MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION

GUIDELINES FOR THE FINANCIAL SECTOR

MONEY LAUNDERING PREVENTION AUTHORITY
CENTRAL BANK OF SAMOA
PRIVATE BAG
APIA
SAMOA

April 2010

Contents

EXPLANATORY FOREWORD

The Money Laundering Prevention Act 2007 (MLPA), the Money Laundering Prevention Regulations 2009 (MLPR) and the Prevention and Suppression of Terrorism Act 2002 (PSTA) makes money laundering and the financing of terrorism a criminal offence. These Acts are important pieces of legislation, which require conscientious application by all concerned for the sake of Samoa's reputation as a responsible jurisdiction and to maintain the integrity of our financial system.

The Governor of the Central Bank of Samoa (CBS) is the Money Laundering Prevention Authority (the "Authority") appointed under Section 4(2) of the MLPA to implement and regulate the provisions of the Act, until such time as the Minister makes a further appointment.

The Money Laundering Prevention Task Force is established under section 5 of the MLPA and is the advisory body to the Money Laundering Prevention Authority. Its objectives include ensuring close liaison between Government agencies, departments and the Financial Intelligence Unit and making recommendations to the Authority in respect of issues relating to money laundering or the financing of terrorism.

The Money Laundering Prevention Authority (the "Authority") is required to produce Guidelines to enable financial institutions or any other person(s) (whether incorporated or unincorporated) to recognize and deal with the criminal offence of money laundering.

This Guideline is issued by the Authority to:

- Outline the requirements of the Money Laundering Prevention Act 2007 (the "MLPA") and the Money Laundering Prevention Regulations 2009 (the "MLPR");
- Provide a practical interpretation of the requirements of the Act and Regulations;
- Give examples of good practice; and
- Assist management of financial institutions in developing policies and procedures appropriate to their business.

The guideline is issued under section 4(3) of the MLPA and is provided as general information only. It is not a legal advice and is not intended to replace the MLPA or MLPR. Financial institutions should seek their own independent legal advice on the interpretation and requirements of the MLPA and the MPLR.

Financial institutions are expected to be aware of the requirements of the MLPA and MLPR. The role of the Authority, the Samoa Financial Intelligence Unit (SFIU) and other supervisory agencies in Samoa such as the Central Bank of Samoa, the Samoa International Finance Authority and the Samoan Institute of Accountants is to ensure compliance with the requirements of the MLPA and MLPR. These agencies will, when assessing compliance of financial institutions, take into consideration the size and complexity of the financial institution.

Financial institutions' reporting of suspicious transactions is a cornerstone of the Financial Action Task Force (FATF)[1] 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. Financial institutions are not being asked or expected to assume the role of law enforcers. A positive approach to Samoa's legislative requirements, however, will greatly improve the efforts of those agencies responsible for enforcement.

These Guidelines will be reviewed periodically to reflect changing circumstances and experiences and to provide additional clarification concerning matters where queries arise. More generally, the Authority will work closely with other bodies in Samoa, such as the Central Bank of Samoa and the Samoa International Finance Authority, to ensure that Samoa's system to combat financial crime and terrorist financing meets international requirements.

The **Scope** of these Guidelines covers "financial institutions" which are defined in Schedule 1 the MLPA. **Terminology** used in this Guideline is consistent with the MLPA and the MLPR.

These Guidelines have been written in several sections:

- Part 1 gives an overview of the powers of the SFIU and obligations placed on financial institutions.
- Part 2 provides information on money laundering and terrorist financing.
- Part 3 outlines key elements of developing effective policies and procedures to assist financial institutions comply with their statutory obligations.
- Part 4 includes a series of appendices which briefly summarises requirements for each class of financial institution along with examples of suspicious transactions.
- Part 5 includes a copy of the suspicious transaction reporting (STR) form that financial institutions are required to complete pursuant to the MLPA.

Financial institutions should contact the SFIU to discuss aspects of these guidelines and any problems or questions arising from the MLPA or MLPR.

Money Laundering Prevention Authority

Phone: (685) 34132, 34130
Facsimile: (685) 20293
Email: cbs@lesamoa.net

1 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.

PART 1 – THE FINANCIAL INTELLIGENCE UNIT AND OBLIGATIONS PLACED ON FINANCIAL INSTITUTIONS

The Financial Intelligence Unit

Section 6 of the MLPA establishes the Samoa Financial Intelligence Unit (SFIU). The SFIU is the principle point of contact for all issues relating to AML/CFT.

Section 7 of the MLPA sets out the functions and powers of the SFIU and, these include but are not limited to:

i) Receiving reports furnished by financial institutions or any person, whether incorporated or unincorporated, on suspicious or unusual transactions. The SFIU considers and obtains more information, as it may require. In terms of section 7(2) of the MLPA, where the FIU has reasonable grounds to suspect that money laundering or terrorist financing is involved, it may apply to the Court for an order to temporarily freeze the funds affected by the transaction or attempted transaction;

ii) Liaising with law enforcement agencies both within Samoa and abroad in respect of transactions involving money laundering or terrorist financing;

iii) Ensuring compliance by financial institutions with the requirements of the MLPA and this Guideline;

iv) Giving instructions to facilitate an investigation; and

v) Compiling statistics, issuing guidelines or giving advice to the Minister and the Attorney General.

Section 10 of the MLPA gives the SFIU, or any person it authorizes in writing, the power to examine the records and inquire into the business and affairs of any financial institution for the purpose of ensuring compliance with the Act or Guidelines.

Section 11(2) of the MLPA provides that the SFIU may direct any financial institution that has without reasonable excuse failed to comply in whole or in part with its obligations under the Act, to implement any action plan to ensure compliance with its obligations under the MLPA. Where a financial institution fails to comply with a directive issued by the SFIU, it may, upon application to the Courts, obtain an order against any or all officers or employees of the financial institution.

Obligations of Financial Institutions

The MLPA and MLPR impose requirements on financial institutions related to reporting of transactions, record keeping, monitoring of transactions, implementation of policies and procedures, staff awareness and customer identification. Aspects of these requirements are outlined in Part 3 of this Guideline to provide assistance to financial institutions to ensure compliance with their statutory obligations.

The SFIU acknowledges that financial institutions subject to the requirements of the MLPA and MLPR operate in different markets with different risks and therefore policies and procedures will vary between firms. Regardless of the size of the organisation or the nature of its activities, internal controls should address the following:

- *Vulnerability:* Provide increased focus on a financial institution's operations (e.g. services, clients and geographic locations) that are more vulnerable to abuse by money launderers.
- *Risk Assessment:* Provide for a periodic review of the risk assessment and management processes, taking into account the environment within which the financial institution operates and the activity in the business environment.
- *Implementation:* Implement risk-based Customer Due Diligence, policies, procedures and processes.
- *Higher risk clients:* Provide for adequate controls for higher risk clients and services as necessary, such as limits on the activity/service offer or management approvals.
- *Responsibility:* Designate an individual or individuals at an appropriate level who is/are responsible for managing compliance with the MLPA.
- *Compliance:* Provide for an AML/CFT compliance function and review program if appropriate given the scale of the organisation and the nature of the reporting institution's business.
- *Common controls:* For those firms, which are part of groups, to the extent possible there should be a common control framework.
- *Feedback:* Inform the principals of compliance initiatives, identified compliance deficiencies and corrective action taken.
- *Continuity:* Provide for continuity in the event of changes to management or employees.
- *Updates:* Focus on meeting all statutory record keeping and reporting requirements, recommendations for AML/CFT compliance and provide for timely updates in response to changes to legislation and the SFIU's requirements.
- *Staff supervision:* Provide for adequate supervision and support for staff activity that forms part of the organisation's AML/CFT compliance program.
- *Staff roles:* Incorporate AML/CFT compliance into job descriptions and performance evaluations of relevant personnel.
- *Training:* Provide for appropriate training to be given to all relevant staff.

Penalties and Offences

The MLPA and MLPR impose severe penalties on financial institutions and their employees. Breaches of Samoa's legislation can result in financial institutions and their imposed being subject to a range of penalties which, upon conviction, include fines and imprisonment or both.

Key aspects are summarized below. However, financial institutions should ensure that they are familiar with all aspects of the legislation and the obligations placed on them to put in place policies and procedures to ensure that their services are not used by those involved in money laundering or the financing of terrorism.

Assisting persons commit the offences of money laundering or terrorist financing

The combined effect of the Money Laundering Prevention Act 2007 and the Prevention and Suppression of Terrorism Act 2002 is to make it an offence for any person to provide assistance to a criminal to obtain, conceal, retain or invest funds and to finance or assist in the financing of terrorism, if that person knows or suspects or, in the case of financing or assisting in the financing of terrorism should have known or suspected, that those funds are the proceeds of crime or to be used to carry out an act of terrorism.

Such assistance is punishable on conviction to a fine not exceeding 10,000 penalty units, or to imprisonment for a period not exceeding 7 years, or to both such fine and imprisonment for a money laundering offence and to a fine not exceeding 1,000 penalty units or to imprisonment for a term not exceeding 5 years for assisting the financing of terrorist acts.

Failure to report

It is an offence for any person who acquires knowledge or a suspicion of money laundering or terrorist financing in the course of their trade, profession, business or employment, not to report the knowledge or suspicion, as soon as it is reasonably practicable, after the information comes to his attention. Failure to report in these circumstances is punishable on conviction by a maximum fine of 500 penalty units. If the person involved is a financial institution as defined under the Money Laundering Prevention Act 2007, the licence of such financial institution may be revoked by the Central Bank or the Minister, as the case may be, pursuant to the provisions of the relevant legislation.

Tipping-off

It is an offence for anyone to take any action likely to prejudice an investigation by the relevant authorities by informing (i.e. tipping off) the person who is the subject of a suspicious transaction report, or anybody else, that a disclosure has been made or that the Police or Customs authorities are carrying out or intending to carry out a money laundering or terrorist financing investigation. The punishment on conviction for this "tipping-off" offence is a maximum of five years imprisonment or a fine not exceeding 500 penalty units or both such fine and imprisonment.

Implementation of AML/CFT in a cross border context

Banks and Insurance Companies

The Central Bank of Samoa expects banking and insurance groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations. Parent institutions 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 programmes to operate effectively globally. Such compliance tests will also be tested by external auditors and supervisors.

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.

Other financial institutions

The Authority and the SFIU expects financial institutions in Samoa which have operations outside of Samoa to follow the requirements for banks and insurance companies outlined above.

PART 2 – GENERAL INFORMATION

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;

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;

[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.

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, section 11 of the Proceeds of Crime Act 2007 goes further and defines money laundering to include:

- Engaging in a transaction that involves property, knowing or having reason to believe that it is derived from the proceeds of crime; or
- The acquisition, possession and use of property by a person or bringing into Samoa property, knowing or having reason to believe that it is derived from the proceeds of crime; or
- Concealing or disguising the true nature, source location, disposition, movement, ownership of or right with respect to property that the person knows or ought reasonably to know to be the proceeds of crime; or
- Rendering assistance to another person to covert or transfer property that the person knows or ought reasonably to know to be the proceeds of crime with the aim of concealing or disguising the illicit origin of that property.

Vulnerability of Financial Institutions to Money Laundering

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

However, criminals have learnt that unusual or large cash payments made into financial institutions can create suspicion and lead to additional enquiries. Criminals have therefore sought other means to convert the illegally earned 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 financial 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.

Financial 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 Samoa 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 Samoan Financial Intelligence Unit (SFIU) by financial institutions, the following methods and trends have been identified in Samoa:

i) Placement of alleged criminal proceeds derived from fraudulent activities which occurred overseas in bank accounts established with the local financial institution;

ii) Smuggling of cash in smaller amounts to avoid detection or attention of relevant authorities or financial institutions of any suspicious nature of transaction;

iii) The use of scam letters to mislead members of the public regarding winning large sums of money or high yields on investment.

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. Samoa 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 financial 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 willful 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) 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.
- 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.

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

The systems financial 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 financial 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 as required by section 23 of the MLPA notify the SFIU and submit a suspicious transactions report, even if the financial institution declines the transaction as a result of its own due diligence.

The SFIU, as part of its responsibilities, will regularly provide financial institutions with details of persons/entities suspected of being related to the financing of terrorism.

PART 3 – DEVELOPING AN EFFECTIVE SYSTEM

Introduction

The MLPA and MLPR impose requirements on financial institutions related to reporting of transactions, record keeping, monitoring of transactions, staff awareness and customer identification. To assist financial institutions develop internal policies and procedures to establish an effective system to combat money laundering and terrorist financing, this section of the Guideline provides guidance on the practical implementation of the requirements and intent of the MLPA and MLPR.

The Duty of Vigilance

Financial 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. Section 31(1)(b) of the MLPA requires financial institutions to establish and maintain policies and 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 MLPA;

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 SFIU;

iii) Keep records for the prescribed period of time;

iv) Train key staff to ensure that they understand their obligations under the MLPA;

v) Liaise closely with the SFIU 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 the requirements of the MLPA and the MLPR.*

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 Financial Institutions

To ensure that Samoa is not used as a channel for criminal or terrorist funds, all financial institutions should:

a) Comply with SFIU policies, regulations, directives and their statutory obligations under the MLPA and MLPR. The Directors and Management of financial institutions should ensure that SFIU 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 a 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 MLPA;

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 SFIU within any limits imposed by legislation on customer confidentiality or where there are reasonable grounds for suspecting money laundering or the financing of terrorism;

e) Implement effective procedures for customer identification, record keeping and reporting suspicious transactions. These procedures should be in line with Parts III and IV the MLPA and the Parts II, III and IV of the MLPR;

f) Screen potential employees to ensure that they are fit and proper;

g) Ensure that its officers and employees are:

- aware of Samoa's laws relating to money laundering and financing of terrorism; and

- aware of the institution's procedures and policies for compliance with anti-money laundering and combating the financing of terrorism standards; and

- trained to recognise suspicious transactions.

Money Laundering Compliance Officer

Section 31(1) of the MLPA, requires financial institutions to appoint an officer who is responsible for ensuring compliance with Samoa's requirements. It is recommended that this officer be designated as the Money Laundering Compliance Officer. In addition to ensuring that the financial institution complies with its statutory obligations, the officer should:

- Be responsible for the review and submission of suspicious transaction reports (STRs) to the SFIU;
- Be responsible for staff training in relation to money laundering and terrorist financing;
- Regularly review the financial institution's policies and procedures to ensure that these are up to date with both Samoa's requirements and international standards as outlined by the Financial Actions Task Force;
- Test policies and procedures to ensure that these are being implemented by staff of the institution; and
- Be the liaison point between the financial institution and the SFIU.

The SFIU 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.

The requirement that a financial institution appoint a compliance officer does not apply to an individual who, in the course of carrying out his/her business, does not employ or act in association with any other person (refer section 31(2) of the MLPA). This exemption *does not remove or negate obligations* on that person to report transactions that may be related to money laundering or terrorist financing to the SFIU or comply with other requirements of the MPLA and the MPLR, such as the customer and verification identification requirements and record keeping requirements.

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 SFIU, and relevant law enforcement and regulatory authorities.

Section 16 of the MLPA requires that financial institutions undertake customer due diligence measures, including identifying and verifying the identity of customers, when:

- establishing business relationships;
- carrying out occasional transactions;
- there is a suspicion of money laundering or terrorist financing;

- the financial institution has doubts about the adequacy of previously obtained customer identification data.

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

Financial institutions should 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. Section 5 of the MPLR provides financial institutions with a list of documents that are acceptable for the purposes of verifying a customer's identity.

In the case of legal persons, section 6 of the MLPR requires verification of the legal existence of the legal person by obtaining copies of the entity's certificate of incorporation and information relating to:

- the customer's name, legal form, address and its directors;
- the principal owners and beneficiaries and control structure, including identifying the natural person who ultimately owns or controls the legal person;
- provisions regulating the power to bind the entity (e.g. its Articles of Association); and
- the authorisation of any person purporting to act on behalf of the customer and the identity of the persons.

The documentation requirements for the identification of natural persons involved in the ownership or control of legal persons are the same as those specified under section 5 of the MPLR.

Know your Customer

The need for financial 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 financial 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 financial 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, financial institutions need to have a clear understanding of the legitimate business of their customers.

The procedures which financial 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.

Section 19 of the MLPA requires a financial institution to maintain accounts in the true name of the account holder. Financial 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's identity from the institution's compliance function or from supervisory authorities.

Components of an Effective System

Essential Elements of Know-Your-Customer Requirements

All financial institutions should 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 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

Financial 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.

Financial institutions should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. These policies should take into account the requirements of section 14 and 15 of the MPLR.

General Guidelines for Establishing Satisfactory Evidence of Identity

The MLPR specifies a number of documents that financial institutions must obtain as evidence of identity. *The overriding requirement is for the financial institution itself to be satisfied that it has established the true identity of the prospective customer as far as it is reasonably possible*.

A financial 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 (refer section 13(3) of the MPLA).

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. As required under section 18(3) of the MLPA, copies of the supporting evidence of a person's identity must be retained for a minimum period of five years. In addition, financial institutions must keep records of every transaction that is conducted through it and must, as required by section 18(3) of the MLPCA retain records for a period of five years after the completion of the transaction or when the account was closed or business relationship ceases.

Any subsequent changes to the customer's name, address, or employment details of which the financial 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 financial 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 18 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. However, if the financial institution has reason to suspect that the transaction is suspicious or unusual it is required under section 16(4)(a) of the MPLA to re-verify the customers identity and take measures to understand the nature and purpose of the transaction.

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

As a general rule, financial institutions should obtain satisfactory evidence of identity of a prospective customer at the time of opening an account or entering into a business relationship.

Section 10 of the MLPR allows financial institutions, in certain circumstances and where the risks of money laundering or terrorist financing are effectively managed, to delay completion of customer identification and verification in certain circumstances. *In such circumstances, unless satisfactory evidence of identity is obtained as soon as is reasonably practicable and prior to the customer carrying out another transaction with the financial institution, the financial institution should pursuant to section 17 of the MPLA not proceed any further with the business relationship or carry out a one-off transaction with the customer, unless directed to do so by the SFIU and shall report the transaction or attempted to the SFIU as a suspicious transaction*.

Some people may not have official documents, such as a passport or birth certificate or other identification documents listed in section 5 of the MLPR. 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; section 15 of the MLPR specifies requirements for financial institutions to apply simplified customer due diligence for low risk customers. This is consistent with the Basel Committee on Banking Supervision's *General Guide to Account Opening and Identification,* which provides a list of acceptable identity documents, but goes on to state that:

> *In particular jurisdictions there may be other documents (other than standard documents such as identity cards) of an equivalent nature which may be produced as satisfactory evidence of customer's identity. (paragraph 12)*
>
> *It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. (paragraph 16)*

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

What is Identity?

Section 5 of the MPLR provides an extensive list of customer identification and verification documents. Financial 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. In circumstances where customers do not have such documents, the financial institution should seek guidance from the SFIU.

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.

Financial 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, financial institutions should obtain information as to the source of funds.

Customers who are legal persons

Section 6 of the MPLR outlines requirements for financial institutions when dealing with legal persons. The following sections of the Guideline provide additional guidance for financial institutions when dealing with certain classes of customer.

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 financial 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 financial 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 Samoa, 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 Samoa.

- 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.

Financial 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.

Financial 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 financial institution may be completely unaware that the bearer shares have changed hands. Therefore, financial 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

As required by section 6(4) of the MPLR, 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.

Financial 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 financial institution's judgement of the money laundering risk involved. However if such a situation arises, the financial institution should take appropriate steps to satisfactorily identify the beneficiaries of the trust.

Non-profit organizations (NPOs)

Section 6(6) of the MLPR requires that where the customer is a non-profit organisation, group (e.g. social club) or agency the financial institution must satisfy itself as to the legitimate purpose of the organisation by reviewing the organisation's charter, constitution, or trust instrument.

In addition, to these requirements a financial institution should also identify and verify the identity of those persons authorised to act on behalf of the organisation. In this regard, procedures for establishing and maintaining business relationships with non-profit organisations should be consistent with the requirements of section 6(1) of the MLPR.

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 financial 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 financial institution's responsibility to satisfy itself that the certifier is appropriate. In all cases, the financial 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 Third Parties or Intermediaries – Introduced business

Verifying identity is often time consuming and expensive and can cause inconvenience for prospective customers. It is therefore important that as far as possible financial 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 financial 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.

Section 11 of the MLPR provides that financial institutions may rely on a third party or intermediary to perform the customer identification requirements of the MLPA and MLPR. Those financial institutions which rely upon third parties or intermediaries are required to have in place policies and procedures consistent with the requirements of the MLPR. Further, financial institutions which rely on

third parties or intermediaries should conduct periodic reviews to ensure that an introducer that it relies on meets the criteria established by the MPLR.

Consistent with section 11(6) of the MPLR, financial institutions are required on an annual basis to provide the SFIU with a list of all third parties and intermediaries upon which it relies to perform the customer identification requirements of the MPLA and MLPR.

Where either a financial institution or the SFIU, in written advice, determines that the third party or intermediary is not complying with standards comparable to those in Samoa, the financial institution should terminate its relationship with that party. In addition, the financial institution should review customer relationships (e.g. identification documentation, nature of business relationship and transactions) established through the third party or intermediary to ensure that it knows its customers and their business. Where a financial institution determines that it does not have adequate information on the customer it should take measures to obtain missing information. Should problems continue, the requirements of section 17 of the MLPA are relevant and the financial institution should contact the SFIU.

Relying on due diligence conducted by a third party or intermediary, in Samoa or in a foreign jurisdiction, however reputable, does not in any way remove the ultimate responsibility of the recipient financial institution to know its customers and their business. Financial 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 Samoa.

Exemptions from Identification Requirements

Section 16(4) of the MLPA provides limited exemptions to the identification requirements of the Act. Specifically, documentary evidence of identity will not normally be required if:

- The transaction is part of an established business relationship with person and the person has already produced satisfactory evidence of identity, *unless the financial institution suspects the transaction is suspicious or unusual*; or
- The transaction is a one-off transaction not exceeding $50,000 or its equivalent in foreign currency, *unless:*
    - There are reasonable grounds for believing that the transaction is linked to one or more other one-off transactions which in aggregate exceed $50,000 or its equivalent in foreign currency; or
    - The financial institution suspects the transaction is suspicious or unusual.

Section 4 of the MPLR provides that verification of a customer's identity is not required in certain circumstances, unless *the financial institution suspects the transaction is related to money laundering or the financing of terrorism.*

Lower Risk Customers, Jurisdictions and Business Relationships

In addition to these exemptions, section 15 of the MLPR provides that a financial institution may apply a simplified customer due diligence procedures to certain customers where the risk of money laundering or the financing of terrorism is considered to be low. Notwithstanding this:

- Financial institutions must at a minimum obtain information as required by section 15(3) of the MLPR.
- Financial institutions should ensure that where appropriate that those persons opening accounts have the authority and approval to open and operate accounts. In all cases, the financial institution should ensure that it fully understands the nature of the relationship and any transactions.
- Non resident customers may only qualify for simplified CDD if they are resident in a jurisdiction that has in place anti-money laundering and countering the financing of terrorism measures that are at a minimum equivalent to those in Samoa. Financial institutions should have in place procedures to monitor developments is those jurisdictions in cases where it decides to apply simplified CDD. Simplified CDD is not acceptable where the financial institution has reason to believe the jurisdiction does not have standards equivalent to those in Samoa. In making this determination, financial institutions should have regard to assessments published by the FATF, International Monetary Fund, World Bank and other agencies such as the Asia Pacific Group on Money Laundering of which Samoa is a member
- Should a financial institution suspect money laundering or terrorist financing it should subject the relationship (and all others from the jurisdiction) to enhanced due diligence and, as appropriate, submit a STR to the SFIU.

Higher Risk Customers, Jurisdictions and Business Relationships

Section 14 of the MLPR requires financial institutions to perform additional customer due diligence measures for categories of customer, business relationships or transactions with a higher risk of money laundering.

Staff and financial 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 SIFIU. Financial 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 financial 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 recommended that financial 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 .

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

- conduct enhanced due diligence in relation to verifying the customer's identity including those of the beneficial owner and controller;
- establish the source of that customer's wealth and funds;
- conduct regular and ongoing monitoring of the customer's transactions;
- establish a profile of the customer.

International experience identifies the following examples of higher risk customers:

- Politically Exposed Persons (PEPs) – individuals entrusted with prominent public functions.
- All non-resident customers – especially customers who are from countries or regions or industries where a high amount of crime is known to exist.
- Customers that work in certain industries or occupations where crime is known to exist.

Financial institutions must make judgments 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.
- 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.

As required by section 14(8) of the MPLR, *the decision to establish a business relationship with a high risk customer should be taken at a senior management level.*

Correspondent banking relationships

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 consistent with the requirements of section 18(1) of the MLPR, 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.

Section 18(1) of the MPLR requires that financial institutions must not enter 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). Where banks have establishing correspondent banking relationships, these should be reviewed and relationships with shell banks must be terminated.

Furthermore consistent with the intent of section 18(1), 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 though 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. Specifically, a bank shall be satisfied that the respondent bank has performed the customer due diligence required in the MLPR for those customers that have direct access to the accounts of the correspondent, and that the respondent is able to provide relevant customer identification information on request of the correspondent.

Politically exposed persons

Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a financial institution 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, *financial 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 financial institution's own reputation and can undermine public confidence in the ethical standards of Samoa's financial system. In addition, a financial 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 financial 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 financial institution's duty to verify a customer's identification, financial 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. Financial institutions should investigate the source of funds before accepting a PEP.

Non face to face Verification

Financial 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:

- Financial 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 financial institution;
- 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 Samoa, 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, financial institutions should seek to verify identity and permanent address with a reputable financial institution in the applicant's home country or country of residence.

Financial institutions should subject non-resident customers to enhanced due diligence if the customer's residency, or previous residency, suggests that they are from jurisdictions that have weaker anti-money laundering and countering the financing of terrorism standards than those of Samoa.

Wire Transfers

The FATF[3] 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.

Section 16 of the MPLR (and section 21 of the MLPA) require that those financial institutions (banks and money transmission services) must ensure that for all electronic funds transfer transactions and all other forms of fund transfers that they obtain and maintain full originator information and verifications.

As required by section 16 of the MLPR, financial 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 financial institution, the financial institution should not proceed any further with the transaction unless directed in writing to do so by the SFIU and must report the transaction to the SIFIU as a suspicious transaction.

In appropriate circumstances, beneficiary financial institutions should consider restricting or terminating business relationships with financial intuitions that do not comply with this Regulation.

[3] 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.

Monitoring and Risk Management

On-going Monitoring of Accounts and Transactions

The effect of section 20 of the MLPA is to place a requirement on financial institutions to monitor transactions. On-going monitoring is an essential aspect of effective KYC procedures. Financial 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, financial institutions are likely to fail in their duty to report suspicious transactions where they are required to do so under the MLPA. The extent of the monitoring needs to be risk-sensitive. For all accounts, financial 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. Certain types of transactions should alert financial 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 when considered against the customer's profile. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account.

Risk Management – Compliance Reviews, Internal and External Audits

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 financial institution should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. To ensure compliance with the MLPA, regulations and guidelines, financial institutions are required under section 31(1) of the MLPA to appoint a compliance officer. Policies and procedures should:

- Allocate explicit responsibility within the financial institution for ensuring that the institution's policies and procedures are managed effectively.

- Clearly specify in writing, the channels for reporting suspicious transactions to the SFIU as required under the MLPA, and this should communicated to all personnel.

- Establish internal procedures for assessing whether the institution's statutory obligations under the MLPA require the transaction to be reported to the SFIU.

Financial institution's internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. The SFIU expects that a financial institution's compliance function 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 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 financial institutions' internal controls and procedures, and in confirming that they are in compliance with the requirements of the MLPA. Where a financial institution is required to have its accounts audited, the external auditor is required under section 32 of the MLPA to report on the institution's compliance with the requirements of the MLPA. Section 20 of the MLPR provides guidance to auditors on the areas and matters to be reviewed. *The SFIU will require that a financial institution's external auditors provide it with a copy of the external audit review.*

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 financial 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 MLPCA.

The customer profile should be based upon sufficient knowledge of the customer, including the customer's proposed business with the financial institution, and where necessary the source of customer funds. Financial 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 MLPA. 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.

To assist financial institutions develop an appropriate risk-based approach to Customer Due Diligence (CDD), in June 2007 the FATF released a document entitled *Guidance on the Risk-based Approach to Combating Money Laundering and Terrorist Financing*.

As noted above, there should be intensified monitoring for higher risk accounts. Every financial 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:

- Financial 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 financial institution.

- Financial 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.

Record Keeping Requirements

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

This is an essential component of the audit trail procedures that the legislation seeks to establish. If the law enforcement agencies investigating a money laundering case cannot link criminal funds passing through the financial system with the original criminal money, then confiscation of the criminal funds cannot be made. Often the only valid role a financial institution can play in a money laundering investigation is through the provision of relevant records, particularly where the money launderer has used a complex web of transactions specifically for the purpose of confusing the audit trail.

Consistent with the requirements outlined in section 18(1) of the MLPA, a financial institution must maintain records of:

a) its transactions and related documentation;

b) a person's identity;

c) all reports made to the Unit;

d) all enquiries relating to the money laundering and the financing of terrorism made to it by the SFIU or a law enforcement agency.

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

a) the evidence of a person's identity was obtained;

b) of any transaction or correspondence;

c) the account is closed or business relationship ceases, whichever is the later.

Section 18(4) of the MLPA outlines the manner in which records may be maintained by financial institutions. These records shall be available upon request

to the SFIU and should be retrieved or reproduced in legible and useable form within a reasonable period of time. *For the purposes of this Guideline a "reasonable period of time" is taken to mean a period not exceeding five working days*.

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

Section 23 of the MLPA requires financial institutions to report to the SFIU any suspicious transaction stating the reason for the suspicion, the identity of the business involved, the transaction or any other circumstances concerning that business transaction which gives any officer or employee of the financial institution reasonable grounds to suspect that the transaction involves proceeds of crime.

Where a financial institution suspects, has reasonable grounds to suspect or has information that a transaction or attempted transaction may be related to a money laundering offence or financing of terrorism, the financial institution must as soon as practicable after forming the suspicion but no later than 2 working days, report the transaction to the FIU. This reporting requirement is outlined in Section 23(2) of the MLPA.

Section 31(1) of the MLPA requires financial institutions to appoint a compliance officer(s) to be responsible for ensuring the company's compliance with the requirements of the MLPA. The Compliance Officer(s) would be responsible for reporting suspicious transactions to the FIU in the format attached (refer Part 5).

Section 23(2) of the MLPA states that a suspicious transaction report must:

a) be in writing and may be given by way of mail, fax or electronic mail or such other manner as may be prescribed;

b) be in such form and contain such details as may be prescribed;

c) contain a statement of the grounds on which the financial institution holds the suspicion; and

d) be signed or otherwise authenticated by the financial institution.

A suspicious transaction report may be given orally, including by telephone, but a written report must be prepared in accordance with section 23(2) of the MLPA within 48 hours after the oral report is given.

Compliance Officers must keep a register of all reports made to the SFIU and all reports made internally to them by employees.

Directors, officers and employees of financial institutions are prohibited from disclosing the fact that an STR or related information is being reported to the FIU. If financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping off when performing the customer due diligence (CDD) process. If the financial institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may not choose to pursue that process, and should file an STR. Financial institutions should ensure that their employees are aware of any sensitive to these issues when conducting CDD.

All financial institutions have a clear obligation to ensure:

a) that each relevant employee knows to which person he or she should report suspicions; and

b) that there is a clear reporting chain under which those suspicions will be passed without delay to the Money Laundering Compliance Officer.

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 financial 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 financial 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. Financial 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.

Examples of suspicious transactions that may be relevant to different classes of financial institutions are included in the Part 4 of this Guideline.

Education and Training

Section 31(1)(c) of the MLPA requires that financial institutions must establish and maintain internal procedures:

- To make the institution's officers and employees aware of Samoa'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.

The Need for Staff Awareness

The effectiveness of the procedures and recommendations contained in these Guidelines 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 Samoa.

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 financial 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.

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.

Protection

Financial institutions and their employees are protected under Section 29 of the MLPA when complying with their obligations under the MLPA.

PART 4 – SPECIFIC GUIDELINES FOR DIFFERENT CLASSES OF FINANCIAL INSTITUTION

This section of the Guideline outlines some of the key requirements for some types of financial institutions and should only be taken as a guide. Financial institutions should ensure that they implement policies and procedures consistent with the requirements of the MLPA and MPLR. Examples of suspicious transactions for different types of financial institution are also provided for information.

Separate appendices address minimum requirements for persons whose regular occupation or business is the carrying out of:

- Banking business as defined in the Central Bank of Samoa Act 1984 and the Financial Institutions Act 1996 and International banking business as defined in the International Banking Act 2005.
- Insurance business transactions, including carrying on the business of an insurer or insurance intermediary.
- Credit unions.
- Trustee company, trust or corporate service provider.
- Lawyers (barristers and solicitors) and Accountants.
- Money transmission services and the issuance of means of payment
- Real Estate Agents
- Dealers in Precious Metals (Bullion), Stones and Jewellery

INFORMATION FOR BANKS & CREDIT UNIONS

The following summary of the legislative requirements under the MLPA applies to you if you are a credit union or carrying out banking business as defined in:

- The Central Bank of Samoa Act 1984; and
- The Financial Institutions Act 1996; or
- The International Banking Act 2005.

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 serious offence, a money laundering offence or a terrorist activity financing offence.

Terrorist Property - You must report where you know, or suspect, that there is property in your possession or control that is owned or controlled by or on behalf of a terrorist or a terrorist group.

Record Keeping

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.

Politically Exposed Person

You have to take reasonable measures to determine whether you are dealing with a politically exposed person for new or existing relationships. You also have to keep records and take additional measures.

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 terrorist financing, and measures to mitigate high risks including having adequate controls for higher risk customers, transactions and products/services, as necessary, such as transaction limits or management approvals. (In practical terms, this means increased focus on the bank's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals. There should be a regular review of the risk assessment and management processes, taking into account the environment within which the bank operates and the activity in its market place).
- Implementation and documentation of an ongoing compliance training program including incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- A documented review of the effectiveness of policies and procedures, training program and risk assessment

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.

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.

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.

INFORMATION FOR INSURANCE COMPANIES, BROKERS & AGENTS

The following summary of the legislative requirements under the MLPA that apply to you if you carrying out insurance transactions, including carrying on the business of an insurer or insurance intermediary.

Insurance companies operating in, or from within Samoa, should also ensure that agents who act on its behalf to sell insurance policies comply with the requirements of the MLPA, the MPLR 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 serious offence, a money laundering offence or a terrorist activity financing offence.

Terrorist Property - You must report where you know, or suspect, that there is property in your possession or control that is owned or controlled by or on behalf of a terrorist or a terrorist group.

Record Keeping

You must keep the following records:

- Client information records
- Receipts from customers unless it relates to the issuance of a compulsory third party insurance policy where the premium paid per annum is less than $500.
- 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.

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 or 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.

Politically Exposed Person

You have to take reasonable measures to determine whether you are dealing with a politically exposed person for new or existing relationships. You also have to keep records and take additional measures.

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 terrorist financing, and measures to mitigate high risks including having adequate controls for higher risk customers, transactions and products/services, as necessary, such as transaction limits or management approvals. (In practical terms, this means increased focus on the company's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals. There should be a regular review of the risk assessment and management processes, taking into account the environment within which the company operates and the activity in its market place).
- Implementation and documentation of an ongoing compliance training program including incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- 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.

INFORMATION FOR ACCOUNTANTS & LAWYERS

Your Obligations

If you are an accountant or accounting firm, lawyer (barristers and solicitors) or law firm, you have the regulatory requirements under the MLPA when you engage in any of the following activities on behalf of any individual or entity:

- Depositing or investing funds;
- Providing investment advice;
- Buying or selling real estate or business entities
- Managing money, securities or other assets
- Opening or managing bank, savings or securities accounts
- Organising contributions for the creation, operation or management of companies
- Creating, operating or managing trusts, companies or similar structures
- Acting on behalf of or for a client in any financial or real estate transaction, but only to the extent that the lawyer receives funds in the course of the lawyer's business for the purpose of deposit of investment or settling real estate transactions.

If you are an employee of a reporting person or entity, these requirements are the responsibility of your employer except with respect to reporting suspicious transactions and terrorist property, which is applicable to you and the employer.

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 or a terrorist activity financing offence.

Terrorist Property - You must report where you know that there is property in your possession or control that is owned or controlled by or on behalf of a terrorist or a terrorist group.

Record Keeping

You must keep the following records:

- Identification records
- Copies of official corporate records (binding provisions)
- Copies of suspicious transaction reports

Identification requirements

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

- Each customer including beneficial owners and measures should be in place to monitor changes in ownership and control. These measures should also address identification requirements where there is a change in control or beneficial ownership.
- Any individual for whom you have to send a suspicious transaction report
- Any individual or entity for whom you have to keep a receipt of funds records

Third Party Determination

Where a large cash transaction record is required (e.g. $10,000 or more), 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, you must obtain specific information about the third party and their relationship with the individual providing the cash.

Politically Exposed Person

You have to take reasonable measures to determine whether you are dealing with a politically exposed person for new or existing relationships. You also have to keep records and take additional measures.

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 terrorist financing, and measures to mitigate high risks including having adequate controls for higher risk customers, transactions and products/services, as necessary, such as transaction limits or management approvals. (In practical terms, this means increased focus on a firm's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals. There should be a regular review of the risk assessment and management processes, taking into account the environment within which the firm operates and the activity in its market place).
- Implementation and documentation of an ongoing compliance training program including incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- A documented review of the effectiveness of policies and procedures, training program and risk assessment

Examples of Suspicious Transaction

Accountants' Transactions

The following scenarios may give reasonable grounds for suspicion:

- Client appears to be living beyond his or her means.
- Client has business activity inconsistent with industry averages or financial ratios.
- Client has cheques inconsistent with sales (i.e. unusual payments from unlikely sources).
- Client has a history of changing bookkeepers or accountants yearly.
- Client is uncertain about location of company records.
- Company carries non-existent or satisfied debt that is continually shown as current on financial statements.
- Company has no employees, which is unusual for the type of business.
- Company is paying unusual consultant fees to offshore companies.
- Company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues without reasonable explanation of the continued loss.
- Company shareholder loans are not consistent with business activity.
- Examination of source documents shows misstatements of business activity that cannot be readily traced through the company books.
- Company makes large payments to subsidiaries or similarly controlled companies that are not within the normal course of business.
- Company acquires large personal and consumer assets (i.e., boats, luxury cars, personal residences and cottages) when this type of transaction is inconsistent with the ordinary business practice of the client or the practice of that particular industry.
- Company is invoiced by organizations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.

Lawyers' Transactions

The following scenarios may give reasonable grounds for suspicion:

- A transaction is proposed, however, the client is not the person being dealt with. The client wants a lawyer to act on behalf of their niece or elderly relative, for example, who is unknown, not available for contact, and has not provided any instructions.

- A client requests a lawyer to hold a sum of money on the client's behalf, which is unrelated to any particular transaction or the provision of any legal services and where there is no other reasonable explanation for it being held by the lawyer.

- New client approaches a firm with a simple proposition. Once access has been gained to the firm's trust account, the proposal is radically changed or developed.

- Client uses lawyer's trust account for transactions that may be more appropriately conducted through a bank or other type of account.

- Client wants to deposit a sum of cash into a firm's trust account pending the proposed purchase of a house in Samoa. The purchase never eventuates or falls through and the client requests a transfer of the funds to a third party without providing an adequate reason for the transfer.

- Payment to a lawyer by means of a cheque drawn on an account other than that of the client in circumstances where no sound reason is given for the third party making funds available.

- Clients or representatives providing conflicting information to different members of a law firm.

INFORMATION FOR MONEY REMITTANCE/SERVICES BUSINESSES

Your Obligations

The following summary of the legislative requirements under the MLPA 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).

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 or a terrorist activity financing offence.

Terrorist Property - You must report where you know or suspect that there is money or other property in your possession or control that is owned or controlled by or on behalf of a terrorist or a terrorist group.

Record Keeping

You must keep the following records:

- Cash transaction 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 in the amount in excess of $500.00 where the transaction is completed domestically and does not involve foreign currency

- Records for money orders cashed in excess of $500.00 where the transaction is completed domestically and does not involve foreign currency
- 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 large cash transaction
- Any individual who conducts a transaction in excess of $500 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 in excess of $500
- 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

Politically Exposed Person

You have to take reasonable measures to determine whether you are dealing with a politically exposed person. You also have to keep records and take additional measures to monitor such higher risk transactions.

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 terrorist financing, and measures to mitigate high risks including having adequate controls for higher risk customers, transactions and products/services, as necessary, such as transaction limits or management approvals. (In practical terms, this means increased focus on the company's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals. There should be a regular review of the risk assessment and management processes, taking into account the environment within which the company operates and the activity in its market place).
- Implementation and documentation of an ongoing compliance training program including incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- 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.

INFORMATION FOR REAL ESTATE AGENTS

Your Obligations

The following summary of the legislative requirements under the MLPA applies to you if you are a real estate broker or sales representative when you act as an agent regarding the purchase or sale of real estate. These requirements do not apply to your activities related to property management.

If you are an employee of a reporting entity, these requirements are the responsibility of your employer except with respect to reporting suspicious transactions and terrorist property, which is applicable to both you and the employer.

If you are a real estate agent acting on behalf of a broker, these requirements are the responsibility of the broker except with respect to reporting suspicious transactions and terrorist property, which is applicable to both.

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 or a terrorist activity financing offence.

Terrorist Property - You must report where you know or suspect that there is property in your possession or control that is owned or controlled by or on behalf of a terrorist or a terrorist group.

Record Keeping

You must keep the following records:

- Receipt of funds records
- Client information records
- Copies of official corporate records (binding provisions)
- Copies of suspicious transaction reports

Identification requirements

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

- Any individual who conducts a large cash transaction (e.g. in excess of $10,000)
- Any individual or entity for whom you have to keep a client information record or a receipt of funds record
- Any individual for whom you have to send a suspicious transaction report

Third Party Determination

Where a cash transaction record is required (i.e. for transactions in excess of $10,000), you must take reasonable measures to determine whether the individual is acting on behalf of a third party. When a client information record is required, 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.

Politically Exposed Person

You have to take reasonable measures to determine whether you are dealing with a politically exposed person. You also have to keep records and take additional measures to monitor such higher risk transactions.

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 terrorist financing, and measures to mitigate high risks including having adequate controls for higher risk customers, transactions and products/services, as necessary, such as transaction limits or management approvals. (In practical terms, this means increased focus on the company's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals. There should be a regular review of the risk assessment and management processes, taking into account the environment within which the company operates and the activity in its market place).
- Implementation and documentation of an ongoing compliance training program including incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- 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:

- Initial deposit is paid by purchaser with a large amount of cash.
- Initial deposit is paid with a cheque from a third party, for example, an associate or relative (other than a spouse).
- A purchaser uses a significant amount of cash to close a real estate deal.

- Property is purchased in the name of a nominee, for example, an associate or relative (other than a spouse).

- Purchaser refuses to put his/her name on any document associated with the property or uses a different name on contracts, agreements or deposit receipts etc.

- Client unsatisfactorily explains the last minute substitution of the purchasing party's name.

- Client purchases property without inspecting location.

INFORMATION FOR TRUST & COMPANY SERVICE PROVIDERS

Your Obligations

If you are a trust or corporate service provider or a trustee company business as defined in the Trustee Companies Act 1987 (collectively "TCSPs"), you have regulatory obligations under the MLPA when you prepare for and carry out transactions for a client in relation to the following activities:

- Forming or managing legal persons
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
- Providing a registered office, a business address or accommodation, correspondence or an administrative address for a company, a partnership or any other legal person or arrangement
- Acting as (or arranging for another person to act as) a trustee of a trust
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

If you are an employee of a reporting person or entity, these requirements are the responsibility of your employer except with respect to reporting suspicious transactions and terrorist property, which is applicable to both.

Nevertheless, exemptions may be granted by the Money Laundering Prevention Authority for trust or corporate service provider or a trustee company business as defined in the Trustee Companies Act 1987 and the Trustee Companies Amendment Act 2009 with respect to any obligations arising under the provisions of the Money Laundering Prevention Act 2007, depending on the nature of activities it undertakes and the level of risks pertaining to such activities or business in relation to money laundering and or terrorist financing activities. As such, these financial institutions must provide a written application, explaining clearly the reasons of interest for such exemptions for due assessment and consideration by the Authority.

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 or a terrorist activity financing offence.

Terrorist Property - You must report where you know or suspect that there is property in your possession or control that is owned or controlled by or on behalf of a terrorist or a terrorist group.

Record Keeping

You must keep the following records:

- Identification records
- Copies of official corporate records (binding provisions) including information on the beneficial owner
- Copies of suspicious transaction reports

Identification requirements

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

- Each customer including beneficial owners and measures should be in place to monitor changes in ownership and control. These measures should also address identification requirements where there is a change in control or beneficial ownership.
- Any individual for whom you have to send a suspicious transaction report
- Any individual or entity for whom you have to keep a receipt of funds records

Third Party Determination

Where a cash transaction record is required, 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, you must obtain specific information about the third party and their relationship with the individual providing the cash.

Politically Exposed Person

You have to take reasonable measures to determine whether you are dealing with a politically exposed person for new or existing relationships. You also have to keep records and take additional measures.

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 terrorist financing, and measures to mitigate high risks including having adequate controls for higher risk customers, transactions and products/services, as necessary, such as transaction limits or management approvals. (In practical terms, this means increased focus on a TCSP's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals.

There should be a regular review of the risk assessment and management processes, taking into account the environment within which the TSCP operates and the activity in its market place).

- Implementation and documentation of an ongoing compliance training program including incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.

- A documented review of the effectiveness of policies and procedures, training program and risk assessment

Examples of Suspicious Transactions for Trust & Company Service Providers

Persons who provide trust and company provider services should understand the purposes and activities of the structures in relation to which they are appointed or to which they provide services. If they are unable to do so, they should consider whether a suspicion is raised that assets are, or represent, the proceeds of crime. If you are unable to obtain an adequate explanation of the following features, or any other feature which causes it concern, suspicion could be raised:

- Complex networks of trusts and/or nominees and/or companies;

- Transactions which lack economic purpose (for example, sales or purchases at undervalued or inflated prices; payments or receipts being split between a large number of bank accounts or other financial services products; companies consistently making substantial losses);

- Transactions which are inconsistent (for example, in size or source) with the expected objectives of the structure;

- Arrangements established with the apparent objective of fiscal evasion;

- Structures or transactions set up or operated in an unnecessarily secretive way, for example, involving “blind” trusts, bearer shares, endorsed cheques, cash or other bearer instruments or use of post office boxes;

- Lack of clarity about beneficial ownership or interests or difficulties in verifying identity of persons with ownership or control;

- Unwillingness to disclose the source of assets to be received by a trust or company;

- Unwillingness for the fiduciary to have the degree of information and control which it needs to fulfil its duties;

- Use of general powers of attorney in a manner which dilutes the control of a company’s directors.

INFORMATION FOR DEALERS IN PRECIOUS METALS, STONES AND JEWELLERY

Your Obligations

A dealer in precious metals and stones (DPMS) means an individual or an entity that buys or sells precious metals, precious stones or jewellery, in the course of its business activities.

- Precious metals include gold, silver, palladium or platinum whether in coins, bars, ingots, granules or in any other similar form.
- Precious stones include diamonds, sapphires, emeralds, or rubies.
- Jewellery means objects made of precious metals, precious stones or pearls intended for personal adornment.

If you are a person engaged in these activities have the following specific regulatory requirements under the MLPA.

If you are an employee of a reporting person or entity, these requirements are the responsibility of your employer except with respect to reporting suspicious transactions and terrorist property, which is applicable to both.

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 or a terrorist activity financing offence.

Terrorist Property - You must report where you know or suspect that there is property in your possession or control that is owned or controlled by or on behalf of a terrorist or a terrorist group.

Record Keeping

You must keep the following records:

- Cash transactions records for any cash transaction in excess of $50,000 or its equivalent in foreign currency
- Customer identification records for those transactions in excess of $50,000 or its equivalent in foreign currency
- Copies of suspicious transaction reports

Identification requirements

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

- Any individual who conducts a large cash transaction (e.g. any cash transaction in excess of $50,000 or its equivalent in foreign currency)

- Any individual for whom you have to send a suspicious transaction report
- Any individual or entity for whom you have to keep a receipt of funds records

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.

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.

Politically Exposed Person

You have to take reasonable measures to determine whether you are dealing with a politically exposed person. You also have to keep records and take additional measures to monitor such higher risk transactions.

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 terrorist financing, and measures to mitigate high risks including having adequate controls for higher risk customers, transactions and products/services, as necessary, such as transaction limits or management approvals. (In practical terms, this means increased focus on the company's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals. There should be a regular review of the risk assessment and management processes, taking into account the environment within which the company operates and the activity in its market place).
- Implementation and documentation of an ongoing compliance training program including incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- A documented review of the effectiveness of policies and procedures, training program and risk assessment

PART 5 – SFIU REPORTING FORM

The following form has been issued by the Samoa Financial Intelligence Unit to enable financial institutions to meet their reporting obligations under the MLPA.

Copies of the forms can be obtained from the SFIU.

MONEY LAUNDERING PREVENTION AUTHORITY
(CENTRAL BANK OF SAMOA)

SUSPICIOUS TRANSACTION REPORT
(Money Laundering Prevention Act 2007)

PLEASE WRITE IN BLOCK LETTERS

PART A IDENTITY OF CUSTOMERS AND /OR AGENTS INVOLVED IN THE SUSPICIOUS TRANSACTION

PERSONAL ACCOUNT OR AGENT

1 Surname

2 Given Names

3 Address (Home) Country (if not Samoa)

4 Address (Work)

5 Date of Birth

6 Occupation / Business

COMPANY ACCOUNT

1 Company Name

2 Full Address Country (if not Samoa)

Telephone

3 Nature of Business

PART B – TRANSACTION DETAILS

TRANSACTION DATE	AMOUNT	CURRENCY	CASH
			Yes or No

NATURE OF TRANSACTION (eg. Deposit/Withdrawal, Purchase, Sale, Foreign Exchange, Telegraphic Transfer, EFTPOS,etc)

NOTE: FOR MULTIPLE TRANSACTIONS OR MULTIPLE FACILITIES PLEASE RECORD DETAILS ON A SEPARATE SHEET

Details Of Facilities With Financial Institutions Involved

Account Name	
Account Type	
Account Number	
Names of Signatories	
1.	4.
2.	5.
3.	6.

STAMP

PART C – GROUNDS FOR SUSPICION

Give details of the nature of circumstances surrounding the transaction and the reason for suspicion

If space is not enough please attach supplementary sheet. Number of additional pages.

PART D – IDENTIFICATION DETAILS (eg. Drivers Licence, Passport, Birth Cert, Id & etc).

Agent Conducting Transaction

ID Type	ID Number	Issuer

Account Holder (eg. Drivers Licence, Passport, Birth Cert, Id & etc).

ID Type	ID Number	Issuer

Description FOR PERSONAL ACCOUNT HOLDERS ONLY

Sex : Male / Female	**Race**
Eye Colour	**Height (Feet)**
Build	**Skin colour**
Hair style/ colour	**Age**

PASSPORT PHOTO

Clothing
Distinguishing marks/identifying features (tattoo, facial, hair, accent, etc)

PART E **FINANCIAL INSTITUTION DETAILS AND PLACE OF TRANSACTION**

FOR MONEY LAUNDERING AUTHORITY USE ONLY

Institution Type (eg: Bank,Trust Co, Insurance Co etc)	
Name of Institution	
Address	
Telephone	
Fax number	
E-Mail Address	

Please forward this form direct to the Money Laundering Prevention Authority L5 of the Central Bank building immediately when a suspicious transaction is detected.