaction, to be able to retrieve relevant information to the extent that it is available, without undue delay.

Reporting institutions must[14] maintain records of:

- all transactions carried out by it, in accordance with the requirements of section 13(3)
- its related documentation; and
- identification data
- account files
- all business correspondences

In addition, reporting institutions should maintain records of:

- all reports made to the TRA;
- all enquiries relating to the money laundering and the financing of terrorism made to it by the TRA or a law enforcement agency.

The records must be kept for a minimum period of five years from the date -

[14] *Money Laundering and Proceeds of Crime Act* section 13(1)(a)

- the evidence of a person's identity was obtained;
- of any transaction or correspondence;
- the account is closed or business relationship ceases, whichever is the later.

All customer and transaction records and information shall be made available on a timely basis to the TRA and other domestic competent authorities upon request by the appropriate authority.

Education and Training

Section 16 of the MLPCA and Part V of the Regulations requires that reporting institutions must establish and maintain internal procedures:

- To make the institution's officers and employees aware of Tonga's laws relating to money laundering;
- To make the institution's officers and employees aware of the policies and procedures put in place to deal with money laundering; and
- To train officers and employees to recognise and deal with money laundering transactions.

A financial institution or cash dealer should maintain a record of the training received by particularly staff members in relation to AML/CFT. Financial Institutions and cash dealers should also regularly assess the AML/CFT knowledge and ability of staff, particularly those in critical positions. These assessments should feed into documented system for managing corrective/disciplinary action.

The Need for Staff Awareness

The effectiveness of this Guideline depends on the extent to which an institution's officers and staff appreciate the serious nature of money laundering and terrorist financing and the impact it could have on the reputation of both the institution and Tonga.

Staff must be aware of their own personal statutory obligations and must be informed that they can be personally liable for failure to report information in accordance with internal procedures. All staff should be encouraged to co-operate fully and to provide a prompt report of any suspicious transactions. It is, therefore, important that reporting institutions introduce comprehensive measures to ensure that staff are fully aware of their responsibilities.

All relevant staff should be educated in the importance of "know your customer" requirements. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know

what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

Staff and reporting institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, and a suspicious transaction report should be submitted to the TRA. Reporting institutions that conduct international transactions should, as part of their customer acceptance policy, maintain lists of jurisdictions which have weak anti-money laundering requirements or are considered to be high risk because organized criminal activities are prevalent.

To assist reporting institutions identify high risk jurisdictions, such as those which do not comply with or insufficiently apply the FATF's recommendations in relation to anti-money laundering and countering the financing of terrorism, it is suggested that reporting institutions that conduct international transactions draw on evaluations conducted by agencies such as the International Monetary Fund, World Bank and the Asia Pacific Group on Money Laundering (APG). In this regard for example, the APG conducts regular assessments of jurisdictions' AML/CFT systems and these can be found on the APG's website, www.apgml.org .

Although Directors and Senior Managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the institution itself. Some form of high-level general awareness training is therefore suggested for those staff that may not be involved in dealing with customers on a day-to-day basis.

Section 16A provides measures and sanctions for the TRA or other regulatory authority that discovers a breach of the obligations established under the MLPC legislations by reporting entities. The TRA or other regulatory authority may impose one or more of the following measures and sanctions;

- written warnings;
- order to comply with specific instructions;
- order reports on a regular basis on the measures it is taking;
- barring individuals from employment within the sector;
- replacing or restricting the powers of managers directors, principals, partners or controlling owners, including the appointing ad hoc administrator;
- a temporary administration of the reporting entity; or
- suspending, restricting or withdrawing the license of the reporting entity

2.4 Reporting and Recognition of Suspicious Transactions

A suspicious transaction will often be one, which is inconsistent with a customer's known legitimate business. The first key is to observe whether a transaction, or series of transactions, is consistent with the nature of the customer's business or occupation.

Examples of what might constitute suspicious transactions are provided in appendices to this Guideline. Identification of these types of transactions should prompt further investigations, such as enquiries about the source of funds.

Reporting of Suspicious Transactions

Where a reporting institution suspects, has reasonable grounds to suspect or has information that a transaction or attempted transaction may be related to money laundering, terrorist financing, a serious offence or the proceeds of a criminal offence including tax matters, a serious offence; linked or related to, or to be used for terrorism, terrorist acts, by an individual terrorist, terrorist organizations or terrorist financing, the reporting institution must as soon as practicable after forming the suspicion but no later than 3 working days and wherever possible before the transaction is carried out, report the transaction to the TRA as required by Regulation 21(3) and section 14 (1) of the MLPCA. This reporting requirement is outlined in section 14(2) of the MLPCA. A copy of the suspicious transaction report (STR) form is included in Part 5 of this Guideline.

Section 15 of the MLPCA requires reporting institutions to appoint a compliance officer(s) to be responsible for ensuring the entity's compliance with the requirements of the MLPC legislations. This officer is the designated Money Laundering Compliance Officer who would be responsible for reporting suspicious transactions to the TRA.

Sections 14(1) and 14(2) of the MLPCA state that a suspicious transaction report shall:

- be in writing;
- be in such form and contain such details as required under section 14 of the MLPCA (refer to Part 5 for a copy of the STR form);
- contain a statement of the grounds on which the reporting institution holds the suspicion; and
- be signed or otherwise authenticated by the reporting institution.

The Money Laundering Compliance Officer must keep a register of all reports made to the TRA and all reports made internally to them by employees.

Directors, officers and employees of reporting institutions are **prohibited** from disclosing the fact that an STR or related information is being reported to the TRA. Section 18(3) and section 24A of the MLPCA states that any person who discloses any information relating to a

suspicious transaction report prepared under section 14 of the MLPCA shall be guilty of an offence and liable on conviction of a fine or imprisonment.

If a reporting institution forms a suspicion that a transaction relates to money laundering, they should take into account the risk of tipping off when performing the customer due diligence (CDD) process. If the reporting institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Reporting institutions should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

Regulation 22 requires financial institutions, their directors, officers and employees, permanent and temporary, not to disclose that a suspicious transaction report or related information is being reported or provided to the transaction reporting authority. In addition, sections 18(3) and 24A of the MLPCA provides penalty for the disclosure of any information about a report that has been prepared or sent to the TRA, to any person other than the Court, NRBT or any other person authorised by the law. However, section 14B(1) of the MLPCA states that the provision of section 14 shall not apply to disclosure of any privileged communication between a law practitioner and his client. A privileged communication is described in section 14B(2) of the MLPCA. It is an offence under section 14A when financial institutions and cash dealers fail to report an STR.

Recognition of Suspicious Transactions

As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. Suspicion is personal and subjective and falls far short of proof based on firm evidence. However, it is more than the absence of certainty that someone is innocent. Nevertheless, the reporting institution would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from a crime.

Where there is a business relationship, a suspicious transaction will often be one which is inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognition is knowing enough about the customer and the customer's business to recognise that a transaction or series of transactions is unusual.

Questions that a reporting institution might consider when determining whether an established customer's transaction might be suspicious are:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer's business or personal activities?
- Has the pattern of transactions conducted by the customer changed?

- Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

As outlined in sections of this Guideline relating to education and training and the need for staff awareness, sufficient guidance must be given to staff to enable them to recognise suspicious transactions. The type of situations giving rise to suspicions will depend on a reporting institution's customer base and range of services and products. Reporting institutions might also consider monitoring the types of transactions and circumstances that have given rise to suspicious transaction reports by staff, with a view to updating internal instructions and guidelines from time to time.

Section 14A of the MLPCA states that any person who fails to comply with the requirements of section 14 commits an offence and upon conviction shall be liable to a fine not exceeding $150,000.

Examples of suspicious transactions that may be relevant to different classes of reporting institutions are included in Part IV of this Guideline.

Protection

Reporting institutions and their employees are protected under Section 24 of the MLPCA when complying with their obligations under the MLPC legislations.

Regulation 4 requires reporting entities to ensure that the requirements of the Regulations are also applied by its branches and subsidiaries located outside of the Kingdom. And that any local prohibitions on the application of the Regulations to such branches or subsidiaries shall be reported to the TRA.

2.6 Additional Consideration to ensure effective AML/CFT procedures

The Financing of Terrorism

Reporting institutions in Tonga can assist the TRA and other Government agencies in the fight against terrorism through prevention, detection and information sharing.

While the financing of terrorism is not specifically addressed in the MLPC legislations, reporting institutions should seek to prevent terrorist organizations from accessing their financial services, assist the Government and the TRA in their efforts to detect suspected terrorist financing and promptly respond to enquiries from the TRA. Accordingly, where reporting institutions have reason to suspect that a transaction or attempted transaction is related to the financing of terrorism they are strongly encouraged to submit a suspicious transaction report to the TRA.

Wire Transfers

The FATF[15] requires that financial institutions must include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message throughout the payment chain. Regulation 17 outlines requirements for wire transfers.

In relation to inward/outward remittance transactions, effective procedures for obtaining satisfactory evidence of the identity of applicants for business shall include:

- Transaction reference number;
- Transaction type, currency, amount and value date of the remittance;
- Date of remitter's instructions;
- Instruction details (including name, address and account number of beneficiary, name and address of beneficiary bank, and remitter's message to beneficiary, if any);
- Name, identity card number (or any other document of identity or travel document number with place of issue) of remitter or his representative must be verified if he appears in person;

[15] FATF Special Recommendation VII was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting such misuse when it occurs.

- Telephone number and address of remitter.

Reporting institutions should conduct enhanced scrutiny of and monitor for suspicious activity, any funds transfers that do not contain complete originator information- i.e. name, address and account number. Should problems of verification arise that cannot be resolved, or if satisfactory evidence is not produced to or obtained by a reporting institution, it should not proceed any further with the transaction unless directed in writing to do so by the TRA and must report the attempted transaction to the TRA as a suspicious transaction.

Introduced Business

The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some instances, reporting institutions may rely on the procedures undertaken by other institutions or introducers when business is being referred. In doing so, reporting institutions risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. In accordance with Regulation 10(6), relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the reporting institution to know its customers and their business. Reporting institutions should not rely on introducers that are subject to weaker standards than those governing the institution's own KYC procedures or that are unwilling to share copies of due diligence documentation.

Regulation 10 outlines the requirements that if a reporting institution relies on an intermediary or third party, the reporting institution should:

a) Satisfy itself that the intermediary is regulated and supervised and has measures in place to comply with the requirements of Part 2 of the Regulations;

b) Ensure that copies of identification documents and other relevant documents will be made available to it upon request without delay;

c) Immediately obtain the information required under Part 2 of the Regulations.

To assist reporting institutions, it is suggested that reporting institutions use the following criteria to determine whether an introducer can be relied upon:

- It must comply with the minimum customer due diligence practices identified in the MLPC legislations and this Guideline;

- The customer due diligence procedures of the introducer should be as rigorous as those which the reporting institutions would have conducted itself for the customer;

- The reporting institution must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer by auditing and reviewing the systems put in place by the introducer;

- All relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the reporting institution, which must carefully review the documentation provided to ensure that it has met its statutory obligations under the MLPC legislations. (Such information must be available for review by supervisory authorities such as the National Reserve Bank of Tonga, and the TRA, where appropriate legal authority has been obtained).

- Reporting institutions should conduct periodic reviews to ensure that an introducer that it relies upon continues to conform to the criteria set out above.

- Financial Institutions may not rely upon intermediaries identified by the Transaction Reporting Authority as non-complying with the FATF 40 and FATF 9, or the intermediaries for the financial institution has independent creditable reason to believe are not complying with the FATF 40 and FATF 9.

Regulation 10(1) states that reporting entities may apply to the TRA for authorization to rely on intermediaries such as trust or company service providers to perform the duties of Regulations 6 and 7. Permission will be granted only if the reporting entity presents a plan of internal policies and practices that comply with these Regulations.

Correspondent banking

Regulation 18 outlines the requirements for Cross Border Correspondent Banking. Correspondent accounts that merit particular care involve the provision of services in countries where the respondent banks have no physical presence. However, if banks fail to apply an appropriate level of due diligence to such accounts, they expose themselves to the range of risks identified earlier in this Guideline, and may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

Therefore it is expected that banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent’s business.

Factors to consider include:

- information about the respondent bank’s management, major business activities, where they are located and its money-laundering prevention and detection efforts;
- the purpose of the account;
- the identity of any third party entities that will use the correspondent banking services; and

- the condition of bank regulation and supervision in the respondent's country.

Banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and KYC policies.

In particular, banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a country in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks).

Furthermore, banks should not open correspondent accounts with banks that deal with shell banks. Banks should pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor KYC standards or have been identified as being "non-cooperative" in the fight against anti-money laundering. Banks should establish that their respondent banks have due diligence standards consistent with the principles outlined in this guideline, and employ enhanced due diligence procedures with respect to transactions carried out through the correspondent accounts.

Banks should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf (e.g. payable-through accounts). Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria for introduced business.

Regulation 18(2)(f) states that a bank shall not enter into a correspondent banking relationship without seeking the prior approval of the Transaction Reporting Authority.

Politically exposed persons

Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials. The FATF defines a PEP as an individual who has been entrusted with prominent public functions in a "foreign country". However, reporting institutions are strongly encouraged to apply similar standards to domestic PEPs.

Accepting and managing funds from PEPs that are related to crime will severely damage a reporting institution's own reputation and can undermine public confidence in the ethical standards of Tonga's financial system. In addition, a reporting institution may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, a reporting institution and/or its officers and employees themselves can be

exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

As part of a reporting institution's duty to verify a customer's identification, reporting institutions should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is a PEP. Reporting institutions should investigate the source of funds before accepting a PEP. The decision to establish a business relationship with a PEP should be taken at a senior management level.

2.6 Monitoring and Risk Management

On-going Monitoring of Accounts and Transactions

Reporting institutions should monitor transactions. On-going monitoring is an essential aspect of effective KYC procedures. Reporting institutions can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity.

Without such knowledge, reporting institutions are likely to fail in their duty to report suspicious transactions where they are required to do so under the MLPCA. The extent of the monitoring needs to be risk-sensitive. For all accounts, reporting institutions should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits and from high risk countries. Certain types of transactions should alert reporting institutions to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account.

Regulation 13 sets out the requirements for reporting institutions in monitoring of customer transactions.

Risk Management

Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of the reporting institution should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the reporting institution for ensuring that the institution's policies and procedures are managed effectively. The channels for reporting suspicious transactions to the TRA as required under the MLPCA should be clearly specified in writing, and communicated to all personnel. Regulation 3 states that reporting institutions should establish internal procedures for assessing whether they are compliant with their statutory obligations under the MLPC legislations.

Reporting institutions are encouraged to appoint or nominate a compliance officer who is responsible for ensuring the institution's overall compliance with the MLPC legislations.

Reporting institution's internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. The TRA expects that a

reporting institution's compliance function should provide an independent evaluation of the institution's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors, if it believes management is failing to address KYC procedures in a responsible manner.

Internal audit plays an important role in independently evaluating the risk management and controls, through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training.

External auditors also have an important role to play in monitoring reporting institutions' internal controls and procedures, and in confirming that they are in compliance with the requirements of the MLPC legislations.

A risk based approach to Customer Due Diligence (CDD)

CDD should be applied on a risk basis, and to be effective it must include enhanced CDD for higher risk customers and may include simplified CDD for lower risk customers.

To assist reporting institutions determine the appropriate level of due diligence to be conducted on customers, they should create a profile for each customer of sufficient detail to enable it to implement the CDD requirements of the MLPC legislations.

The customer profile should be based upon sufficient knowledge of the customer, including the customer's proposed business with the reporting institution, and where necessary the source of customer funds. Reporting institutions must apply enhanced CDD for customers that are likely to pose a higher risk of money laundering or terrorist financing ("enhanced CDD") including, but not limited to politically exposed persons. Enhanced CDD must include reasonable measures to establish the source of wealth and source of funds of customers. Enhanced CDD must be applied to higher risk customers at each stage of the CDD process. The general rule is that customers must be subject to the full range of customer due diligence measures as provided in the MLPC legislations. In certain circumstances where the risk of money laundering or terrorist financing is lower or, where information on the identity of the customer and the beneficial owner is publicly available, or where adequate checks and controls exist elsewhere in national systems, simplified measures may be employed.

As noted above, there should be intensified monitoring for higher risk accounts. Every reporting institution should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors. For higher risk accounts:

- Reporting institutions should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. For example,

the types of reports could include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the reporting institution.

- Reporting institutions should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them. As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

Staff Recruitment and Training

Reporting institutions must put in place screening procedures to ensure high standards when hiring employees and to prevent the employment of persons convicted of offences involving fraud and dishonesty.

Employee screening procedures must ensure that:

- employees have the high level of competence necessary for performing their duties;
- employees have appropriate ability and integrity to conduct the business activities of the reporting institution;
- potential conflicts of interests are taken into account, including the reporting background of the employee;
- fit and proper and code of conduct requirements are defined;
- persons charged or convicted of offences involving fraud, dishonesty or other similar offences are not employed by the reporting institutions.

Extraterritorial Application

Reporting institutions shall ensure that the requirements set out on this Guideline are also applied by their branches and subsidiaries located outside of the Kingdom. Any local prohibition to the application of these requirements shall be reported to the TRA.

PART III – BANKS, FIDUCIARY SERVICE PROVIDERS AND INSURERS

This part of the Guideline summarises some of the potential risks of money laundering and terrorist financing for banks, fiduciary service providers and insurers.

3.1 Banks

Essential Elements of Know-Your-Customer Requirements

All banks are required to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements. Certain key elements should be included by banks in the design of KYC programmes. Such essential elements should start from the banks' risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) risk management. Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit.

Customer acceptance policy

As outlined in Part 2 of this Guideline, banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers, e.g. customers from jurisdictions which have weak anti-money laundering requirements or are considered to be high risk because organized criminal activities are prevalent.

Customer identification

Customer identification is an essential element of KYC standards and these are outlined in Part 2 of this Guideline. As providers of a wide range of money transmission and lending services, banks are vulnerable to being used in the layering and integration stages of money laundering as well as the placement stage. Electronic funds transfer systems increase the vulnerability by enabling cash deposits to be switched rapidly between accounts in different names and different jurisdictions.

Banks will additionally be susceptible to the attention of the more sophisticated criminal organisations and their "professional money launderers". Such organisations, possibly under the

disguise of front companies and nominees, will create large scale but false international trading activities in order to move their illicit monies from one country to another. They will create the illusion of international trade using false/inflated invoices to generate apparently legitimate international wire transfers and will use falsified/bogus letters of credit to confuse the trail further. Many of the front companies may even approach their bankers for credit to fund the business activity. Financial institutions offering international trade services should be on their guard for laundering by these means.

Hence, vigilance should govern all the stages of the bank's dealings with its customers including:

a) Account opening;

b) Non-account holding customers;

c) Safe custody and safe deposit boxes;

d) Deposit –taking; and

e) Lending.

Account Opening

In the absence of a satisfactory explanation the following should be regarded as suspicious customers:

a) A customer who is reluctant to provide usual or customary information or who provides only minimal, false or misleading information; or

b) A customer who provides information which is difficult or expensive for the bank to verify.

Non-account holding customers

Banks which undertake transactions for persons (and any underlying beneficial owners) who are not account holders should be particularly careful and subject such clients to the same customer due diligence requirements as it would for existing customers.

Safe custody and safe deposit boxes

Particular precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the identification and verification procedures set out in these Guidelines should be followed.

Deposit Taking

A deposit taking transaction is a common method used by criminals to legitimise their illegal proceeds through the financial system. Financial institutions must therefore ensure that all the necessary information regarding the identity of the customer are obtained at the outset in order to provide assurance of the genuine transaction.

Lending

It needs to be borne in mind that loan and mortgage facilities (including the issuing of credit and charge cards) may be used by launderers at the layering or integration stages of money laundering.

3.2 Fiduciary Services

For the purpose of this section of the Guidelines:

i. "Fiduciary services" comprise any of the following activities carried on as a business, either in a single form or in combination:

   - Formation and/or administration of trusts;
   - Acting as corporate and/or individual trustee;
   - Formation and/or administration of foreign registered companies;
   - Provision of corporate and/or individual directors;
   - Opening and/or operating bank accounts on behalf of clients; or
   - Trustee company business.

ii. "Fiduciary services provider" means any person or body of persons, corporate or unincorporated, who are engaged in fiduciary services.

iii. "Foreign regulated institution" means an entity-

   - That is incorporated in, or if it is not a corporate body, has its principal place of business in a jurisdiction outside Tonga (its "home jurisdiction");
   - That carries on relevant financial business in its home jurisdiction; and
   - That is subject to obligations in its home jurisdiction that are at least equivalent to Tonga's legislation, regulations and Guidelines.

Trust, nominee and fiduciary accounts are a popular vehicle for criminals wishing to avoid the identification procedures and mask the origin of the proceeds of crime they wish to launder. Trusts and corporate entities created in jurisdictions without equivalent money laundering procedures to those in Tonga will warrant additional enquiries and vigilance.

Fiduciary service providers must take reasonable measures to establish and verify the identity of the ultimate beneficial owner or beneficiary on whose behalf an applicant for business is acting. The trustees/nominees should therefore be asked from the outset the capacity in which they are operating or making application.

3.3 Insurance and Other Investment Business

Although it may not appear obvious that insurance and retail investment products might be used for money laundering purposes, vigilance is necessary throughout the financial system to ensure that non-traditional banking products and services are not exploited.

Intermediaries and product providers who deal direct with the public may be used at the initial placement stage of money laundering, particularly if they receive cash. Premiums on insurance policies may be paid in cash with the policy subsequently being cancelled in order to get a return of premium, or an insured event may occur resulting in a claim being paid out.

Retail investment products are, however, more likely to be used at the layering and integration stages. The liquidity of a unit trust may attract money launderers since it allows them quickly and easily to move their money from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy.

Lump sum investments in liquid products are clearly most vulnerable to use by money launderers, particularly where they are of high value. Payment in cash is likely to merit further investigation, particularly where it cannot be supported by evidence of a cash-based business as the source of funds.

Insurance and investment product providers and intermediaries, including agents and brokers, should therefore keep transaction records that are comprehensive enough to establish an audit trail. Such records can also provide useful information on the people and organisations involved in laundering schemes.

PART IV – SPECIFIC GUIDELINES FOR DIFFERENT CLASSES OF REPORTING INSTITUTION

This section of the Guideline outlines information for specific classes reporting institutions to meet their obligations under the MLPCA. Examples of suspicious transactions are also provided for information.

Separate appendices address minimum requirements for the following reporting institutions:

- Banks licenced under the Financial Institutions Act 2004.
- Insurance companies, agents and brokers
- Money remittance/services businesses

4.1 INFORMATION FOR BANKS

The following summary of the legislative requirements under the MLPCA applies to you if you are a banks licenced under the Financial Institutions Act 2004.

Reporting

Suspicious Transactions - You must report where there are reasonable grounds to suspect that a transaction or an attempted transaction is related to the commission or attempted commission of a money laundering offence. (Refer to Part 5 for a copy of the TRA's suspicious transaction report).

Record Keeping

Records of all transactions must be maintained in accordance with the requirements of section 14(3) of the MLPCA. You must keep the following records:

- Signature cards
- Copies of official corporate records (binding provisions)
- Account holder information
- Account operating agreements
- Deposit slips
- Debit and credit memos
- Account statements
- Cleared cheques drawn on or deposited to an account
- Client credit files
- Foreign currency exchange transaction tickets
- A copy of the trust deed and settlor's identification (trust companies)
- Intended use of an account (except for credit card accounts)
- Credit card account records
- Copies of the suspicious transaction reports
- Records for the sale of traveller's cheques, money orders or other similar negotiable instruments
- Records for money orders redeemed
- Records for certain funds transfers that you send at the request of a client and include information with certain transfers
- Beneficial ownership records
- Correspondent banking relationship records

Identification requirements

You must take specific measures to identify the following individuals or entities:

- Any individual who signs a signature card

- Any corporation or other entity for which you open an account (including reasonable measures to obtain beneficial ownership information)
- Any settlor or co-trustee (trust companies)
- Any individual for whom you issue or redeem traveller's cheques, money orders or other similar negotiable instruments, unless a signed signature card exists
- Any individual who requests a funds transfer, unless a signed signature card exists
- Any individual for whom you have to send a suspicious transaction report (reasonable measures and exceptions apply)
- Any individual or entity for which you open a credit card account (including reasonable measures to obtain beneficial ownership information)

Third Party Determination

Where a cash transaction record is required, or when a signature card or account operating agreement is created, you must take reasonable measures to determine whether the individual is acting on behalf of a third party.

In cases where a third party is involved, specific information about the third party and their relationship with the individual providing the cash or the account holder must be obtained.

Compliance Regime

The following five elements must be included in a compliance regime:

- The appointment of a compliance officer
- The development and application of written compliance policies and procedures
- The assessment and documentation of risks of money laundering and measures to mitigate high risks
- Implementation and documentation of an ongoing compliance training program
- A documented review of the effectiveness of policies and procedures, training program and risk assessment

Implementation of KYC standards in a cross-border context

The National Reserve Bank of Tonga expects banking groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as trust companies, and have a routine for testing compliance against both home and host country KYC standards in order for their programs to operate effectively globally. Such compliance tests will also be tested by external auditors and supervisors. Regulations 4 & 27 set out requirements for branches and subsidiaries.

However small an overseas establishment is, a senior officer should be designated to be directly responsible for ensuring that all relevant staff are trained in, and observe, KYC procedures that

meet both home and host standards. While this officer will bear primary responsibility, internal auditors and compliance officers from both local and head offices as appropriate should support him/her.

Examples of Suspicious Transactions

Account transactions

Transactions conducted through accounts operated in the following circumstances may give reasonable grounds for suspicion:

- Customers who wish to maintain a number of trustee or client accounts that do not appear consistent with the type of business, including transactions involving nominee names.
- Customers who, for no apparent or logical reason, have numerous accounts and deposit cash to each of them in circumstances where the total credit, if or when combined together, would be a large amount.
- Customers who have active accounts with several financial institutions within the same locality, particularly when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of funds.
- Matching payments paid-out with credits paid-in by cash on the same or previous day.
- Payments in large third party cheques endorsed in favour of the customer.
- Customers who give conflicting information to different staff members.
- Large cash withdrawals from a previously inactive account, or from an account which has just received an unexpected large credit from abroad.
- Reluctance to use normal banking facilities, for example, avoiding high interest rate facilities for large balances.
- Large number of individuals making payments into the same account without adequate explanation.
- Customers who appear to be acting together, simultaneously using separate tellers to conduct large cash transactions or foreign exchange transactions.
- Company representatives who avoid contact with bank staff when opening accounts or making business transactions.
- Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.
- Transactions involving customers who are suspected of having attempted to open accounts in fictitious names or in the names of other persons (including cases where accounts failed to be opened due to the absence of identifications or any other reason).

  Particularly, cases where customers act in the following ways with regard to their personal identification when opening their accounts:

  a. Cases where customers refuse to present their personal identification documents (including cases where customers desire to establish their identity through means other than their personal identification documents without any rational reasons).

b. Cases where customers submit copies of their personal identification documents while refusing to present the originals.
c. Cases where customers provide doubtful or unclear information.
d. Cases where customers take procedure to open accounts in the names of other persons (including cases where bank officials in the personal identification process find that the customers taking procedures to open accounts are different from the persons whose names are to be used for the accounts)

- Transactions involving accounts bearing the names of corporations that are suspected or never having existed. Especially, cases where bank officials, during contact with such corporations after their accounts were opened, suspect faults in their identification information (addresses, telephone numbers, etc.) that had been presented when opening the accounts.
- Transactions involving customers who wish to have cash cards sent to destinations other than their addresses or refuse to have any bank notice sent to their addresses.
- Transactions involving customers who have tried to open accounts by mail-order without success due to the absence of personal identification.
- Transactions involving customers who attempt to open multiple accounts,.
- Transactions involving customers who have been found to have multiple accounts.
- Transactions involving customers who have no convincing reasons to make transactions at a particular branch. For example, such customers include those who, while being able to make transactions at branches close to their residence, are doing so at branches further away.
- Transactions involving accounts that have not been active for a long time and suddenly experiences large deposits and withdrawals.
- Transactions that are unusual from the viewpoint of economic rationality. For example, cases where customers with large deposits refuse to invest them in higher-yield products.
- Transactions involving customers who refuse to explain reasons or submit information when requested to verify the intended beneficiary and clear the suspicion regarding whether or not the customer is acting on its own behalf. These transactions include those that are made by representatives of customers and are expected to benefit other than the customers.
- Transactions that are made by employees of financial institutions or their relatives to benefit parties that are unknown.
- Transactions where employees of financial institutions are suspected of committing crimes
- Transactions where deposits are made with forged or stolen money or securities and the customers are suspected of knowing that the money or securities are forged or stolen.
- Transactions involving customers who emphasise the secrecy of the deals and customers who attempt to ask, force or bribe staff not to report deals to authorities.

- Transactions that are identified as unusual by staff based on their knowledge and previous experience, and transactions involving customers whose attitudes or actions are identified as unusual by staff based on their knowledge and previous experience.

Cash Transactions

Cash transactions involving the following types of activities may give reasonable grounds for suspicion:

- Company accounts that are dominated by cash transactions, for example, an absence of other monetary instruments normally associated with commercial businesses, such as cheques or credit cards.
- Frequent exchanges of cash into other currencies, where there appears to be no logical explanation for such activity.
- Transfers of large sums of money to or from overseas locations with instructions for payment in cash.
- Accounts operated by customers who refuse to provide appropriate identification or use misleading identification, or make it difficult to verify information. Bank accounts may be opened with forged documentation, which is difficult to detect.
- Several transactions conducted on the same day and at the same branch of a financial institution with a deliberate attempt to use different tellers.
- Cash deposits or withdrawals fall consistently just below occasional transaction thresholds. This practice is commonly referred to as structuring or smurfing and is often used to avoid threshold amounts that trigger identification requirements.
- Transactions where large deposits and withdrawals (including trading in securities, remittances and exchanges; the same hereinafter) are made in cash (including foreign currencies; the same hereinafter) or by cheque.
- Transactions that are made frequently in short periods of time and accompanied by large deposits and withdrawals made in cash or by cheque.
- Transactions where large amounts of small-denomination coins or bills (including foreign currencies) are deposited or exchanged.
- Transactions involving large cash deposits into night safe facilities or rapid increases of amount.

Customer Characteristics

Unusual transactions that are out of character with known customer routines or behaviour may give reasonable grounds for suspicion:

- Stated occupation of an individual does not correspond with the type or size of transactions conducted.
- Unusual discrepancies in identification, such as, name, address or date of birth.
- Individuals involved in cash transactions who share addresses, particularly when the addresses are also business locations.

- Customers seemingly acting together simultaneously using separate tellers to conduct large cash transactions or foreign exchange transactions.
- Company representatives who avoid contact with bank staff when opening accounts or making business transactions.

Deposits and Withdrawals

The following types of deposits and withdrawals may give reasonable grounds for suspicion:

- Inactive accounts that contain a minimal sum and then unexpectedly receive a deposit, or several deposits, followed by constant withdrawals that continue until the sum has been completely removed.
- Deposits that contain counterfeit notes or forged instruments, as well as cash that has an unusual appearance or smell.
- Large cash deposits using automatic teller machines (ATMs) or drop boxes to avoid direct contact with bank staff.

International Transactions

The following types of off-shore international activity may give reasonable grounds for suspicion:

- Use of letters of credit and other methods of trade finance to move money between countries, where such trade is not consistent with the customer's usual business.
- Customers who make regular, large payments, including electronic transfers, that are unable to be clearly identified as genuine transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs or transnational crimes; or tax haven countries.
- Build up of large balances, not consistent with the known turnover of customer's business, and subsequent transfer to accounts held overseas.
- Unexplained electronic fund transfers by customers on an in-and-out basis or without passing through an account.
- Frequent cashing of travellers' cheques or foreign currency drafts, particularly if originating from overseas.

Wire transfers

Wire transfers have long been considered one of the more popular and convenient means of transferring money across international borders. The speed and sheer volume in which wire transfers are carried out makes them an ideal mechanism for criminals to hide transactions.

Examples of potentially suspicious wire transfers include:

- Multiple personal, business or non-profit organisation accounts are used to collect then channel funds to a small number of foreign recipients.

- 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.

Loan transactions

The following scenarios may give reasonable grounds for suspicion:

- 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.

4.2 INFORMATION FOR INSURANCE COMPANIES, BROKERS & AGENTS

The following summary of the legislative requirements under the MLPCA applies to you if you are an insurance company, broker or agent.

Insurance companies operating in, or from within Tonga, should also ensure that agents who act on its behalf to sell insurance policies comply with the requirements of the MLPCA and this Guideline.

Reporting

Suspicious Transactions - You must report where there are reasonable grounds to suspect that a transaction or an attempted transaction is related to the commission or attempted commission of a money laundering offence. (Refer to Part 5 for a copy of the TRA's suspicious transaction report).

Record Keeping

You must keep the following records:

- Client information records
- Copies of official corporate records (binding provisions)
- Copies of suspicious transaction reports
- Beneficial ownership records

Identification requirements

You must take specific measures to identify the following individuals or entities:

- Any individual or entity that purchases an annuity or life insurance policy (including reasonable measures to obtain beneficial ownership information for an entity)
- Any individual for whom you have to send a suspicious transaction report (reasonable measures and exceptions apply)

Third Party Determination

You must take reasonable measures to determine whether the client is acting on behalf of a third party where a client purchases an annuity of life insurance policy.

In cases where a third party is involved, you must obtain specific information about the third party and their relationship with the individual providing the cash or the client.

Compliance Regime

The following five elements must be included in a compliance regime:

- The appointment of a compliance officer
- The development and application of written compliance policies and procedures
- The assessment and documentation of risks of money laundering and measures to mitigate high risks
- Implementation and documentation of an ongoing compliance training program
- A documented review of the effectiveness of policies and procedures, training program and risk assessment

Examples of Suspicious Transactions

The following scenarios may give reasonable grounds for suspicion:

- 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 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 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 unfavourable conditions unrelated to his or her health or age.
- Transaction involves use and payment of a performance bond resulting in a cross border payment.
- Client requests to make a lump sum payment by a wire transfer or with a foreign currency.
- The transfer of the benefit of a product to an apparently unrelated third party.
- Client establishes a large insurance policy and within a short time period cancels the policy, requests the cash value returned payable to a third party.
- Introduction of a client by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where organized criminal activities are prevalent.

4.4 INFORMATION FOR MONEY REMITTANCE/SERVICES BUSINESSES

Your Obligations

The following summary of the legislative requirements under the MLPCA applies to you if you are a money services business. A money services business means an individual or an entity that is engaged in the business of any of the following activities:

- foreign exchange dealing;
- remitting or transmitting funds by any means or through any individual, entity or electronic funds transfer network; or
- issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments.

Money services businesses include alternative money remittance systems (such as Hawala), etc.

Reporting

Suspicious Transactions - You must report where there are reasonable grounds to suspect that a transaction or an attempted transaction is related to the commission or attempted commission of a money laundering offence. (Refer to Part 5 for a copy of the TRA's suspicious transaction report).

Record Keeping

You must keep the following records:

- Client information records for entities with which you have an ongoing service agreement
- Foreign currency exchange transaction tickets
- Client credit files
- Internal memoranda about services to clients
- Copies of official corporate records (binding provisions)
- Records for the sale of travellers' cheques, money orders or other similar instruments
- Records for money orders cashed
- Records about individuals who sign an ongoing service agreement on behalf of an entity
- Lists of employees authorized to order transactions under ongoing service agreements
- Copies of suspicious transaction reports
- Records for the remittance or transmission of funds and include information with these transfers
- Beneficial ownership records

Identification requirements

You must take specific measures to identify the following individuals or entities:

- Any individual who conducts a transaction for the issuance or redemption of travellers' cheques, money orders or other similar negotiable instruments
- Any entity with which you have an ongoing business relationship
- Any individual who conducts a foreign currency exchange transaction
- Any entity for which you have to keep a client information record (including reasonable measures to obtain beneficial ownership information)
- Any individual who conducts a transaction for the remittance or transmission of funds by any means or through any individual or entity
- Any individual for whom you have to send a suspicious transaction report

Third Party Determination

Where a large cash transaction record is required, you must take reasonable measures to determine whether the individual is acting on behalf of a third party. When a client information record is created, you must take reasonable measures to determine whether the client is acting on behalf of a third party.

In cases where a third party is involved, you must obtain specific information about the third party and their relationship with the individual providing the cash or the client.

Compliance Regime

The following five elements must be included in a compliance regime:

- The appointment of a compliance officer
- The development and application of written compliance policies and procedures
- The assessment and documentation of risks of money laundering and measures to mitigate high risks
- Implementation and documentation of an ongoing compliance training program
- A documented review of the effectiveness of policies and procedures, training program and risk assessment

Examples of Suspicious Transactions

The following scenarios may give reasonable grounds for suspicion:

- Client requests a transaction at a foreign exchange rate that exceeds the posted rate.
- Client wants to pay transaction fees that exceed the posted 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 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.
- Transactions in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Transactions where customers transfer large sums of money to overseas locations with instructions to the foreign entity for payment in cash.
- Transactions where customers receive large sums of money from an overseas location via electronic funds transfer that include instructions for payment in cash.
- Transactions where customers makes frequent or large electronic funds transfers for persons who have no account relationship with the institution.
- Transactions where customers receive electronic funds transfers and immediately make a payment to a third party which is inconsistent with or outside the normal course of business for the client.
- Transactions where customers instruct the financial institution 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.
- Transactions where customers send frequent wire transfers to foreign countries, but appear to have connection to destination country.
- Transactions where sending entities having no apparent business connection with recipient.
- Transactions where the size of electronic transfers is out-of-keeping with normal business transactions for that client.
- Transaction which have no information about the beneficial owner or originator when the inclusion of this information would be expected.
- Transactions where the stated occupation of the customer 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 electronic transfers).

- Transactions involving customers who are based in jurisdictions, which do not cooperate with international anti-money laundering efforts. (“Non-cooperative countries and territories (NCCTs)”) or are shipping illegal drugs.
- Transactions involving customers introduced by parties (including corporations) based in NCCTs or jurisdictions, which are shipping illegal drugs.

PART V – TRA REPORTING FORMS

The following form has been issued by the Transaction Reporting Authority to enable financial institutions to meet their reporting obligations under the MLPC legislations.

Copies of this form can be obtained from the TRA.

FORM 1 - SUSPICIOUS TRANSACTION REPORTING FORM

STR form.pdf

For more information about:

Egmont Group refer to http://www.egmont.org/about_egmont.pdf

APG refer to http:// www.apgml.org/

United Nations Conventions refer to http://www.incb.org/e/conv/menu.htm.

For more information about money laundering, you can also refer to the following web sites:

* United Nations Office of Drug Control and Crime Prevention (http://www.odccp.org/money_laundering.html);
* Australian Transaction Reports Analysis Centre

  (http://www.austrac.gov.au/);
* International Money Laundering Information Network (http://www.imolin.org/);
* Moneylaundering.com (http://moneylaundering.com/)