VANUATU FINANCIAL INTELLIGENCE UNIT

Financial Intelligence Unit
Bureau des Renseignements Financiers

ANTI-MONEY LAUNDERING & COUNTER-TERRORISM FINANCING ACT NO. 13 OF 2014

GUIDELINES FOR REPORTING ENTITIES

Contents

FOREWORD

This Guideline is issued by the Vanuatu Financial Intelligence Unit (VFIU) to outline the requirements of the Anti-Money Laundering & Counter-Terrorism Financing Act No. 13 of 2014 (the "AML&CTF Act"), to provide a practical interpretation of the AML&CTF Act and AML&CTF Regulation Order No. 122 of 2014 (the "AML&CTF Regulation"), to give examples of good practice, and to assist management in developing policies, processes and procedures appropriate to their business. The Guideline is issued pursuant to section 5(1)(n) of the AML&CTF Act.

This Guideline is provided as general information and it is not intended to replace the AML&CTF Act and the AML&CTF Regulation but provide detailed expectations of the VFIU.

Reporting entities are expected to be aware of the requirements of the AML&CTF Act. The role of the VFIU and other supervisory agencies in Vanuatu is to ensure compliance with the requirements of the AML&CTF Act through compliance examinations. Such examinations will be conducted by VFIU staff and, where appropriate, with staff from either the Reserve Bank of Vanuatu (RBV) or the Vanuatu Financial Services Commission (VFSC) or other supervisory authorities.

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

This Guideline will be reviewed periodically to reflect changing circumstances and experiences and to provide additional clarification concerning matters where queries arise. More generally, the VFIU will work closely with other bodies in Vanuatu, such as the Reserve Bank of Vanuatu and the Vanuatu Financial Services Commission, to ensure that Vanuatu's system to combat financial crime and terrorist financing meets international requirements.

The **Scope** of this Guideline covers "reporting entities" which are defined under section 2 of the AML&CTF Act.

Terminology used in this Guideline is consistent with the AML&CTF Act and the AML&CTF Regulations..

This Guideline has been written in several Parts:

- Part 1 gives an overview of money laundering, terrorist financing and proliferation financing.

- Part 2 describes key obligations placed on reporting entities by the AML&CTF Act in developing an effective AML&CTF system.
- Part 3 describes detailed customer due diligence component of an effective AML&CTF system.
- Part 4 describes detailed other essential component of an effective AML&CTF system
- Part 5 summaries the protection afforded to reporting entities and their employees

Reporting entities should contact the VFIU to discuss aspects of this guideline and any problems or questions arising from the AML&CTF Act and Regulations.

PART 1 – GENERAL INFORMATION

Section 1.1 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[1]. 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 entity 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;

[1] In 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, subsection 11(3) of the Proceeds of Crime Act [Cap. 284] (POCA) goes further and defines money laundering to include:

- The acquisition, possession and use of property by a person, directly or indirectly, in an arrangement that involves property that the person knows or ought reasonably to know to be the proceeds of crime; or
- Coverts or transfers property that the person knows or ought reasonably to know to be the proceeds of crime; or
- Conceals or disguises 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.

Vulnerability of Reporting entities to Money Laundering

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

However, criminals have learnt that unusual or large cash payments made into reporting entities 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 reporting entities and ultimately the entire financial sector. The increased integration of the world's financial systems and the removal of barriers to the free movement of capital have made money laundering easier and complicated the tracing process.

Reporting entities 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 Vanuatu as a safe and reliable country for investors.

Money laundering is often thought to be associated solely with banks, other credit institutions and bureau 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.

Vanuatu has developed its first national risk assessment which concluded that certain sectors within the economy pose high risk of money laundering and terrorist financing.

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 and suspicious activity reports submitted to the VFIU by reporting entities, the following methods and trends have been identified in Vanuatu:

i) Credit cards used to pre-pay travel and accommodation costs which is subsequently cancelled and funds are reimbursed to a third party;

ii) Registration of international companies which establish bank accounts in Vanuatu. Funds are then transferred between companies for no apparent economic purpose and then subsequently transferred out of Vanuatu;

iii) Presentation of fraudulent or altered cheques;

iv) The Nigerian "Advance Fee" and other lottery scams which require potential 'winners' to provide bank account details and fees to pay taxes in anticipation of receiving a large payout;

v) Deposits into accounts more than expected for the customer's occupation;

vi) Transactions with high risk jurisdictions (e.g. such as jurisdictions where drug trafficking is common);

vii) Non declaration of currency at the border; and

viii) Misuse of personal accounts for business transactions.

Section 1.2 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. Vanuatu continues to work with other nations to confront terrorism and bring those who support, plan and carry out acts of terrorism to justice.

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

International Efforts to Combat Terrorist Financing

The FATF Revised 40 Recommendations have incorporated earlier FATF Recommendations relating to combating terrorist financing and has imposed further requirements on terrorist financing. The revised FATF Recommendations require 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.

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

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

Should a reporting entity 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 entity should immediately notify the VFIU and submit a suspicious transactions report, even if the reporting entity declines the transaction as a result of its own due diligence.

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

Section 1.3 what is Proliferation of Weapons of Mass Destruction and its Financing?

Proliferation financing relates to the act of providing funds or financial service, which are used or will be used, in whole or in part for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling of weapons or for the use of nuclear, chemical or biological weapons and their means of delivery or related materials.

Over the years, the global community recognized that weapons of mass destruction and their availability are detrimental to the security and sound economies of the world. Such weapons, whenever used, caused catastrophic and indiscriminative destruction to economies, infrastructures and wide spread loss of lives.

In order for terrorists and terrorist organisation to obtain such weapons of mass destruction, they should be able to have sufficient funds and have access to financial services to purchase such weapons. It is the responsibilities of financial services providers to ensure that their businesses, services and delivery methods are not abused by terrorists and terrorist organisation in channeling the funds to the weapons sellers.

Similar to the terrorist financing methods, the terrorists and terrorist organisation may receive financial support from terrorist sympathizers and/or conduct revenue generating activities. The funds may be laundered through the formal financial system and used to purchase weapons.

Hence, reporting entities must ensure their AML&CTF programs are strong, comprehensive and effective to detect and track proliferation financing.

PART 2 – DEVELOPING AN EFFECTIVE AML&CTF SYSTEM

Introduction

The AML&CTF Act imposes requirements on reporting entities related to reporting of transactions, record keeping, staff awareness and implementing customer due diligence processes. These statutory requirements are briefly outlined in this Part of the Guideline. In addition, to assist reporting entities develop internal policies, processes and procedures to establish an effective system to combat money laundering and terrorist financing, this Part provides guidance on the practical implementation of the requirements and intent of the AML&CTF ACT and AML&CTF Regulations.

Section 2.1 AML&CTF Risk Assessment

The foundation stone in developing an effective AML&CTF regime is to identify and assess potential ML&TF risks in the business as it necessitates the requirement to develop and implement effective measures to counter those risks. The AML&CTF Act imposes a requirement on reporting entities to undertake a ML&TF risk assessment on its:

I) Types of customer;
II) Type of services/products it provides to the customer;
III) Method by which it delivers the services/products;
IV) Jurisdictions with which it deals with;
V) Its organisational structure; and
VI) Its staff recruitment and retention.

By adequately identifying and analysing its ML&TF risks, reporting entities are able to effectively implement controls to mitigate and/or manage these risks and minimise any exposure or abuse by criminal elements.

- **Customers**

The types of customers that reporting entities accept to establish business relationships with, offer their services to or open accounts for must be reviewed. Any ML&TF vulnerabilities identified must be understood and control measures implemented.

Reporting entities may, for instance identify that introduced customers or non-resident customers may pose some ML&TF vulnerabilities on the business in that such customers do not appear in person to complete the entities'' CDD requirements.

Control measures may include ensuring that CDD documents from introduced and non-resident customers are sighted and signed off by a reputable notary, commissioner of oath, lawyer or accountant.

In addition, control measures may include conducting enhanced CDD measures on introduced and/or non-resident customers or customers using high risk product/services, dealing with high risk jurisdictions.

- **Services/Products**

Reporting entities must ensure that any ML&TF vulnerabilities identified on their services and/or products must be adequately assessed and evaluated.

For instance, entities providing money exchange or foreign currency exchange may identify that this service can be exploited by launderers and terrorist financiers as these services do not require prolonged business relationships or opening of accounts.

Such services may require the submission of identification/verification documents and purpose of transaction as its means of controls.

- **Delivery Methods**

In addition to assessing the risks of services and products, reporting entities must ensure that their methods of delivering these services and products are not vulnerable to criminal elements.

Entities, for instance, providing customers online access to their accounts or business relationship with the entities may identify that the delivery method (internet access) is vulnerable to hackers. In mitigating the ML&TF vulnerability, the entities should implement stringent anti-hacking softwares and measures.

- **Jurisdictions**

It is important that reporting entities ensure that their customers are not from high risk jurisdictions, and their services/products and delivery methods are not used by or in high risk jurisdictions. If they allow such customers, their services/products and delivery methods are used by high risk jurisdictions, entities must develop and implement effective control measures to mitigate or manage these ML&TF vulnerabilities.

- **Organisational Structure**

Organisation structure of each reporting entity must be reviewed to identify any ML&TF vulnerability. For instance, entities must ensure that their beneficial owners or senior management officials are without any adverse information. If an official does have a

criminal record, the entity must ensure that the official does not accept customers or handle the entity's finances.

- **Staff Recruitment and Retention**

In addition, each entity must implement a staff recruitment and retention program for its staff and must review the program for any ML&TF vulnerability. For instance, the entity may identify the employment of a close associate of a PEP in the business as a ML&TF vulnerability and may implement measures such as separation of duties and stringent oversight.

On identifying and assessing ML&TF risk within the entity, reporting entities should be able to develop and implement adequate risk-based controls and measures to mitigate and/or manage the ML&TF risks.

The AML&CTF Risk Assessment must also incorporate measures recommended in the Vanuatu National Risk Assessment Framework.

Section 2.2 The Duty of Vigilance

Reporting entities are required to have in place adequate policies, processes, practices and procedures that promote high ethical and professional standards and prevent the entity from being used, intentionally or unintentionally, by criminal elements. Section 33 of the AML&CTF Act requires reporting entities to establish and maintain policies, processes 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) customer due diligence processes;

ii) Recognition of suspicious transactions;

iii) Reporting of transactions as required by the AML&CTF Act;

iv) Keeping records; and

v) Training

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

i) Determine the true identity of customers wishing to establish business relationship, requesting their services or opening an account with them;

ii) Recognise and report suspicious transactions and activities to the VFIU;

iii) Keep records for the prescribed period of time;

iv) Train key staff to ensure that they understand their obligations under the AML&CTF Act;

v) Liaise closely with the VFIU 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 entity's anti-money laundering and counter terrorist financing (AML/CTF) policies, processes and procedures.

The nature and scope of the policies, processes and procedures will vary depending on its size, structure and the nature of the business. However, irrespective of size and structure, all entities should establish policies, processes and procedures which in effect capture the measures set out in this Guideline and the requirements of the AML&CTF Act and Regulations.

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

As required under subsection 34 (a) of the AML&CTF Act all reporting entities must appoint an AML&CTF Compliance Officer. The AML&CTF Compliance Officer is responsible for ensuring the entity's compliance with the requirements of the AML&CTF ACT and Regulations, and must be a senior staff member with the necessary powers to ensure the effective management of the system.

Section 2.3 Responsibilities of reporting entities

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

a) Register their business or financial services prior to commencement of business with the VFIU as required under section 9 of the AML&CTF Act.

b) comply with VFIU policies, regulations, directives and the AML&CTF Act. The Directors and Management of reporting entities should ensure that VFIU policies and all relevant Acts are adhered to and that a business relationship is not established, a service is not provided or an account is not opened where there are reasonable grounds to believe that transactions are associated with proceeds of crime or relates to terrorist financing, proliferation financing;

c) appoint an AML&CTF compliance officer in terms of section 34 of the AML&CTF Act to be responsible for ensuring the entity's compliance with the requirements of the AML&CTF Act;

d) in terms of paragraph 33(2)(g) of the AML&CTF Act establish an independent audit function to test its anti-money laundering and combating financing of terrorism procedures and systems;

e) co-operate with law enforcement agencies such as the VFIU on any constraints imposed by legislation on customer confidentiality or where there are reasonable grounds for suspecting money laundering;

f) implement effective policies, processes and procedures for customer due diligence, record keeping, transaction monitoring, transaction reporting and reporting suspicious transactions and activities. These procedures should be in line with Parts 4, 5 and 6 of the AML&CTF Act;

g) implement effective group-wide policies, processes and procedures as required under section 33A of the AML&CTF Act, if the entity has other agents/branches/subsidiaries;

h) conduct its AML&CTF Risk Assessment so to better identify, assess and evaluate its ML&TF risks;

i) submit its AML&CTF Compliance Report to the VFIU so to assist in the VFIU better understanding the entity:

j) report financial transactions exceeding the prescribed threshold to the VFIU;

k) screen potential employees to ensure that they are fit and proper;

l) ensure that its officers and employees are:

- aware of the laws relating to money laundering and financing of terrorism; and

- aware of the processes, procedures and policies for compliance with anti-money laundering and combating the financing of terrorism standards; and

- trained to recognise suspicious transactions and activities.

Section 2.4 Wire Transfers

Section 37 of the AML&CTF Act requires that reporting entities must include accurate and meaningful originator and beneficiary information on funds transfers and related messages that are sent, and the information should remain with the transfer or related message throughout the payment chain.

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

- Transaction reference number;
- Transaction type, currency, amount and value date of the remittance;
- Date of remitter's instructions;
- Instruction details;
- name and account number and address or national ID card number or customer ID card number or passport number or date and place of birth of the remitter;
- Name and account number or a unique transaction reference number of the beneficiary or representative must be verified if appearing in person;
- Telephone number and address of remitter and beneficiary.

If any funds transfer does not contain complete originator information (i.e. name, address and account number) reporting entities should conduct enhanced scrutiny and monitor for suspicious activity. Should problems of verification arise that cannot be resolved, or if satisfactory evidence is not produced to or obtained by a reporting entity under section 13 of the AML&CTF Act, the reporting entity should not proceed any further with the transaction unless directed in writing to do so by the VFIU and must report the attempted transaction to the VFIU as a suspicious transaction.

In addition, the entity may decline the transaction and/or terminate its relationship with the customer.

Section 2.5 Correspondent Banking

As a measure in supporting the global fight against terrorism and terrorist financing, reporting entities relying on intermediary entities to remit or transfer funds across borders must ensure that the intermediary entity is adequately identified and verified, sufficient information is gathered about the nature of the intermediary entity's business, determine that the intermediary entity is reputable and subject to quality supervision and has assessed AML&CTF controls. It must obtain senior management approval before establishing correspondent relationship with the intermediary entity and record the responsibilities of the entity and the intermediary entity.

Further, should the intermediary entity establish accounts in the reporting entity for use by the intermediary entity's customers, the reporting entity must, in addition to its obligations under the AML&CTF Act, be satisfied that the customers' identity are verified, and subject to on-going due diligence process and CDD documents easily retrievable.

This is necessary to ensure that movements of funds and originator and beneficiary information are verifiable and the intermediary entity is reputable. In addition, the entity is not abused by launderers and terrorist financiers.

Section 2.6 Existing Legal Provisions for Anti-Money Laundering and Penalties

The VFIU may impose penalties on any person or body corporate that are found to contravene the provisions of the AML&CTF Act. VFIU imposes two penalty regimes – civil and criminal. In the civil regime, VFIU: (i) may issue penalty notices to entities for any breaches (first and second instances) under section 50A of the AML&CTF Act; (ii) remove, suspend or temporarily remove the name and detail of a offending entity under section 10 of the AML&CTF Act; and (iii) under section 47, apply to the Court for specific court orders directing entities to comply with the AML&CTF Act.

Under the criminal regime, the VFIU may pursue criminal investigation and prosecution on offending entities under relevant provisions of the AML&CTF Act.

Any person that engages in money laundering is liable for conviction under section 11 of the POCA and if found guilty is liable to a fine of up to Vatu 10 million and/or imprisonment for 10 years for an individual, and a fine of up to Vatu 50 million for a body corporate.

Section 9 of the AML&CTF Act requires reporting entities to register their names and details with the VFIU prior to commencement of business. Entities that fail to meet the legal requirements commits an offence and is liable on conviction to a fine not exceeding Vatu 25 million or imprisonment for a term not exceeding 5 years or both for an individual, and a fine not exceeding Vatu 100 million for a body corporate.

Section 46 of the AML&CTF Act states that "if a person obstructs or hinders or fails to cooperate with any authorised person in the lawful exercise of the powers under subsection (1) or (2)" commits an offence and is liable on conviction to a fine not exceeding Vatu 2.5 million or imprisonment for a term not exceeding 2 years or both for an individual, and a fine not exceeding Vatu10 million for a body corporate.

Under sections 20 and 22 of the AML&CTF Act, a reporting entity which fails to report a suspicious transaction commits an offence and is liable to a fine not exceeding Vatu 25 million or to a term of imprisonment not exceeding 5 years or both for an individual, and a fine not exceeding Vatu100 million for a body corporate.

Under section 21 of the AML&CTF Act, a reporting entity which fails to report a suspicious activity commits an offence and is liable to a fine not exceeding Vatu 25 million or to a term of imprisonment not exceeding 5 years or both for an individual, and a fine not exceeding Vatu100 million for a body corporate

A person not disclosing information relating to the property of terrorist groups can be fined under section 23 of the AML&CTF Act to a fine not exceeding Vatu 25 million or to a term of imprisonment not exceeding 5 years or both for an individual, and a fine not exceeding Vatu100 million for a body corporate.

Section 24 of the AML&CTF Act requires reporting entities to submit a suspicious transaction report if it suspects that a transaction or attempted transaction does not have any apparent or visible economic or lawful purpose or is part of an unusual

pattern of transactions. If a reporting entity fails without reasonable excuse to submit a suspicious transaction report it is liable to a fine not exceeding Vatu 25 million or to a term of imprisonment not exceeding 5 years or both for an individual, and a fine not exceeding Vatu100 million for a body corporate.

Section 39 of the AML&CTF Act states that any person that makes a false or misleading statement, can be liable for a conviction to a fine not exceeding Vatu 2.5 million or to a term of imprisonment not exceeding 2 years or both for an individual, and a fine not exceeding Vatu10 million for a body corporate.

The VFIU requires that all directors, managers, secretaries or beneficial owners of reporting entities be free of any money laundering/terrorist financing/proliferation financing/finance related offences. Instances where such person(s) of a reporting entity is/are found to be engaged in money laundering/terrorist financing/proliferation financing/fraudulent activities or convicted of money laundering/terrorist financing/proliferation financing/finance related offences, the VFIU may direct the entity to remove the person from the entity and may suspend or remove the entity's name and detail from the registration register. The VFIU may also, in consultation with other stakeholders such as the Reserve Bank of Vanuatu and the Vanuatu Financial Services Commissions and other supervisory authorities require the entity to replace the persons(s). The VFIU may also seek the revocation of the business license of the reporting entity, should it have sufficient information that the operations of the business would be detrimental to the reputation or soundness of Vanuatu's financial system.

Section 2.7 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) found to be conducting or attempting to conduct any proceeds of crime or terrorist financing or proliferation financing, is easily detected, traced and dealt with by the VFIU, and relevant law enforcement and regulatory authorities.

Reporting entities should undertake customer due diligence measures, including identifying and verifying the identity of customers, when:

- establishing business relations;
- carrying out occasional transactions;
- there is a suspicion of money laundering or terrorist financing;
- the reporting entities has doubts about the adequacy of previously obtained customer identification data.

Section 17 of the AML&CTF Act requires reporting entities to conduct continuous due diligence in the course of its business relationship.

Sections 12 and 16 of the AML&CTF Act require reporting entities to undertake the prescribed identification and verification processes. In addition, subsection 12(2) and

section 17 of the AML&CTF Act requires that a reporting entity must undertake the prescribed identification and verification processes on the person conducting, and person on whose behalf, and the beneficial owner of, the transaction being conducted.

Clause 3 of the AML&CTF Regulation sets out the prescribed identification process for natural persons, legal persons and legal arrangements including at the minimum the following information:

Natural Persons

- the customer's full name;
- the customer's date of birth;
- the customer's residential address;
- the customer's occupation;
- the purpose and intended nature of the business relationship;
- an understanding of the ownership and control structure and purpose and intended nature of the business relationship.

Legal Persons

- the customer's full registered name, legal form, address and nature of customer's business;
- the full name and address of beneficial owners and control structure;
- full name and address of director and secretary or similar positions of the customer
- provisions regulating the power to bind the entity (e.g. its Articles of Association); and
- the authorisation of any person purporting to act for or on behalf of the customer and the identity of the persons.
- The purpose and intended nature of the business relationship with the reporting entity
- An understanding of the ownership and control structure and purpose and intended nature of the business relationship.

Legal Arrangements

- The full business name of the customer;

- The full business address of the customer;
- The type of customer (e.g. trust, express etc…);
- Country of the establishment;
- The full name and address of trustees or similar positions;
- The full name and address of the settlor or similar position; the protector or similar position and each beneficiaries of the customer;
- Authorisation of any person purporting to act for or on behalf of the customer and the identity of the persons;
- The purpose and intended nature of the business relationship with the reporting entity;
- Obtain an understanding of the purpose and intended nature of the business relationship and the ownership and control structure.

in terms of practicality in relation to legal persons and legal arrangements, should the reporting entities can reasonably prove that: (i) there is doubt on the identification of the beneficial owners of the customer or where no natural person exerts control through ownership interest on the customer, the reporting entity must carry out the prescribed identification process on the beneficial owner exercising control through other means; or (ii) there is no identifiable natural person under (i), the entity must carry out the prescribed identification process on the relevant natural person who holds the position of senior managing official.

Section 2.8 Know your Customer

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

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

The procedures which reporting entities 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 reporting entity 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.

Sections 14 and 15 of the AML&CTF Act require a reporting entity to maintain accounts in the true name of the account holder. Reporting entities must 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. In fact 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. In no circumstances should such accounts be used to hide the customer identity from a bank's compliance function or from supervisory authorities.

PART 3 – CDD COMPONENTS OF AN EFFECTIVE AML&CTF SYSTEM

Section 3.1 Essential Elements of Know-Your-Customer Requirements

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

a) customer acceptance policy,
b) customer identification,
c) customer verification,
d) on-going monitoring of high risk accounts, and
e) risk management (including risk-based control and measures).

Entities should not only establish the identity of their customers, but should also monitor account/service activity and the business relationship to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account or services.

Section 3.1.1 Customer acceptance policy

From the outcome of the entities' ML&TF risk assessment, reporting entities should develop clear customer acceptance policies, processes and procedures, including a

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

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

Section 3.1.2 General Guidelines for Establishing Satisfactory Evidence of Identity

The AML&CTF Regulation does specify what may represent adequate evidence of identity and this Part of the Guidelines therefore sets out, as good industry practice, what might reasonably be expected as a minimum for reporting entities. However, the overriding requirement is for the reporting entity itself to be satisfied that it has established the true identity of the prospective customer as far as it is reasonably possible.

A reporting entity should establish to its satisfaction that it is dealing with a real person (natural, legal or arrangement), and verify the identity of those persons who have power to establish and operate the business relationship. 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.

Clause 3 of the AML&CTF Regulation sets out the necessary collection of customer identification information for a natural person, a legal person and a legal arrangement.

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.

Reporting entities are required to obtain adequate customer identification information, based on their risk-based control and measures, from Table A of the AML&CTF Regulation. Entities must ensure that the minimum customer identification information requirements are satisfied.

In addition, the identification of the customer must satisfactorily be completed by the reporting entity before a business relationship is established with the customer.

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 verification required should be obtained from documents issued by reputable, reliable and independent sources. As required under clause 4 of the AML&CTF Regulation, reporting entities must verify the customer identification information collected under Table A including the information under the minimum requirements.

Customer verification must be conducted within the prescribed event, circumstance and/or period timeframes.

Prescribed event; - if an entity suspects that the customer is involved in or that the transaction involves ML, TF or other serious offences, the entity must verify the identity of the customer undertaking the transaction within 2 working days;

Prescribed circumstance:- if an entity suspects on reasonable grounds that the customer is not the person he or she claims to be, the entity must, within 3 working days; (i) collect the necessary identification information of the customer; or (ii) verify the customer's identification.

Prescribed period:-a reporting entity must verify the identification of its customer within 5 working days except (i) if the entity's ML&TF risk is low or medium low, it must verify within 15 working days or (ii) if it reasonably believe that by doing so may inform the customer of the suspicions, the entity is exempted from conducting the verification process and must file a STR/SAR to the VFIU.

In between the identification process and the verification process, entities must ensure that transactions conducted by the customers and the business relationship must be subject to the entity's effective risk-based control and measures.

Such controls and measures must include sets of measures such as limitation of the number, types and/or amount of transactions that can be performed, and monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

Copies of or references to the supporting evidence should be retained for a minimum period of six years. As required under Subsection 19(1) of the AML&CTF Act, reporting entities must keep records of every transaction that is conducted through it and must retain records for a period of six years after the completion of the transaction. Subsection 19(6) of the AML&CTF Act requires that records must also be retained for a period of six years after the account is closed or the business relationship ceases, whichever is the later.

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

Once identification and verification procedures have been satisfactorily completed, and the business relationship has been established and, as long as records concerning that customer are maintained in line with section 19 of the AML&CTF Act, no further

evidence of identity is needed when transactions are subsequently undertaken for that customer as long as regular contact is maintained (clause 8 of the AML&CTF Regulation refers). When an existing customer closes one relationship, service or 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.

Section 3.1.3 Evidence of Identity

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

Section 3.1.4 what is Verification?

As a guide, a list of documents that are acceptable for verifying a person's identification is provided in Table B of the AML&CTF Regulation. Reporting entities should include in their internal policies, processes and procedures a list of documents that it is prepared to accept from a customer to verify identity. This list establishes minimum requirements that the VFIU would expect reporting entities to obtain from customers.

Further, entities must ensure that all information collected in the identification process must be satisfactorily verified under the verification process.

Section 3.1.4A Natural Persons

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

a) Two 'Category A' documents, or

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

c) Three 'Category B' letters.

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

A risk-based approach should again be adopted. 'Category A' documents are more robust than 'Category B' documents. When verifying an individual's identity, a 'top-down' approach should be used by asking individuals to provide 'Category A' documents first, before drawing on 'Category B' documents. The process of

identification should be documented and the reporting entity should state in writing why the decision was made to accept Category B documents to verify an individual's identity.

Category A – Official Documents:

- Current passport (all countries)
- Current driver's license (all countries)
- Government identification documents
- Certificate of Christening/Baptism
- Citizenship certificate
- Birth certificate
- Employment identification
- Employment records
- Employment pay slips
- Other official records from the Government of the Republic of Vanuatu
- An existing customer who is known favourably to the reporting entity (verified by a reporting entity signature)
- An existing customer with a bank who has held an account with the bank for more than two years
- Foreign pensioner's card
- Vanuatu work permit
- Marriage certificate
- Educational institution certificates
- Student card or registration document for an educational institution (such as a primary or high school)
- Government health card
- License or permit issued by the Government of the Republic of Vanuatu
- Public utilities record (such as an electricity or telephone bill)
- Current records of membership of professional or trade organisation
- Records from a bank (including bank or credit cards such as Visa, Diners Club, Master Card, American Express; or statements for an account or credit card)
- Superannuation or provident fund membership card
- Fire arms license
- Mortgage or other security document over the customer's property

Category B Documents

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

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

- A Minister of Religion
- A Church leader
- person who has known the customer for 5 years or more
- A village leader

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

As required by subsection 17 of the AML&CTF Act, reporting entities must 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 entity's knowledge of the customer, the customer's business and risk profile. Where necessary, for example in the case of Politically Exposed Persons, reporting entities must obtain information as to the source of funds.

Section 3.1.4B Direct Clients - Partnerships

Where an application for business is made by a partnership, the identity of each individual partner who is an account signatory or who is authorised to give instructions to the reporting entity, 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).

Section 3.1.4C Direct Legal Person Clients

A reporting entity should obtain and understand the following information and documentation concerning all prospective direct legal person clients:

- Certificate of incorporation and any change of name certificates; where the corporate body is incorporated outside Vanuatu, 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 Vanuatu Financial Services Commission; such return must be notarized where the corporate body is incorporated outside Vanuatu.
- 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 entity 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 entity;

- 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 entity concerning the account, together with their specimen signatures;

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

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

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

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

Section 3.1.4D Direct Clients – Legal Arrangements

The identification of trustees or similar positions, settlors or similar positions, protectors or similar positions, any person having power to appoint or remove trustees or similar positions and any person (other than the settlor or similar positions) 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 and understood:

- Evidence verifying proper appointment of trustees or similar positions, 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 arrangement; and

- Details of the source of funds.

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

Section 3.1.4E Certification of Documents

Suitable Certifiers

A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated bank, trust company or trustee company, notary public or member of the judiciary. The certifier should sign the copy document (printing his or her name clearly underneath) and clearly indicate his position or capacity on it together with a contact address and telephone number.

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

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

Reliance on Other Institutions to Verify Identity

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

Although the responsibility to obtain satisfactory evidence of identity cannot be avoided by the reporting entity that is performing a service for customer, there are occasions when it is reasonable to rely on another entity to undertake the procedures or to confirm identity; intermediaries or third parties. Relying on due diligence conducted by another reporting entity, however reputable, does not in any way remove the ultimate responsibility of the recipient reporting entity to know its customers and their business.

Reporting entities should not rely on reporting entities that are subject to weaker standards than those governing the entitys' own KYC procedures or those applicable to Vanuatu.

Section 3.1.5 Higher Risk Customers, Jurisdictions and Business Relationships

Reporting entities are required to perform additional customer due diligence measures for categories of customer, business relationships or transactions, products/services, delivery methods and jurisdictions with a higher risk of money laundering and financing of terrorism.

Clause 6 of the AML&CTF Regulation sets out the requirement for reporting entities to have in place enhanced customer identification and verification processes for customers, services, designated deliver method and jurisdiction that are deemed to be high ML&TF risks. The processes must be undertaken in addition to the normal identification and verification process.

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

- Collect and verify additional information on the intended nature of the business relationship;
- Collect and verify information on the source of funds or source of wealth of the customer;
- Collect and verify information on the ultimate beneficial owner of the customer;
- Collect and verify information on the reason for intended or performed transactions;
- Obtaining the senior management's approval of the reporting entity to commence or continue the business relationship;; and
- conduct regular and ongoing monitoring of the customer's transactions.

International experience identifies the following examples of higher risk customers:

- Politically Exposed Persons (PEPs) – individuals (domestic and foreign) entrusted with prominent public functions, senior executive members of state owned corporations or international organisations and officials of a political party including their immediate family and close associates.
- All non-resident customers – especially customers who are from countries or regions or industries where a high level of crime is known to exist.
- Customers that work in certain industries or occupations where crime is known to exist.

as part of its risk assessment, reporting entities must make judgements about which industries are higher risk. Industries at higher risk of being associated with money laundering include:

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

Section 3.1.5A Politically exposed persons

Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose an entity to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") are domestic and foreign 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 state-owned corporations and international organisations, and important political party officials.

Accepting and managing funds from PEPs that are related to crime will severely damage a reporting entities own reputation and can undermine public confidence in the ethical standards of Vanuatu's financial system. In addition, a reporting entity may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, a reporting entity and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

As part of a reporting entity's duty to verify a customer's identification, reporting entities 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 or is an immediate family member or close associate of a PEP. Reporting entities should investigate the source of funds before accepting a PEP or a close associate or immediate family member of a PEP. The decision to establish a business relationship with a PEP should be taken at a senior management level.

Section 3.1.5B Non face to face Verification

Based on their risk assessment, reporting entities should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview.

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

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

- Reporting entities should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview; and
- There must be specific and adequate measures to mitigate the higher risk.

Examples of measures to mitigate risk include:

- Certification of documents presented;
- Requisition of additional documents to complement those which are required for face-to-face customers;
- Independent contact with the customer by the reporting entity;
- Seeking verification of the source of funds for the initial deposit, including sighting documentary evidence confirming the source of the funds.

Section 3.1.5C Non-Resident Customers

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

Section 3.1.5D Introduced Business

The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some instances, reporting entities may rely on the procedures undertaken by other institutions or

introducers when business is being referred. In doing so, reporting entities risk placing excessive reliance on the due diligence procedures that they expect *the introducers to have performed.* Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the reporting entity to know its customers and their business. Reporting entities should not rely on introducers that are subject to weaker standards than those governing the entity's own KYC procedures or those are unwilling to share copies of due diligence documentation.

If a reporting entity relies on an intermediary or third party, section 18 of the AML&CTF Act requires that the reporting entity must:

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

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

c) Immediately obtain the information required for customer due diligence requirements (Part 4 of the Act).

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

- It must comply with the minimum customer due diligence practices identified in the AML&CTF Act, the AML&CTF Regulation and this Guideline;
- The customer due diligence procedures of the introducer should be as rigorous as those which the reporting entities would have conducted itself for the customer;
- The reporting entity must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer by auditing and reviewing the systems put in place by the introducer;
- The reporting entity must have a written agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- As required by the AML&CTF Act, all relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the reporting entity, which must carefully review the documentation provided to ensure that it has met its statutory obligations under the AML&CTF Act. (Such information must be available for review by supervisory authorities such as the Reserve Bank of Vanuatu, the Vanuatu Financial Services Commission, and the VFIU, where appropriate legal authority has been obtained).

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

Section 3.1.6On-going Monitoring of Accounts and Transactions

The effect of section 17 of the AML&CTF Act is to place a requirement on reporting entities to monitor transactions and relationships with customers. On-going monitoring is an essential aspect of effective KYC procedures. Reporting entities can only effectively control and reduce their risk if they have an understanding of normal and reasonable relationship activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of a customers activity.

Without such knowledge, reporting entities are likely to fail in their duty to report suspicious transactions and activities where they are required to do so under the AML&CTF Act. The extent of the monitoring needs to be risk-sensitive. For all relationships, reporting entities 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, services or relationships. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert reporting entities to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being “washed” through the account.

It is practical that reporting entities have policies, processes and procedures in place on the frequencies of such monitoring. For low or medium low customers, entities may conduct such monitoring on 6-12 month intervals, while high risk customers should be subject to the below enhanced ongoing due diligence process on a regular frequency but no later than 2 months. Enhanced transaction monitoring must be conducted on all transactions undertaken by a high risk customer or customer utilising a high risk product/service or delivery method or dealing with a high risk jurisdiction.

Similar to the enhanced customer identification and verification processes, reporting entities, based on their risk assessment, must put in place enhanced customer and transaction due diligence processes.

Customers who are classified as high risk, customers who use high risk services/products and delivery methods or customers who deal with high risk jurisdiction, based on the entity’s risk assessment, must be subject to the entity’s enhanced customer and transaction due diligence process. Clause 8 of the AML&CTF Regulation sets out the requirement on reporting entities to:

- Regularly collect information from the customer or third party sources in order to update its knowledge of the customer;

- Undertake more detailed analysis of the customer information including examining as far as possible the background and purpose of the transaction and business relationship;
- Regularly verify or re-verify the customer information;
- Undertake more detailed analysis and monitoring of the customer transactions, both past and future including the purpose and nature of the specific transaction; the expected nature and level of transaction behaviour; and
- Seek senior management approval for establishing or continuing the relationship with the customer, whether the transaction should be processed or service provided.

PART 4 – OTHER COMPONENT OF AN EFFECTIVE AML&CTF SYSTEM

Section 4.1 Record Keeping

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

In line with the requirements outlined in section 19 of the AML&CTF ACT and clause 9 of the AML&CTF Regulation, a reporting entity must maintain records of:

- its transactions and related documentation;
- the nature of the transaction;
- the amount of the transactions and the currency in which it was denominated;
- the date on which the transaction was conducted;
- the name, address and occupation, business or principal activity of the person conducting the transaction and person for whom the transaction is conducted and for whose ultimate benefit the transaction is being conducted;
- the type and identifying number of any account/service with the entity involved in the transaction;
- if the transaction involves a negotiator instrument, the names of the drawer, the drawing institution, the payee and the amount and date of instrument and detail of endorsement;
- the name and address of the entity, and of each officer, employee or agent who prepared the relevant record;
- account files, business correspondence and findings of CDD analysis relating to the transaction; and

- any other information relating to the transaction. The records must be kept for a minimum period of 6 years from the date on which the transaction was made.

Further, if evidence of a customer's identity and verification is obtained under the CDD processes, the reporting entity must maintain a record that indicates the kind of evidence that was obtained and either a copy of the evidence or information that enable a copy of it to be obtained.

The records must be kept for a minimum of 6 years after the closure or termination of the account, service or business relationship.

In addition, reporting entities are required to maintain records of their findings under the CDD processes (particularly sections 15 and 17 of the AML&CTF Act) and copies of their AML&CTF procedure manual and group-wide manuals.

The records must be kept and well maintained by reporting entities electronically or paper-based and must be readable by the VFIU or law enforcement agencies.-

Section 4.2 Education and Training

Section 33 of the AML&CTF Act requires that reporting entities must establish and maintain internal procedures:

- To make the entity's officers and employees aware of Vanuatu's laws relating to money laundering and the financing of terrorism;
- To make the entity's officers and employees aware of the policies, processes and procedures and systems put in place to deal with money laundering and the financing of terrorism; and
- To train officers and employees to recognise and deal with money laundering and the financing of terrorism.

Section 4.2.1 The Need for Staff Awareness

The effectiveness of the procedures and recommendations contained in these Guidelines depends on the extent to which an entity'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 entity and Vanuatu.

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 the AML&CTF procedure manual and/or group-wide procedure manual. All staff should be encouraged to co-operate fully and to provide a prompt report of any suspicious transactions and activities. It is, therefore, important that reporting entities introduce comprehensive measures to ensure that staff are fully aware of their responsibilities.

Staff should be made aware of the risk assessment conducted by the entity and the regular updated national risk assessment and VFIU Sectoral risk assessment to assist in viewing and appreciating the risk factor of their compliance.

All relevant staff should be educated in the importance of "know your customer" requirements. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

Staff and reporting entities should give special attention to business relationships and transactions with persons, including companies and reporting entities, 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 or suspicious activity report should be submitted to the VFIU. Reporting institutions that conduct international transactions should, as part of their customer acceptance policy, maintain lists of jurisdictions which have weak anti-money laundering requirements or are considered to be high risk because organized criminal activities are prevalent.

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

Although Directors and Senior Managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the entity 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.

It is of practical importance that policies, processes and procedures implemented by entities should spell out the frequency of such training/awareness/refreshers and mode of ensuring staff are fully aware or trained to deal with ML and TF. Trainings should be held annually and test be conducted to assess the level of staff understanding on the matter.

Further, new staff members should be made aware or trained within 3 months of employment.

Section 4.3 Staff Recruitment

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

Employee screening procedures must ensure that:

- employees have the high level of competence necessary for performing their duties;
- employees have appropriate ability and integrity to conduct the business activities of the reporting entity;
- potential conflicts of interests are taken into account, including the financial background of the employee;
- fit and proper and code of conduct requirements are defined;
- persons charged or convicted of offences involving fraud, dishonesty or other similar offences are not employed by the reporting entities.
    - Clause 15B of the AML&CTF Regulation provides a list of the prescribed criteria for fitness and suitability.

Section 4.4 Reporting of Financial Information

Section 4.4.1A Reporting and Recognition of Suspicious Transactions and Activities

A suspicious transaction and activity 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.

The suspicious transaction report must be completed and submitted to the VFIU within 2 working days if the entity suspects or has reasonable grounds to suspect that a transaction is not consistent with the customer's known background, purpose or nature of relationship with the entity.

Further, a STR may be submitted if the transaction is suspected of involving proceed of crime or is related to terrorist financing, terrorist property, proliferation financing or has no economic or legal purpose.

The suspicious activity report must be completed and submitted to the VFIU within 2 working days if the entity suspects or has reasonable grounds to suspect a series of transactions is inconsistent with the customer's known information, involves proceeds

of crime or is related to terrorist financing, terrorist property, proliferation financing or have no economic or legal purposes.

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.

Section 4.4.1B Reporting of Suspicious Transactions and Activities

Where a reporting entity suspects, has reasonable grounds to suspect or has information that a transaction or attempted transaction involves proceeds of crime or is related to terrorist financing, a prescribed entity, terrorist property, proliferation financing or has no economic or lawful purpose, the reporting entity must as soon as practical after forming the suspicion but no later than 2 working days, report the transaction to the VFIU by completing the Suspicious Transaction Report.

Similarly, if an entity suspects, has reasonable grounds to suspect or has information that a series of transactions or attempted transactions involve proceeds of crime, or is related to terrorist financing, a prescribed entity, terrorist property, proliferation financing or have no economic or lawful purpose, the reporting entity must as soon as practical after forming the suspicion but no later than 2 working days, report the activity to the VFIU by completing the Suspicious Activity Report. Section 34 of the AML&CTF Act requires reporting entities to each appoint an AML&CTF compliance officer to be responsible for ensuring the entity's compliance with the requirements of the AML&CTF Act. The AML&CTF Compliance Officer would be responsible for reporting suspicious transactions and activities to the VFIU.

Section 26 of the AML&CTF Act states that a suspicious transaction report and suspicious activity report:

- be in writing and may be given by way of fax or electronic mail or hand delivery;
- may be given orally including by telephone, followed by a written report within 24 hours after the oral report is given;
- be in such form and contain such details as may be prescribed;
- contain a statement of the grounds on which the reporting entity holds the suspicion; and
- be signed or otherwise authenticated by the reporting entity.

AML&CTF Compliance Officers should keep a register of all reports made to the VFIU and all reports made internally to them by employees.

Directors, officers and employees, agents and contractors of reporting entities are **prohibited** from disclosing the fact that an STR, SAR or related information is being reported to the VFIU. If a reporting entity forms a suspicion that transactions relate to proceeds of crime or terrorist financing, they should take into account the risk of tipping

off when performing the customer due diligence (CDD) process. If the reporting entity reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR or SAR. Reporting entities should ensure that their employees, staff and agents are aware of and are sensitive to these issues when conducting CDD.

Under section 13 of the AML&CTF Act if satisfactory evidence of identity is not produced to or obtained by a reporting entity, the reporting entity should not proceed any further with the transaction unless directed in writing to do so by the VFIU and must report the attempted transaction to the VFIU as a suspicious transaction. In addition, the reporting entity may decline the transaction(s) or terminate its relationship with the customer.

Section 4.4.1C 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. Reporting entities and their staff 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, service or relationship. Therefore, the first key to recognition is to know enough about the customer and the customer's business to recognise that a transaction or series of transactions is unusual. Questions that a reporting entity 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, 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 entity's customer base and range of services and products and its knowledge and understanding of its risk assessment. Reporting entities might also consider monitoring the types of transactions and circumstances that have given rise to

suspicious transaction and activity reports by staff, with a view to updating internal instructions and guidelines from time to time.

Section 4.4.2 Reporting of Cash and Electronic Transactions

As required under sections 27 and 28 of the AML&CTF ACT, reporting entities must report to the VFIU, in the prescribed form and manner:

a) any cash transactions exceeding the prescribed threshold Vatu 1 million or its equivalent in foreign currency in the course of a single transaction;

b) the transmission or receipt of an electronic or other currency transfer of an amount exceeding the prescribed threshold or its equivalent in foreign currency

Reports must be submitted to the VFIU in the prescribed format and in the case of:

a) a transaction or transfer in Vatu, within 10 working days after the transaction or transfer; and

b) a transaction or transfer in foreign currency, within 2 working days after the transaction or transfer.

Reporting entities should ensure that their staff are aware of these reporting requirements and implement procedures to report to the VFIU within the timeframe specified in the AML&CTF Regulation.

Section 4.5 Risk Management

Effective KYC processes and procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors or similar senior management level of the reporting entity should be fully committed to an effective risk assessment and KYC programme by establishing appropriate policies, processes procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the reporting entity for ensuring that the entity's policies and procedures are managed effectively. The channels for reporting suspicious transactions and activities to the VFIU as required under the AML&CTF Act should be clearly specified in writing, and communicated to all personnel. Reporting entities should establish internal processes and procedures for assessing whether the entity's statutory obligations under the AML&CTF Act require the transaction to be reported to the VFIU.

Section 34 of the AML&CTF Act requires that reporting entities appoint an AML&CTF compliance officer who is responsible for ensuring compliance with the Act. The appointed AML&CTF Compliance Officer must be a senior officer of the entity.

Reporting entity's internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures.

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

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

External auditors also have an important role to play in monitoring reporting entities internal controls and procedures, and in confirming that they are in compliance with the requirements of the AML&CTF Act. Entities must ensure that their internal controls and procedures are assessed by external and independent auditors on a regular basis.

Reporting entities must ensure that they have in place adequate AML&CTF procedure manual which must contain written internal policies, processes and procedures on the entity's compliance with the requirements of the AML&CTF Act. A copy of the procedure manual must be submitted to the VFIU for review and approval.

Further, it is a requirement on entities operating agents, branches or subsidiaries in the country or in foreign jurisdiction to also implement group-wide AML&CTF Procedure Manual which must contain group-wide policies, processes and procedures on the group's compliance with the Act.

In addition, a compliance report must be completed by reporting entities and lodged with the VFIU if the VFIU enforces a compliance breach on any requirements under the AML&CTF Act. The report should provide ample information to the VFIU on whether the compliance breach has been effectively rectified by the defaulting entity.

PART 5 – REPORTING ENTITY PROTECTION

Reporting entities and their officers, employees and agents are protected under section 40A of the AML&CTF Act when complying in good faith with their obligations under the AML&CTF Act.

In addition, reporting entities and their officers, employees and agents are protected from liability for any act done or omitted to be done in good faith in the exercise or performance of a power, function or duty conferred to him by the AML&CTF Act.

However, reporting entities and their officers, employees and agents may be in breach of section 39 if they provide any information to the VFIU that they know is false or misleading or have omitted a material particular from the information.

Further, the VFIU respects the legal professional privilege afforded to lawyers and their clients for legal matters under section 40 of the AML&CTF Act.