FIA

FINANCIAL INTELLIGENCE AUTHORITY

Anti-Money Laundering/ Combating Terrorist Financing Guidance for Attorneys-at-Law

September 2019

Table of Contents

Introduction 1

Purpose of the Guidance 1

Legislation 1

What is Money Laundering? 2

What Is Terrorism? 3

What Is Financing of Terrorism? 4

Sector Vulnerability 4

Risk Based Approach to AML/CFT 5

Risk Identification and Assessment 6

Assigning a Risk Rating 8

Risk Mitigation and Monitoring 8

Internal AML/CFT Policies, Procedures and Controls 9

Compliance Function and Compliance Officer 9

Appointment of Compliance Officer 9

Role and Responsibilities of the Compliance Officer 10

Details of Compliance Officer 11

Compliance Monitoring 11

Compliance Audits 12

Report to the Board of Directors or Audit Committee 13

Risk-Based (KYC) 13

Customer Due Diligence/ Know Your Customer 13

CDD for Politically Exposed Persons 15

Verification (Know Your Customer (KYC)) 15

When Must Identity Be Verified? 16

Verification of Subject 16

Methods of Verification 22

Results of Verification 26

Recognition of Suspicious Customers/Transactions 27

Reporting of Suspicions 28

Reporting to the Financial Intelligence Authority 28

Record Keeping 29

Time Limits 29

Contents of Records 30
Register of Enquires 31
Training Records 31
Staff Training 31
Training Programmes 32
Who to Train 32
Updates and Refreshers 33
Appendix One: Suspicious Transactions 34
Appendix Two: ML/TF Offences 37
Appendix Three: Declaration of Source of Funds 39
Appendix Four: Suspicious Activity Report 40

Introduction

These guidelines being issued to Attorneys at Law listed as other business activities under Schedule 2 of the Money Laundering Prevention Act, Chapter 12.20 of the 2013 Revised Laws of Saint Lucia and includes **all** Attorneys-at-law that carry out the following transactions in accordance with the MLPA Amendment Act No. 20 of 2016 on behalf of their clients:

- buying and selling real estate;
- creating, operating or managing companies;
- managing bank, savings or securities accounts;
- managing client's money, securities or other assets; and
- raising contributions for the creation, operation or management of companies.

The guidance was created in recognition of the risks that Attorneys in Saint Lucia are exposed to with regard to the laundering of the proceeds of criminal activity and reflect best practice internationally. It is in keeping with the key requirements of the FATF 40 recommendations and the Caribbean Financial Action Task Force (CFATF).

The expected outcome of the guidance is to ensure that the operations and services of Attorneys-at-law are not abused by money launderers or terrorist financiers and that they are aware of their obligations and responsibilities under the law.

Purpose of the Guidance

The purpose of the guidance is to:

- Inform of the sector specific responsibilities and obligations of Attorneys at Law.
- Enable Attorneys to understand what the Risk Based Approach (RBA) is and outlining the key elements involved in applying a RBA
- Assist Attorneys at Law in the design and implementation of a Risk Based Approach to AML/CFT compliance
- Provide guidance on the minimum standards of AML/CFT measures required in order to enable the reporting entity to develop its own risk based internal AML/CFT policies, procedures and controls.

Legislation

As a reporting entity the legislations which govern your operations and with which you must be familiar are:

- The Money Laundering (Prevention) Act, Chapter 12.20 of the 2013 Revised Laws of Saint Lucia

- The Proceeds of Crime Act, Chapter 3.04 of the 2013 Revised Laws of Saint Lucia
- The Anti-Terrorism Act, Chapter 3.16 of the 2010 Revised Laws of Saint Lucia

The legislations and all subsequent amendments can be viewed in full and downloaded from our website at www.slufia.com.

What is Money Laundering?

The phrase "money laundering" covers all procedures to conceal the origins of criminal proceeds so that they appear to originate from a legitimate source. There are 3 stages of money laundering:

Placement

The physical disposal of cash proceeds. In the case of many serious crimes, e.g. drug trafficking, the proceeds take the form of cash which the criminal wishes to place in the financial system. Placement may be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of the criminal, his advisers, and their network. Typically, it may include:

- placing cash on deposit at a bank (often intermingled with a legitimate credit to obscure the audit trail), thus converting cash into a readily recoverable debt;
- physically moving cash between jurisdictions;
- making loans in cash to businesses which seem to be legitimate or are connected with legitimate businesses, thus also converting cash into debt;
- purchasing high value goods for personal use or expensive presents to reward existing or potential colleagues with cash;
- purchasing the services of high value individuals with cash;
- purchasing negotiable assets in one-off transactions; or
- placing cash in the client account of a professional intermediary.

Layering

This is the separating of the proceeds of crime from their source by creating sometimes complex layers of transactions designed to mask their origin and hamper the investigation, reconstruction and tracing of the proceeds; for example, by international wire transfers using nominees or "shell companies", by moving in and out of investment schemes or by repaying credit from the direct or indirect proceeds of crime.

Integration

This is the placing of the laundered proceeds back into the economy as apparently legitimate business funds, for example, by realizing property or legitimate business assets, redeeming shares or units in collective investment schemes acquired with criminal proceeds, switching between forms of investment, or by surrendering paid up insurance policies.

The criminal remains relatively safe from vigilance systems while proceeds are not moving through these stages and remain static. Certain points of vulnerability have been identified in the stages of laundering which the launderer finds difficult to avoid and where his activities are therefore more susceptible to recognition, in particular:

- Cross border flows of cash;
- Entry of cash into the business and financial system;
- Acquisition of investments and other assets;
- Incorporation of companies; and
- Formation of trusts.

Attorneys may be used at all stages of ML. Accordingly, Attorneys and their staff must be vigilant of criminals seeking to launder their criminal proceeds and must also be knowledgeable of what constitutes suspicious activity within their sector and sector specific typologies.

What Is Terrorism?

Under the Anti-Terrorism Act a terrorist act is defined as:

a. an act or omission in or outside Saint Lucia which constitutes an offence within the scope of a counter terrorism convention;
b. an act or threat of action in or outside Saint Lucia which—
    i. involves serious bodily harm to a person,
    ii. involves serious damage to property,
    iii. endangers a person's life,
    iv. creates a serious risk to the health or safety of the public or a section of the public,
    v. involves the use of firearms or explosives,
    vi. involves releasing into the environment or any part thereof or distributing or exposing the public or any part thereof—
        - any dangerous, hazardous, radioactive or harmful substance,
        - any toxic chemical,
        - any microbial or other biological agent or toxin,
    vii. is designed or intended to disrupt any computer system by the provision of services directly related to communications infrastructure, banking or financial services, utilities transportation or other essential infrastructure,
    viii. is designed or intended to disrupt the provision of essential emergency services such as police, civil defense or medical services,
    ix. involves prejudice to national security or public safety,

    and is intended, or by its nature and context, may reasonably be regarded as being intended to—
        - intimidate the public or a section of the public, or
        - compel a government or an international organization to do, or refrain from doing, any act, and
        - is made for the purpose of advancing a political, ideological, or religious cause;

c. an act which—
   i. disrupts any services, and
   ii. is committed in pursuance of a protest, demonstration or stoppage of work,

   shall be deemed not to be a terrorist act within the meaning of this definition, so long and so long only as the act is not intended to result in any harm referred to in sub-paragraphs (i), (ii), (iii) or (iv) of paragraph (b);

What Is Financing of Terrorism?

Financing of terrorism is the term used to describe the accommodating or facilitating of financial transactions that may be directly related to terrorist groups or organizations and their activities.

Financing of terrorism may involve funds raised from criminal activity e.g. fraud (credit cards and cheques), prostitution, smuggling, intellectual property theft (e.g. CD piracy), kidnapping and extortion.

Some terrorists operations, however, do not depend on outside sources of money and may be self-funding either through legitimate sources such as employment, personal donations and profits from charitable organizations.

Money laundering (ML) and terrorist financing (TF) often share similar transactional features mostly in relation to the concealment and disguise of funds. It should be noted, however, that terrorist financing tends to be in smaller amounts than in the case with money laundering, and when terrorist raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult.

Sector Vulnerability

The legal profession is governed by the Legal Profession Act, Cap. 2.04. of the Revised Laws of Saint Lucia (the LPA) which provides for the regulation of all attorneys, including the admittance of persons to the law practice in Saint Lucia. Persons admitted to practice go through a formal admittance process which includes the performance of due diligence, including background checks and the requirement for police certificates of character.

The Saint Lucia BAR Association is the self-regulatory body which oversees attorneys practicing on island. The BAR Association enforces the LPA, provides continuing education for its members and is responsible for disciplinary action against its members. However, it is not a requirement of law that all attorneys be members of the BAR Association. Information obtained on the BAR Association website reveals that only one hundred (100) of the two hundred (200) practicing Attorneys-at-Law are members of the BAR Association.

The services commonly engaged in by the attorneys in Saint Lucia are:

- the buying and selling real estate
- creating, operating or managing companies
- managing client's money – clients' accounts are maintained

The National Risk Assessment (NRA) conducted in 2018 rated Attorneys at Law as High Risk for the following reasons:

- They offer high risk services and products, including the maintenance of clients' accounts some of which involve cross border activities;
- There is no requirement in the LPA for Attorneys to comply with the MLPA, thus there is a lack of awareness of the sector's responsibilities and obligations under the MLPA
- They generally lack AML/CFT compliance systems in accordance with the MLPA;
- There has been inadequate AML/CFT monitoring and supervision by the Regulatory bodies;
- Although due diligence procedures are performed in some cases, most attorneys do not have a designated compliance officer which is a key requirement of the MLPA
- No administrative sanctions are in place for the non-compliance with the MLPA;
  Criminal sanctions for non-compliance exist under the MLPA, however the FIA has no recorded instances of lawyers being prosecuted for any such offence.

Risk Based Approach to AML/CFT

The MLPA recommends that a risk-based approach (RBA) be applied to combatting money laundering and terrorist financing. The RBA requires Attorney at Law identify, assess and understand the ML/TF risks to which they are exposed and take the required AML/CFT measures effectively and efficiently mitigate and manage the risks giving regard to the resources they have available.

The key elements of the RBA include:

1. Risk Identification and Assessment
   This entails identifying the inherent ML/TF risks facing a firm, given its customers, products and services offered, countries of operation and the use of publicly available information regarding ML/TF risks and sector specific typologies.

2. Risk Management and Mitigation
   This entails identifying and applying measures to effectively and efficiently mitigate and manage the identified ML/TF risks.

3. Risk Monitoring
   The establishment of an AML/CFT program which includes policies, procedures and processes to monitor changes to ML/TF risks.

The upcoming section will look at each element of the RBA in depth.

Risk Identification and Assessment

Attorneys must be vigilant to ML/TF risks posed by their clients and the services they provide to avoid unwittingly committing or becoming an accessory to the commission of a ML/TF offence. When applying the RBA, Attorneys should be minded that certain activities are more vulnerable to ML/TF especially when it involves the movement/management of clients' assets. Therefore, greater attention and resources must be invested to the more vulnerable areas to minimize abuse by criminals attempting to launder their proceeds of crime.

Attorneys must consider the following factors prior to establishing relationships with new clients:

- The nature and scale of the business;
- Type of client (e.g. ownership structure, whether the client is high net worth or a PEP, whether client is a known criminal);
- The complexity, volume and size of transactions;
- The delivery channels open to clients (e.g. internet banking, wire transfers to third parties, remote cash transactions);
- The geographical location of client (e.g. whether clients are local or international, whether clients reside in countries known to have weak AML/CFT laws); and
- The value and frequency of transactions.

However, at a minimum Attorneys must pay attention to the following risk categories and must determine their exposure to each of these risk categories:

Client Risk

An understanding of your firm's clients is key in building an AML/CFT risk framework. Certain customer types may pose higher ML/TF risks than others. Categories of clients whose activities may indicate a higher risk include:

- Non-resident clients/ clients resident in high risk jurisdictions
- Non-salaried clients whose income varies
- Clients who are PEPS, including their relatives and close associates of PEPS (See FIA's website for list of St. Lucian PEPs)
- Clients who operate through third parties, especially through persons who are not relatives
- High net worth client
- Clients with no known source of legitimate income
- Clients who title property in the name of third parties; a friend, relative, business associate, or use legal entities (corporations or partnerships) that obscure the identity of the person who owns or controls them without a legitimate business explanation.
- Client companies that operate a considerable part of their business in or have major subsidiaries in, countries that may pose higher geographic risk.
- Client with cash intensive businesses
- Clients that are themselves reporting entities listed under the MLPA

- Clients where the structure or nature of the entity or relationship makes it difficult to identify the true beneficial owner or controlling interests or clients
- Businesses with international clients, especially clients located in high risk jurisdictions

Transaction/Service Risk

The broad range of services offered by attorneys can enable criminals to manage all their financial and business affairs in one place, via a reputable and respectable channel. Thus, as part of their risk assessment process Attorneys must assess the ML/TF risk associated with each of the services they offer. Consideration must be given to the following:

- Services that involve the movement of funds
- Services that allow clients to utilize the Attorney's client trust account to deposit and transfer funds
- Services requested by the client knowing that the Attorney does not possess the necessary expertise
- Services that conceal beneficial ownership
- Services that can be performed through third parties
- Payment for services by unknown/unassociated third parties
- Services that involve the transfer of real estate or other high value assets between parties in an unusually short space of time than is normal for such transactions for no particular reason
- Transferring funds through the client account without providing an underlying legal service
- Client sells/buys assets to/from another at a value that is severely under or over the market price
- Payments for services received in large amounts of cash or cash equivalent for which the source of funds are illegitimate or cannot be determined/verified
- Purchasing property without a mortgage which is inconsistent with the client's occupation or income
- Purchases being made without viewing the property, no interest in the characteristics of
- the property
- Client purchases assets with funds known to be illegitimate or from a source that cannot be determined/verified
- Services that allow for purchasing of assets through use of companies or trusts, obscuring ownership

Geographic Risk

Attorneys conduct business both locally and internationally thus, close attention must be paid to the following high risk jurisdictions:

- Clients resident/transacting business in jurisdictions that are not members of FATF/FATF style regional bodies or resident in jurisdictions with weak/ineffective AML/CFT laws
- Clients resident/transacting business in jurisdictions with high levels of public/private sector corruption.

- Clients resident/transacting business in jurisdictions listed on terrorism and sanctions list published by UNSCR and other reputable bodies such as FATF (see FIA's website for updated list).
- Clients who reside/transact business in jurisdictions considered to be High Intensity Drug Trafficking Areas (HIDTA) and High Intensity Financial Crime Areas (HIFCA) both locally and internationally

Attention should also be paid to whether transactions originated from jurisdictions meeting the above criteria

Assigning a Risk Rating

Subsequent to completing the risk assessment, the firm should be in a position to provide itself with an overall risk rating, that is, classifying the firm as low, medium or high risk, giving consideration to the above risk categories i.e., client, service and geographic risk.

A risk rating must also be assigned to each client at the beginning of every new client relationship, giving consideration to the same factors, i.e., the client profile and the types of transactions that the client intends to conduct. Thus, each client must be assigned a low, medium or high risk rating. It must be noted that the process of assigning clients with a risk rating must also be done at the point when the client profile changes and/or when the types of transactions they perform changes.

The ratings assigned must be documented and justification must be provided for selecting each rating. The written risk assessment must be made available to all employees who perform AML/CFT due diligence. In assigning risk levels, you must bear in mind the following:

- **Low Risk-** indicates normal/expected activity and therefore represents the baseline risk of money laundering. Basic due diligence measures must be performed.

- **Medium Risk**- additional scrutiny is required as there is some level of risk to money laundering. Due diligence measures performed depend on the area of risk.

- **High Risk**- the risk is significant and therefore more stringent measures are required to reduce the risk of ML/TF. Enhanced due diligence must be performed and rigorous transaction monitoring

Risk Mitigation and Monitoring

Upon completion of the risk assessment and designation of risk ratings, an AML/CFT programme must be developed to control and mitigate the ML/TF risks identified. The AML/CFT programme should at a minimum comply with your obligations and responsibilities under the MLPA and its

regulations. It is particularly important that the programme be tailored to the specific risks of ML/TF faced so that the appropriate controls can be applied.

The basic elements of the AML/CFT programme include:

1. Internal AML/CFT policies, procedures and controls
2. A Designated Compliance Function With A Compliance Officer
3. Ongoing Customer Due Diligence/Know Your Customer
4. Ongoing staff training
5. Independent Audit Function to test the overall effectiveness of the AML/CFT programme

Internal AML/CFT Policies, Procedures and Controls

The policies, procedures and controls are the foundations of a successful AML/CFT programme as they represent the blueprint outlining how the firm is fulfilling the requirements of the MLPA.

The AML/CFT programme should be in writing and must include all the firm's policies, procedures and controls. The documented programme should be approved by the board of directors and/or senior management and should be disseminated to all staff members.

Compliance Function and Compliance Officer

The MLPA requires all reporting entities to have a Compliance Officer. The compliance role is critical and the position should be a senior one in the firm's organisational structure. Depending on the size of the firm and its level of exposure to ML/TF risk, there may be one such officer or the firm should set up a Compliance Department. It may be possible in very small operations, for example, for the Attorney himself to be designated the Compliance Officer.

Compliance Officers must be fully acquainted with the provisions of the MLPA, its amendments and regulations as well as the Proceeds of Crime Act and the Anti-Terrorism Act. They must, in particular, be cognizant of the requirements of confidentiality regarding money laundering reports and investigations into money laundering.

Appointment of Compliance Officer

The appointed Compliance Officer must be responsible for the establishment and implementation of policies, programmes, procedures and controls for the purposes of preventing or detecting money laundering. The Officer should be separate and apart from the day-to-day activities/operational aspects of the business and report directly to the Board of Directors (where possible). This measure will serve to preserve the integrity of the work carried out by the Compliance Officer, and additionally protect the individual from what may be deemed as victimization.

Any individual who occupies the office of Compliance Officer should be fit and proper - that is to say, at a minimum, he or she has not been convicted of an offence involving dishonesty or is an undischarged bankrupt. Failure to adhere to this criterion should result in the individual immediately vacating the post.

To fulfill the role of the Compliance Officer such a person should—

- have the trust and confidence of the management and staff;
- have sufficient knowledge of the organization, its products, services and systems;
- have access to all relevant information throughout the organization and, or have knowledge of the existence of such information;
- warrant the trust and confidence of the enforcement agencies.

Once appointed, all staff should be aware of the identity of the Compliance Officer.

Role and Responsibilities of the Compliance Officer

Section 44 of the MLPA requires Compliance Officers to have the following minimum responsibilities—

- establish and implement policies, programmes, procedures and controls as may be necessary for the purpose of preventing or detecting money laundering. This duty includes but is not limited to—
    - organizing training sessions for staff on various compliance related issues and instructing employees as to their responsibilities in respect of the provisions of the Act, the Proceeds of Crime Act and the Anti-Terrorism Act,
    - the establishment of procedures to ensure high standards of integrity of employees,
    - the development of a system to evaluate the personal employment and financial history of staff;
- make modifications or adjustments to aspects of paragraph (a) above that may be deemed necessary;
- arrange for independent audits in order to ensure that the programmes as mentioned above, are being complied with;
- analyze transactions and verify whether any of them is subject to reporting, in accordance with the relevant laws;
- review all internally reported unusual transaction reports on their completeness and accuracy with other sources;
- prepare and compile the external reports of unusual transactions to the FIA;
- undertake closer investigations in respect of unusual or suspicious transactions, as directed by the FIA;
- remain informed of the local and international developments on money laundering;
- prepare reports to the Board of Directors and other relevant persons on the institution's efforts in combating money laundering;
- exercise control and review the performance of lower level AML officers within the organization and /or within each branch or unit;

- maintain contact with the FIA.

Details of Compliance Officer

Section 45 of the MLPA requires reporting entities to submit the following details on their Compliance Officer to the FIA within seven (7) days of his or her appointment—

- name;
- job title;
- telephone number (and extension where applicable);
- e-mail address;
- current resume.

Any change in the office of the Compliance Officer should be communicated to the FIA within a month of such a change.

Compliance Monitoring

Section 16(1)(j) and (o) of the MLPA, has made it mandatory for reporting entities to conduct independent audits to ensure that anti money laundering systems, which include programmes, procedures and controls, are operating in accordance with the organization's existing policy manual.

The compliance monitoring of the institution's system should be done on an ongoing basis by the Compliance Officer. Any deficiencies or findings which are noteworthy should be communicated in writing to the senior management of the institution, at least on a monthly basis.

The Compliance Officer should be accountable to the Board of Directors where possible. In such cases he or she is not, and should not be accountable to the senior management of the institution. Submission of monthly reports to senior management is for the purpose of providing information on existing or potential areas in which deficiencies may occur and the corrective actions implemented or required to be implemented in order to rectify the situation.

The Compliance Officer is required to implement corrective actions as soon as deficiencies have been noted in the system. It is not acceptable for the Compliance Officer to argue that recommendations for change must be delayed until the next monthly management report submission. The next monthly report should be used as a means of assessing the success (or otherwise) of the changes that have been implemented.

As soon as the Compliance Officer is aware that there is a significant problem within the institution he or she needs to notify management immediately.

It is recommended that an independent audit be conducted at least annually, with professionals retained specifically to assess the AML, controls of the firm. This will aid in assessing the level of

compliance with existing regulations within the organization and serve as a measure of the effectiveness of the work being done by the Compliance Officer.

Compliance Audits

Section 54 of the MLPA requires that at a minimum, the audits conducted by both the Compliance Officer and the independent auditor should include:

- testing of internal procedures for employee evaluation with respect to integrity, personal employment and financial history;
- evaluation of the extent and frequency of training received by employees;
- testing of employees' knowledge of AML procedures;
- a review of investments by clients for possible structured transactions;
- analysis of a sampling of reportable transactions including a comparison of those transactions with reports submitted on those transactions;
- a review of transactions for possible suspicious transactions;
- testing of record keeping of all money laundering reports, identification documentation of customers and transaction records.

For compliance audits carried out by independent auditors, findings must be documented, and violations of the law and AML procedures must be promptly reported to the Compliance Officer of the firm or the Board of Directors.

There should be written audit procedures for assessing compliance with money laundering prevention legislation and guidelines. These audit procedures or programme steps should be reviewed on an ongoing basis in order to ensure their usefulness.

In carrying out the routine audit, the Compliance Officer should have the following information included in his working papers, at a minimum—

- date the work was performed;
- the rationale or method of selecting the sample;
- adequate narrative on the sample selected, (e.g. for testing the adequacy of customer identification - the name of the individual, customer number, means of identification used and any associated number, etc.);
- deficiencies noted;
- corrective action recommended or taken.

All working papers are required to be maintained for a period of five (5) years.

Report to the Board of Directors or Audit Committee

Reports should be submitted to the Board of Directors at least quarterly. A more detailed report than the one submitted to senior management should be submitted to the Board of Directors. The following is a list of items that should be included in this report—

- any changes made or recommended in respect of new legislation;
- serious compliance deficiencies that have been identified relating to current policies and procedures, indicating the seriousness of the issues and either the action taken, or recommendations of change;
- a risk assessment of any new types of products and services, or any new channels for distributing them and the money laundering compliance measures that have either been implemented or are recommended;
- the means by which the effectiveness of ongoing procedures have been tested;
- the number of internal reports that have been received from each separate division, product, area, subsidiary, etc.;
- the percentage of those reports submitted to the FIA;
- any perceived deficiencies in the reporting procedures and any changes implemented or recommended;
- information regarding staff training during the period, the method of training and any significant key issues arising out of the training;
- any recommendations concerning resource requirements to ensure effective compliance.

Risk-Based (KYC)

The means and mechanisms of laundering funds change. Accordingly institutions should be aware of emerging trends which create a greater risk for money laundering. Primary concern should be for determining the legitimacy of the source of funds entering the business system and the real owners of these funds. Risks may be categorized as high or low depending on the circumstances.

Reporting entities are required to implement enhanced due diligence for transactions involving high risk activities. This requires—

- stricter know-your-customer procedures e.g. more detailed information on customer's background, reputation, etc;
- management information systems in order to monitor these transactions with greater frequency than low risk transactions;
- senior management to monitor transactions.

Customer Due Diligence/ Know Your Customer

A sound CDD programme is one of the best ways of mitigating AML/CFT risk. Knowledge is what the entire AML/CFT programme is built on. Thus, the more you know about your clients, the greater the chance of preventing ML abuse. In accordance to Section 17 of the MLPA,

Attorneys have a statutory obligation to perform CDD when there is doubt about the veracity or adequacy of previously obtained customer identification data including identifying and verifying the identity of customers, when—

- establishing business relations;
- carrying out occasional transactions above $25,000 or that are wire transfers;
- on funds transfers and related messages that are sent;
- when funds are transferred and do not contain complete originator information;
- there is a suspicion of money laundering or terrorist financing.

The reporting entity must ensure that any document, data or information collected under the customer due diligence process is kept up-to-date and relevant by undertaking routine reviews of existing records particularly for high risk categories of customers or business relationships. The CDD programme must provide for—

- performing enhanced due diligence for higher risk categories of customer, business relationship or transaction;
- applying reduced or simplified measures where there are low risks of money laundering or terrorist financing or where adequate checks and controls exist in national system respectively;
- applying simplified or reduced customer due diligence to customers resident in another country which is in compliance and have effectively implemented the Financial Action Task Force recommendations.

The customer due diligence measures to be taken under the MLPA are as follows—

- identifying a customer and verifying a customer's identity using reliable, independent source documents, data or information;
- identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution or person engaged in other business activity is satisfied that it knows who the beneficial owner is and for legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer;
- obtaining information on the purpose and intended nature of the business relationship;
- conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the financial institution's or person engaged in other business activity knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

If the reporting entity is unable to conduct due diligence, then the reporting entity shall not open the account, commence business relations or perform the transaction; or shall terminate the business relationship; and shall consider making a suspicious transaction report in relation to the customer.

Reporting entities may rely on intermediaries or third parties to perform its customer due diligence. However, the following criteria must be followed-

- the reporting entity relying on the third party shall immediately obtain the necessary information on the customer, beneficial owners and the intended nature of business

- the reporting entity shall take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements will be made available from the intermediary or third party upon request without delay
- the reporting entity shall satisfy itself that the intermediary or third party is regulated and supervised for, and has measures in place to comply with the customer due diligence requirements.

However, it must be noted that the ultimate responsibility for customer identification and verification remains with the reporting entity.

Reporting entities shall perform enhanced due diligence for high risk categories and reduced or simplified measures for low risk categories.

The reporting entity shall verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers and complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business. CDD must be performed on all new and existing customers on the basis of materiality and risk.

CDD for Politically Exposed Persons

Reporting entities shall—

- document money laundering and terrorist financing policies and procedures and appropriate risk management systems;
- create policies and procedures that deal with politically exposed persons;
- configure information technology systems to identify politically exposed persons;
- ensure that transactions relating to politically exposed persons are authorized by senior management;
- ensure that source of funds and source of wealth are determined for politically exposed persons;
- enhance customer due diligence that must be performed on an on-going basis on all accounts held by politically exposed persons.

Verification (Know Your Customer (KYC))

A reporting entity undertaking verification should establish to its reasonable satisfaction that every verification subject, relevant to the application for business, really exists. All the verification subjects of joint applicants for business should normally be verified. On the other hand, where the guidelines imply a large number of verification subjects it may be sufficient to carry out verification to the letter on a limited group only, such as the senior members of the family, the principal shareholders, the main directors of the company, etc.

Verification must be carried out in respect of the parties conducting business. Where there are underlying principals, however, the true nature of the relationship between the principals and the agents or signatories must also be established and appropriate enquiries performed on the former, especially if the agents or signatories are accustomed to acting on their instructions. In this context "principals" should be understood in its widest sense to include, for example, beneficial owners, settlers, controlling shareholders, directors, major beneficiaries, etc., but the standard of due diligence will depend on the exact nature of the relationship.

When Must Identity Be Verified?

Whenever a business relationship commences or a significant one-off transaction is undertaken, the prospective customer must be identified. Once identification procedures have been satisfactorily completed, then the business relationship has been established and as long as records are maintained as required in these Guidelines, no further evidence of identity is required when transactions are subsequently undertaken. However, identity must be verified in all cases where money laundering is known or suspected.

Verification of Subject

Face-to-Face Customers

Individuals
The verification subject may be the client/customer himself or one of his agents. An individual trustee should be treated as a verification subject unless the organization has completed verification of the trustee in connection with a previous business relationship or one-off transaction and termination has not occurred. Where the applicant for business consists of individual trustees, all of them should be treated as verification subjects unless they have no individual authority to conduct business or otherwise to give relevant instructions.

Partnerships and Unincorporated Businesses
Business activities should treat as verification subjects all partners/directors of a firm which is an applicant for business who are relevant to the application and have individual authority to conduct business or otherwise to give relevant instructions. Verification should proceed as if the partners were directors and shareholders of a company in accordance with the principles applicable to non-quoted corporate applicants. In the case of a limited partnership, the general partner should be treated as the verification subject. Limited partners need not be verified unless they are significant investors.

Companies (including corporate trustees)
Unless a company is quoted on a recognized stock exchange or is a subsidiary of such a company or is a private company with substantial premises and pay roll of its own, steps should be taken to verify the company's underlying beneficial owner/s – namely those who ultimately own or control the company. The expression "underlying beneficial owner/s" includes any person/s on whose instructions the signatories of an account, or any intermediaries instructing such signatories, are for the time being accustomed to act.

Intermediaries
If the intermediary is a locally regulated institution or business activity and is transacting business in its own name but on behalf of an underlying customer (perhaps with reference to a customer name, etc.), this may be treated as an exempt case but otherwise the customer (or other persons on whose wishes the intermediary is prepared to act) should be treated as a verification subject. If documentation is to be in the customer's name but the intermediary has power to transact business, the intermediary should be treated as a verification subject.

Politically Exposed Persons (PEPs)
Business activities are asked to apply enhanced due diligence when dealing with politically exposed persons (PEPs). Business relationships with individuals holding important public positions and with companies clearly related to them may expose the organization to a significant reputational and /or legal risk.
The PEP risk is associated with providing business services to government ministers or officials from countries with widely-known problems of bribery, corruption and financial irregularity within their government and society. This risk is particularly acute in countries that do not have AML standards that meet internationally accepted norms.

There is the risk that such persons, especially in countries were corruption is widespread, may abuse their public powers for their own illicit enhancement through the receipt of bribes, embezzlement, diverting international aid payments, etc. in exchange for arranging for favourable decisions, contracts or job appointments. The proceeds of such corruption are often transferred to other jurisdictions and concealed in business activities there.

Where a business activity is considering forming a business relationship with a person whom it suspects of being a PEP it must exercise enhanced due diligence to identify that person fully. In relation to PEPs in addition to performing normal due diligence measures, business activities should be using a risk sensitive approach which should include the following—

- having appropriate risk management systems to determine whether the customer or potential customer is a PEP or whether he is acting on behalf of another person who is a PEP,
- having developed a clear policy and internal guidelines, procedures and controls regarding such business relationships,
- obtaining senior management approval for the commencement of business relationships with such customers or to continue business relationships with customers who are found to be or who subsequently become PEPs,
- taking reasonable measures to establish source of wealth and source of funds, and
- ensuring the proactive monitoring of the activity on such accounts, so that any changes are detected and consideration given as to whether such changes suggest corruption or misuse of public assets.

In the context of this risk analysis, it would be appropriate if business activities focus their resources on products and transactions that are characterized by a high risk of money laundering.

Reporting entities should ensure that timely reports are made to the FIA where proposed or existing business relationships with PEPs give grounds for suspicion and should develop and maintain "enhanced scrutiny" practices which may include the following measures, to address PEPs risk—

- Assess country risks where they have financial or similar business relationships, evaluating, amongst other things, the potential risk for corruption in political and governmental organizations. Financial institutions which are part of an international group might also use the group network as another source of information;
- Where reporting entities entertain business relations with entities and nationals of countries vulnerable to corruption, they should establish who the senior political figures are in that country, and should also seek to determine, whether or not their customer has close links with such individuals (for example immediate family or close associates). Reporting entities should note the risk that customer relationships may be susceptible to acquiring such connections after the business relationship has been established; and
- Reporting entities should be vigilant where their customers are involved in those businesses which appear to be most vulnerable to corruption, such as, but not limited to trading or dealing in precious stones or precious metals.

In particular, detailed due diligence should include—

- Close scrutiny of any complex structures (for example, those involving legal structures such as corporate entities, trusts, foundations and multiple jurisdictions);
- Every effort to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship, both at the outset of the relationship and on an ongoing basis;
- The development of a profile of expected activity of the business relationship so as to provide a basis for future monitoring. The profile should be regularly reviewed and updated;
- A review at senior management or board level of the decision to commence the business relationship and regular review, on at least an annual basis, of the development of the relationship; and
- Close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of unknown financial institutions and regular transactions involving sums just below a typical reporting level.

There should be full documentation of the information collected in line with the policies to avoid or close business relationships with PEPs. If the risks are understood and properly addressed then the acceptance of such persons becomes a business/commercial decision as with all other types of customers.

Reporting entities should assess countries with which they have business relationships, and which are most vulnerable to corruption. One source of information is the Transparency Corruption Perceptions index at www.transparency.org

Non-Face-to-Face Customers

Reporting entities are sometimes asked to form business relationships with persons who are not available for a personal interview, for example in the case of non-resident customers. Business activities should apply equally effective customer identification procedures and on-going monitoring standards to non-face-to-face customers as for those available for personal interview. Even though the same documentation can be provided by face-to-face and non-face-to-face customers, there is a greater difficulty in matching the customer with the documentation in the case of non-face-to-face customers.

In accepting business from non-face-to-face customers business activities should—

- apply equally effective customer identification procedures for non- face-to-face customers as for those available for interview;
- ensure that there are specific and adequate measures to mitigate the higher risk.

These measures to mitigate risk may include—

- Certification of documents presented;
- Requisition of additional documents to complement those which are required for non-face-to-face customers;
- Independent verification of documents by contacting a third party.

Internet and Cyber Business

Reporting entities offering services over the internet should implement procedures to verify the identity of its clients. Care should be taken to ensure that the same supporting documentation is obtained from internet customers as for other customers, particularly where face-to-face verification is not practical. In view of the additional risks of conducting business over the internet, businesses should apply enhanced due diligence and monitor on a regular basis, the business activity of customers over the internet.

Regarding the difficulties of following internet links between possible criminal proceeding and the individual attempting to launder such funds and finance terrorism, the FATF within its 2000 – 2001 typologies report offered the following suggestions—

- Require Internet Service Providers (ISPs) to maintain reliable subscriber registers with appropriate identification information.
- Require ISPs to establish log files with traffic data relating internet-protocol number to the subscriber and to telephone numbers used in the connection.
- Require that this information be maintained for a reasonable period.
- Ensure that this information may be available internationally in a timely manner when conducting criminal investigations.

Other products of emerging technology which require enhanced due diligence include—

- smartcards;
- E-cash.

Emerging Technologies
Reporting entities should apply enhanced due diligence when dealing with emerging technologies and should have policies in place or take such measures as may be needed to prevent the misuse of technology developments for money laundering. The level of verification used should be appropriate to the risk associated with the particular product or service.

A risk assessment should be carried out to identify the types and levels of risk associated with their product applications and, whenever appropriate, they should implement multi-factor verification measures, layered security or other controls reasonably calculated to mitigate those risks. Ongoing monitoring of these types of business relationships is required.

Exempt Cases
Unless a transaction is a suspicious one, verification is not required in the following defined cases, which fall into two (2) categories, that is, those which do not require third party evidence in support; and those which do. However, where an institution knows or suspects that laundering or terrorism financing is or may be occurring or has occurred, the exemptions and concessions as set out below do not apply and the case should be treated as a case requiring verification (or refusal) and, more importantly, reporting.

<u>Cases Not Requiring Third Party Evidence in Support</u>

Exempt Institutional Applicants
Verification of the institution or organization is not needed when the applicant for business is an entity itself subject either to these Guidelines or to their equivalent in another jurisdiction. Reasonable effort should be made to ensure that such entities actually exist and are contained on the relevant regulator's list of regulated institutions or organizations.

Small one-off transactions
Verification is not required in the case of small one-off transactions (whether single or linked) unless at any time between entry and termination it appears that two or more transactions which appeared to have been small one-off transactions are in fact linked and constitute a significant one-off transaction. For the purposes of these Guidelines, transactions which are separated by an interval of three months or more are not required, in the absence of specific evidence to the contrary, to be treated as linked.

These Guidelines do not require any reporting entity to establish a system specifically to identify any aggregate linked one-off transactions but business activities should exercise care and judgment in assessing whether transactions should be treated as linked. If, however, an existing system does indicate that 2 or more one-off transactions are linked, it should act upon this information in accordance with its vigilance system.

Cases Requiring Third Party Evidence in Support

Reliable Introductions
Verification may not be needed in the case of a reliable introduction from a locally regulated institution or other reporting entity which does this preferably in the form of a written introduction. Judgment should be exercised as to whether a local introduction may be treated as reliable, utilizing the knowledge which the business activity has of local institutions generally, supplemented as necessary by appropriate enquiries. Details of the introduction should be kept as part of the records of the customer introduced.

Verification may not be needed where a written introduction is received from an introducer who is—

- a professionally qualified person or independent financial advisor operating from a recognized foreign regulated institution or business activity; and
- the receiving institution is satisfied that the rules of his or her professional body or regulator (as the case may be) include ethical guidelines, which taken in conjunction with the money laundering regulations in his or her jurisdiction, include requirements at least equivalent to those in these Guidelines; and
- the individual concerned is reliable and in good standing and the introduction is in writing, including an assurance that evidence of identity would have been taken and recorded, which assurance may be separate for each customer.

Details of the introduction should be kept as part of the records of the customer introduced.

Verification is not needed where the introducer of an applicant for business is either an overseas branch or member of the same group as the receiving institution. In such cases, written confirmation or evidence of the relationship should be obtained from the holding or parent company.

To qualify for exemption from verification, the terms of business between the business activity and the introducer should require the latter to—

- complete verification of all customers introduced to the business activity or to inform the business activity of any unsatisfactory conclusion in respect of any such customer;
- keep records in accordance with these Guidelines; and
- supply copies of any such records to the business activity upon demand.

In the event of any dissatisfaction on any of these, the business activity should (unless the case is otherwise exempt) undertake and complete its own verification of the verification subjects arising out of the application for business either by—

- carrying out the verification itself; or
- relying on the verification of others in accordance with these Guidelines.

Where a transaction involves a business activity and an intermediary, each needs separately to consider its own position to ensure that its own obligations regarding verification and records are duly discharged.

The best time to undertake verification is not so much at entry as prior to entry. Verification should whenever possible be completed before any transaction is completed. It would not be appropriate to complete settlement of the relevant transaction, with a third party, or dispatch documents of title before adequate verification is obtained.

If it is necessary for sound business reasons to carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls. A senior member of key staff may give appropriate authority. This authority should not be delegated. Any such decision should be recorded in writing.

Verification, once begun, should normally be pursued either to a conclusion or to the point of refusal. If a prospective customer does not pursue an application, key staff may consider that this is in itself suspicious.

In the case of telephone business, where payment is or is expected to be made from a bank or other account, the verifier—

- should satisfy himself/herself that such account is held in the name of the applicant for business at or before the time of payment; and
- should not remit the proceeds of any transaction to the applicant for business or his or her order until verification of the relevant subjects has been completed.

Methods of Verification

These Guidelines do not seek to specify what, in any particular case, may or may not be sufficient evidence to complete verification. They do set out what, as a matter of good practice, may reasonably be expected of business activities. Since, however, these Guidelines are not exhaustive; there may be cases where a business activity has properly satisfied itself that verification has been achieved by other means which it can justify as reasonable in all the circumstances.

Verification is a cumulative process. Except for small one-off transactions, it is not appropriate to rely on any single piece of documentary evidence.

The best possible documentation of identification should be required and obtained from the verification subject. For this purpose "best possible" is likely to mean that which is the most difficult to replicate or acquire unlawfully because of its reputable or official origin.

File copies of documents should, whenever possible, be retained. Alternatively, reference numbers and other relevant details should be recorded.

The process of verification should not be unduly influenced by the particular type of services being applied for.

It is important to obtain references from banks and other professional firms. These references should be requested by the business activity and be received directly from the banks and other firms providing such references. Under no circumstances should a letter of reference be accepted

from the new customer as it could be forged or altered. Verify bank references and document confirmations.

Individuals
A personal introduction from a known and respected customer or member of key staff is often useful but it may not remove the need to verify the subject in the manner provided in these Guidelines. The introduction should in any case contain the full name and permanent address of the verification subject and relevant information contained below.

Save in the case of reliable introductions, the business activity should, whenever feasible, interview the verification subject in person.

The relevance and usefulness in this context of the following information should be considered—

- full name/s used;
- date and place of birth;
- nationality;
- current permanent address including postal code (Any address printed on a personal account cheque tendered to commence business if provided, should be compared with the address);
- telephone and fax number;
- occupation and name of employer (if self-employed, the nature of the self-employment)

In this context "current permanent address" means the verification subject's actual residential address, as it is an essential part of identity.

To establish identity the following documents are considered to be appropriate, in descending order of acceptability—

- current valid passport;
- national identity card;
- armed forces identity card; and
- driver's licence, which bears a photograph.

Documents sought should be pre-signed by, and if the verification subject is met face to face, preferably bear a photograph of the verification subject.

Documents which can be easily obtained in any name should not be accepted without verification—

- birth certificates;
- credit cards;
- business cards;
- national health or insurance cards;
- provisional health or insurance cards;
- provisional driver's licences;
- student union cards.

It is acknowledged that there will sometimes be cases, particularly involving young persons and the elderly, where the appropriate documentary evidence of identity and independent verification of address are not available. In such cases a senior member of key staff could authorize the transaction if he is satisfied with the circumstances and should record these circumstances in the same manner and for the same period of time as the identification records.

If the verification subject is an existing customer of an organization acting as an intermediary in the application, the name and address of that organization and that entity's personal reference on the verification subject should be recorded.

If information cannot be obtained from the above-mentioned to enable verification to be completed a request may be made to another business activity or business activities for confirmation of such information from its/their records. Failure of that organization to respond positively and without undue delay should put the requesting business activity on its guard.

Companies
All signatories should be duly accredited by the company. The relevance and usefulness in this context of the following documents or their foreign equivalent) should be carefully considered—

- Certificate of Incorporation (duly notarized where such body is incorporated in Saint Lucia);
- Notice of Directors;
- Notice of Secretary;
- The most recent annual return filed with the Registrar, duly notarized where such corporate body is incorporated outside Saint Lucia;
- The name(s) and address(es) of the beneficial owner/s or the person/s on whose instructions the signatories to the account are empowered to act;
- Articles of Association or by laws;
- Resolution, Bank Mandate, signed application form or any valid account opening authority, including full names of all directors and their specimen signatures and signed by no fewer than the number of directors required to make up a quorum;
- Copies of identification documents should be obtained from all directors and authorized signatories in accordance with the general procedure for the verification of the identity of individuals;
- Copies of Powers of Attorney or other authorities given by the directors in relation to the company;
- A signed director's statement as to the nature of the company's business;
- A statement of the source of funds should be completed and signed;
- For large corporate entities the following may be obtained; annual reports/audited financial statements, description and place of principal line(s) of business, list of major business units, suppliers and customers, etc. where appropriate; and
- A confirmation from another institution

As legal controls vary between jurisdictions, particular attention may need to be given to the place of origin of such documentation and the background against which it is produced.

Partnerships and Unincorporated Businesses

- The relevance and usefulness of obtaining the following (or other foreign equivalent) should be carefully considered as part of the verification procedure—
- The partnership agreement;
- The same information as required for individuals above must also be obtained in respect of the partners and managers relevant to the application for business; and
- A copy of the mandate from the partnership or unincorporated business authorizing the establishment of the business relationship and confirmation of any authorized signatories.

Clubs, Societies and Charities

In the case of transactions for clubs, societies and charities, the business activity should satisfy itself as to the legitimate purpose of the organization by, for example, requesting a copy of the constitution.

Trustees

A trustee should verify the identity of a settler/guarantor or any person adding assets to the trust in accordance with the procedures relating to the verification of identity of clients. In particular, the trustee should obtain the following minimum information—

- *Settler or any person transferring assets to the trust*.—name, business, trade or occupation, and other information in accordance with the procedures relating to the verification of client identity outlined in these Guidelines;
- *Beneficiaries*.—name, address and other identification information such as passport number, etc.;
- *Protector*.—name, address, business occupation and any relationship to the settler;
- Purpose and nature of the trust.—a statement of the true purpose of the trust being established, even where it is a purpose or charitable trust;
- *Source of funds*.—identify and record the source(s) of funds settled on the trust and the expected level of funds so settled; and
- *Authorisation of payments*.—the trustee should also ensure that payments from the trust are authorized and made in accordance with its terms.

Politically Exposed Persons (PEPs)

Ongoing enhanced scrutiny must be applied to transactions by senior foreign or domestic political figures, their immediate family and closely related persons and entities (i.e politically exposed persons – PEPs). They include—

- a senior official in the executive, legislative, administrative, military or judicial branches of a foreign or domestic government (whether elected or not);
- a senior official of a major foreign or domestic political party;
- any corporation, business or other entity formed by, or for the benefit of, a senior political figure;
- ‘immediate family’ i.e. parents, siblings, spouse, children and in-laws as well as ‘close associates’ (i.e. person known to maintain unusually close relationship with PEPs).

Reporting entities must—

- ascertain identity of the customer/client and or agent;

- obtain adequate documentation regarding the PEP;
- understand the PEP's anticipated business transactions;
- determine the PEP's source of wealth;
- apply additional oversight to the PEP's business transactions.

Particular attention should be paid to—

- requests to establish relations with business activity unaccustomed to doing business with foreign persons;
- requests for secrecy with transaction e.g. booking transaction in the name of another person or entity whose beneficial owner is not disclosed or readily apparent;
- use of accounts at the nation's central bank or other government-owned bank, or of government accounts, as the source of funds in a transaction;
- routing of transactions into or through a secrecy jurisdiction;
- enquiry by or on behalf of PEP regarding exceptions to reporting requirements.

Reporting entities should consult several sources of information to assist it in determining whether to conduct business with an individual who may be a PEP, including—

- reports by non-government organizations that identify corruption, fraud and abuse e.g. Corruption Perceptions Index of Transparency International;
- reports on corruption and money laundering issued by international financial institutions e.g. World Bank, and the International Monetary Fund (IMF);
- information published on the World Wide Web by foreign countries;
- the World Fact Book published by the Central Intelligence Agency (CIA).

Results of Verification

Satisfactory

Once verification has been completed (and subject to the keeping of records in accordance with these Guidelines), no further evidence of identity is needed when transactions are subsequently undertaken, except in cases where either doubt arises as to the identity of the client or about the veracity or adequacy of previously obtained customer identification data. Where doubts arise, the entire due diligence process must be carried out anew, from start to finish. This is known as the "duty of continuous verification."

The duty of continuous verification also requires the business activities to monitor transactions for their consistency continuously against the stated business purpose or the source of funds, or pattern.

The file of each applicant for business should show the steps taken and the evidence obtained in the process of verifying each verification subject or, in the appropriate cases, details of the reasons which justify the case being an exempt case.

Unsatisfactory
In the event of a failure to complete verification of any relevant verification subject or where there are no reasonable grounds for suspicion, any business relationship with, or one-off transaction for, the applicant for business should be suspended and any funds held to the application order returned in the form in which it was received, until verification is subsequently completed (if at all). Funds should never be returned to a third party but only to the source from which they came. If failure to complete verification itself raised suspicion, a report should be made to the Reporting Officer/Compliance Officer for determination as to how to proceed. Generally business activities should consider making a suspicious transaction report when unable to obtain satisfactory evidence or verification of identity of customers, agents or beneficial owners.

Recognition of Suspicious Customers/Transactions

A suspicious transaction will often be one which is inconsistent with a customer's known legitimate business or activities. It follows that an important pre-condition of recognition of a suspicious transaction is for the business activity to know enough about the customer's business to know that a transaction or series of transactions is/are unusual.

Although these Guidelines tend to focus on new business relationships and transactions, institutions should be alert to the implications of the financial flows and transaction patterns of existing customers, particularly where there is a significant unexpected and unexplained change in the behaviour of the account.

Against such patterns of legitimate business, suspicious transactions should be recognizable as falling into one or more of the following categories—

- any unusual financial activity of the customer in the context of his own usual activities;
- any unusual transaction in the course of his usual business activity;
- any unusually linked transactions;
- any unusual employment of an intermediary in the course of some transaction;
- any unusual method of settlement; and
- any unusual or disadvantageous early redemption of an investment product.

From time to time, the authorities or management may determine that because a high incidence of money laundering is associated with persons from certain countries or regions, additional precautions are required to safeguard against use of accounts or other facilities by such persons, their immediate relatives, associates and representatives. The source of wealth and economic activities that generated the level of wealth should be substantiated. Under these circumstances, it may be necessary to request a letter of reference (confirmed), in addition to other identification requirements, from a regulated bank which is not from the countries or regions in question.

The Compliance Officer should be well versed in the different types of transactions which the institution handles and which may give rise to opportunities for money laundering. Examples of common and relevant transaction types, are set out in Appendix One. These are not intended to be exhaustive.

Reporting of Suspicions

Reporting of suspicions is an important defense against possible accusation of assisting in the retention or control of the proceeds of money laundering/criminal conduct, or of acquiring, possessing or using the proceeds of criminal conduct. In practice, a Compliance Officer will normally only suspicions, without having any particular reason to suppose that the suspicious transaction or other circumstances relate to the proceeds of one sort of crime or another.
It should be noted in this context that the suspicion of criminal conduct is more than the absence of certainty that someone is innocent. It is rather an inclination to believe that there has been criminal conduct. Institutions should ensure—

- that key staff know to whom their suspicions should be reported; and
- that there is a clear procedure for reporting such suspicions without delay to the Compliance Officer.

Key staff should be required to report any suspicion of money laundering either directly to their Compliance Officer, or if the institution so decides, to their line manager for preliminary investigation in the event that there are any known facts which may negate the suspicion.

Employees should comply at all times with the approved vigilance systems of their institution and will be treated as having met appropriate standards of vigilance if they disclose their suspicions to the Compliance Officer or other appropriate senior colleague according to the vigilance systems in operation in their institutions.

On receipt of a report concerning a suspicious customer or a suspicious transaction, the Compliance Officer should determine whether the information contained in such report supports the suspicion. He should investigate the details in order to determine whether in all the circumstances he in turn should submit a report to the FIA.

If the Compliance Officer decides that the information does substantiate a suspicion of money laundering, he or she should disclose this information immediately. If he or she is genuinely uncertain as to whether such information substantiates a suspicion, he or she should nevertheless submit the report. If in good faith he or she decides that the information does not substantiate a suspicion, he or she would be well advised to record fully the reasons for his or her decision not to report to the FIA in the event that his judgment is later found to be wrong.

It is for each business activity or group to consider whether its vigilance systems should require the Compliance Officer to report suspicions within the individual business activity or group to the inspection or compliance department at head office.

Reporting to the Financial Intelligence Authority

If the Compliance Officer decides that a disclosure should be made, a report, preferably in the form set out in Appendix 3, should be sent to the FIA.

If the Compliance Officer considers that a report should be made urgently (e.g. where a customer is already under current investigation), initial notification to FIA should be made by facsimile.

The receipt of a report will be promptly acknowledged by the FIA. The report will be forwarded to trained financial investigation officers who alone will have access to it. They may seek further information from the reporting business activity and elsewhere. It is important to note that after a reporting business activity makes an initial report in respect suspicious transaction, that initial report does not relieve the business of the need to report further of a specific suspicions in respect of the same customer and the business activity should report any further suspicious transactions involving the customer.

Discreet inquiries will be made to confirm the basis of the suspicion but the customer is never approached. In the event of a prosecution the source of the information is protected, as far as the law allows. Maintaining the integrity of the confidential relationship between law enforcement agencies and business activity is regarded by the former as being of paramount importance.

Vigilance systems should require the maintenance of a register of all reports made to the FIA pursuant to this paragraph. Such register should contain details of—

- the date of the report;
- the person who made the report;
- the person/s to whom the report was forwarded;
- a reference by which supporting evidence is identifiable; and
- the receipt of acknowledgement from the FIA.

Record Keeping

Once a business relationship has been established, the reporting entity is required to maintain all relevant records on the identity and transactions of their customers, both locally and internationally, for seven (7) years, or longer if required by the FIA.

It may be necessary for business activities to retain business transaction records for a period exceeding the date of termination of the last business transaction where certain circumstances predate this event, for example—

- date of termination of business relationship; or
- date of insolvency.

Time Limits

In order to facilitate the investigation of any audit trail concerning the transactions of their customers, business activities should observe the following—

- *Entry records*.—businesses should keep all account opening records, including verification documentation and written introductions, for a period of at least 7 years after termination.
- *Ledger records*.—institutions should keep all account ledger records for a period of at least 7 years following the date on which the relevant transaction or series of transactions is completed.

- *Supporting records*.—institutions should keep all records in support of ledger entries, including cheques, for a period of at least 7 years following the date on which the relevant transaction or series of transactions is completed.

Where an investigation into a suspicious customer or a suspicious transaction has been initiated, the FIA may request a business activity to keep records until further notice, notwithstanding that the prescribed period for retention has elapsed. Even in the absence of such a request, where a business activity knows that an investigation is proceeding in respect of its customer, it should not, without the prior approval of the FIA, destroy any relevant records even though the prescribed period for retention may have elapsed.

Contents of Records

Records in relation to verification will generally comprise—

- a description of the nature of all the evidence received in relation to the identity of the verification subject; and
- the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

Reporting entities should retain customer identification records, current files and business correspondence since it may be necessary to establish a financial profile of any suspected transaction as part of an investigation. To satisfy this requirement, additional information such as the following may be sought—

- volume of funds involved in the transaction;
- origin of the funds;
- forms in which the funds were offered, e.g. cash or cheque;
- identification of the person undertaking the transaction including the names and addresses of the beneficial owners of the product and also any counter-party;
- form of instruction and authority.

Reporting entities should maintain transaction records in such a manner that will allow them to comply expeditiously with information requests from the FIA. The records must be sufficient to permit reconstruction of individual transactions.

A retrievable form may consist of—

- an original hard copy;
- copies;
- microform; or
- computerized or electronic form.

Records held by third parties are not regarded as being in a readily retrievable form unless the business activity is reasonably satisfied that the third party is itself an entity which is able and willing to keep such records and disclose them to it when required.

Where the FIA wishes to view records which would ordinarily have been destroyed in accordance with a business activity's vigilance systems, the business activity is nonetheless required to conduct a search for those records and provide as much detail to the FIA as is possible.

Register of Enquires

A business activity should maintain a register of all enquiries made to it by the FIA. The register should be kept for a period of at least 7 years and separate from other records and should contain at a minimum the following details—

- the date and nature of the enquiry; and
- details of the transaction involved.

Training Records

Reporting entities should document a formal AML policy including evidence of compliance relating to audit and training. At a minimum, records should be maintained on the following—

- details and contents of the training programme;
- names of staff receiving training;
- dates of training sessions; and
- assessment of training.

Staff Training

Business activities have a duty to ensure that key staff receive sufficient training to alert them to the circumstances whereby they should report customers/clients or their transactions to the Compliance Officer. Such training should include making key staff aware of the basic elements of—

- the MLPA and any Regulations made under the Act, and in particular the personal obligations of key staff under the Act, as distinct from the obligations of their employers under the MLPA;
- vigilance policy and vigilance systems;
- the recognition and handling of suspicious transactions;
- other pieces of AML legislation for example the Proceeds of Crime Act;
- any Code of Conduct/Practice issued under regulatory legislation or voluntarily adopted by various industry associations; and
- any additional guidelines and instructions issued by the FIA.

The effectiveness of a vigilance system is directly related to the level of awareness engendered in key staff, both as to the background of international crime against which the Act and other AML legislation have been enacted including these Guidelines as well as to the personal legal liability of each of them for failure to perform the duty of vigilance and to report suspicions appropriately.

Training Programmes

While each business activity should decide for itself how to meet the need to train members of its key staff in accordance with its particular commercial requirements, the following programmes will usually be appropriate.

Training should include—

- the company's instruction manual;
- a description of the nature and processes of money laundering;
- an explanation of the underlying legal obligations contained in the Act and any Regulations made under the Act; and other AML legislation and guidelines;
- an explanation of vigilance policy and systems, including particular emphasis on verification and the recognition of suspicious transactions and the need to report suspicions to the Compliance Officer (or equivalent).

Who to Train

Cashier/Dealers/Salespersons/Advisory Staff

Key staff dealing directly with the public is the first point of contact with money launderers and their efforts are vital to the implementation of vigilance policy. They need to be aware of their legal responsibilities and the vigilance systems of the business activity, in particular the recognition and reporting of suspicious transactions. They also need to be aware that the offer of suspicious funds or the request to undertake a suspicious transaction should be reported to the Compliance Officer in accordance with vigilance systems, whether or not the funds are accepted or the transaction proceeded with.

New Customer and New Business Staff/Processing and Settlement Staff

Key staff who deal with new business and the acceptance of new customers, or who process or settle transactions or the receipt of completed proposals and cheques, should receive the training given to cashiers, etc. In addition, verification should be understood and training should be given in the institution's procedures for entry and verification. Such staff also needs to be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the Compliance Officer in accordance with vigilance systems, whether the funds are accepted or the transaction proceeded with.

Administration/Operations Supervisors and Managers

A higher level of instruction covering all aspects of vigilance policy and systems should be provided to those with the responsibility for supervising or managing staff. This should include—

- the MLPA and other relevant money laundering legislation and any Regulations made under the Act;
- the offences and penalties arising from the relevant primary legislation for non-reporting or assisting money launderers or terrorism financers;

- procedures in relation to the service of production and restraint orders;
- internal reporting procedures; and
- the requirements for verification and records.

Compliance Officers

In depth training concerning all aspects of the relevant laws, vigilance policy and systems will be required for the Compliance Officer. In addition, the Compliance Officer will require extensive initial and continuing instruction on the validation and reporting of suspicious transactions, on the feedback arrangements and on new trends of criminal activity.

Updates and Refreshers

It will also be necessary to make arrangements for updating and refresher training at regular intervals to ensure that key staff remain familiar with and are updated as to their responsibilities.

Appendix One: Suspicious Transactions

Examples of Common Indicators

The following are examples of common indicators followed by examples of some specific types of business activities that may point to a suspicious transaction, whether completed or attempted.

General Indicators

- Client admits or makes statements about involvement in criminal activities.
- Client does not want correspondence sent to home address.
- Client appears to have accounts with several financial institutions in one area for no apparent reason.
- Client conducts transactions at different physical locations in an apparent attempt to avoid detection.
- Client repeatedly uses an address but frequently changes the names involved.
- Client is accompanied and watched.
- Client shows uncommon curiosity about internal systems, controls and policies.
- Client presents confusing details about the transaction or knows few details about its purpose.
- Client appears to informally record large volume transactions, using unconventional bookkeeping methods or "off-the-record" books.
- Client over justifies or explains the transaction.
- Client is secretive and reluctant to meet in person.
- Client is nervous, not in keeping with the transaction.
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Client's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after transacting business.
- Normal attempts to verify the background of a new or prospective client are difficult.
- Client appears to be acting on behalf of a third party, but withholds that information.
- Client is involved in activity out-of-keeping for that individual or business.
- Client insists that a transaction be done quickly.
- Inconsistencies appear in the client's presentation of the transaction.
- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the client.
- Client appears to have recently established a series of new relationships with different financial entities and business activities.
- Client attempts to develop close rapport with staff.
- Client uses aliases and a variety of similar but different addresses.
- Client spells his or her name differently from one transaction to another.
- Client uses a post office box or general delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
- Client provides false information or information that you believe is unreliable.

- Client offers you money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious.
- Client pays for services or products using financial instruments, such as money orders or travelers cheques, without relevant entries on the face of the instrument or with unusual symbols, stamps or notes.
- You are aware that a client is the subject of a money laundering investigation.
- You are aware or you become aware, from a reliable source (that can include media or other open sources), that a client is suspected of being involved in illegal activity.
- A new or prospective client is known to you as having a questionable legal reputation or criminal background.
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).

Examples Specific to Attorneys-at-Law

Attorney-at-Law should consider the following indicators when you are carrying out certain activities on behalf of your client—

- Client uses an unknown intermediary to approach attorney.
- Client wants to use foreign companies but does not seem to have a legitimate, legal or commercial reason for doing so.
- Client wishes to form or purchase a company with a corporate objective that is irrelevant to the client's normal profession or activities without a reasonable explanation.
- Client performs activities that are irrelevant to his or her normal activities or profession and cannot provide a reasonable explanation.
- Client repeatedly changes attorneys within a short period of time without any reasonable explanation.
- Client often transfers funds or securities to a third party.
- Client is reluctant to discuss his or her financial affairs regarding behaviour that is inconsistent with his or her ordinary business practices.
- Client has a history of changing bookkeepers or accountants yearly.
- Client is uncertain about location of company records.
- Client is invoiced by organizations located in a country that does not have adequate money laundering laws and is known for high secretive banking and as a corporate tax haven.
- Third party is present for all transactions but does not participate in the actual transaction.
- Client uses an attorney to structure deposits and purchase real estate.
- Client does not want to put his or her own name on any document that would connect him or her with the property or uses different names on Offer to Purchase, closing documents and deposit receipts.
- Client negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference surreptitiously.
- Client's desire to create or buy a company that has a suspicious objective, does not realize profits or does not seem to be connected to his usual profession or related activities without being able to submit sufficient explanations to the attorney.

- Client purchases property in the name of a nominee such as an associate or a relative (other than a spouse).
- Client purchases multiple properties in a short time period and seems to have a few concerns about the location, condition, and anticipated repair costs, etc. of each property.
- Client insists on providing signature on documents by fax only.
- Client frequently makes large investments in stocks, bonds, investment trusts or other securities in cash or by cheque within a short time period, which is inconsistent with the normal practice of the client.
- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.
- Client's documentation to ascertain identification, support income or verify employment is provided by an intermediary who has no apparent reason to be involved.
- Client seems uncertain with terms of credit or cost associated with completion of a loan transaction.
- Client frequently uses trust accounts for transactions where it may not make business sense to do so.
- The client sells assets or real estate properties repeatedly without realizing any profit margin or submitting a reasonable explanation in this respect.
- Clients receipt of cash money or high value cheques, which do not suit the volume of his work or the nature of his activity, particularly if they come from certain people who are not clearly or justifiably connected to the client.
- Repeated large amount cash transactions including foreign exchange transactions or cross-border fund movement when such types of transactions are not commensurate with the usual commercial activity of the client.
- The client request, upon having an attorney, to incorporate a company to deposit the services of the incorporation fees or the capital to/in the bank account of the attorney through multiple accounts that he has no relation to without a reasonable justification.

Appendix Two: ML/TF Offences

Section of Legislation	Offence/Breach	Fine/Penalty
Section 15 of the MLPA Guidelines for Other Business Activities	Engaging in ML	1. *Summary Conviction:* fine not less than $500,000 (not exceeding $1 million) and/or imprisonment of not less than 5 years (not exceeding 10 years) 2. *Indictable Conviction:* fine not less than $1 million (not exceeding $2 million) and/or imprisonment of not less than 10 years (not exceeding 15 years)
Section 16 of the MLPA Guidelines for Other Business Activities	Tipping Off	Punishment on Summary Conviction to a term of 5 years (not exceeding 10 years) and/or a fine of not less than $50,000
Section 33 (4) and (5) of the MLPA Section 17 of the MLPA Guidelines for Other Business Activities	Prejudicing Investigation	Punishment on Summary Conviction to a term of 7 years (not exceeding 15 years) and/or a fine of not less than $500,000
Section 18 of the MLPA Guidelines for Other Business Activities	Failure to Disclose	Punishable on Indictment to a fine of $500,000
Section 28 of the MLPA	Concealing or transferring proceeds of criminal conduct	1. *Summary Conviction:* fine not less than $0.5 million (not exceeding $1 million) and/or imprisonment of not less than 5 years (not exceeding 10 years) 2. *Indictable Conviction:* fine not less than $1 million (not exceeding $2 million) and/or imprisonment of not less than 10 years (not exceeding 15 years)
Section 29 of the MLPA	Arranging with another to retain the proceeds of criminal conduct	1. *Summary Conviction:* fine not less than $0.5 million (not exceeding $1 million) and/or imprisonment of not less than 5 years (not exceeding 10 years)

		2. *Indictable Conviction:* fine not less than $1 million (not exceeding $2 million) and/or imprisonment of not less than 10 years (not exceeding 15 years)
Section 30 of the MLPA	Acquisition, possession or use of proceeds of criminal conduct	1. *Summary Conviction:* fine not less than $0.5 million (not exceeding $1 million) and/or imprisonment of not less than 5 years (not exceeding 10 years) 2. *Indictable Conviction:* fine not less than $1 million (not exceeding $2 million) and/or imprisonment of not less than 10 years (not exceeding 15 years)
Section 31 of the MLPA	Attempts, aiding, abetting, counselling, procuring and conspiracy	1. *Summary Conviction:* fine not exceeding $1 million) and/or imprisonment for 5 years 2. *Indictable Conviction:* fine not exceeding $2 million and/or imprisonment for exceeding 15 years
Section 33 (4) and (5) of the MLPA	Failing to Report a Suspicious Activity	Indictment to a fine of $500,000
Section 6 (2) of the MLPA	Failure or refusal to comply with the request for production of information is an offence	Maximum $50,000.00 and or imprisonment up to 10 years
Section 16 (3) of the MLPA	Disclosure to Person who has been reported to the FIA	Summary conviction to a fine of not less than $100,000 and not exceeding $500,000 or to imprisonment for a term of not less than 7 years and not exceeding 15 years or both.
Section 16 (8) of the MLPA	Failure to Keep Transaction Records in Legible Form for Retrieval in Reasonable Period	Summary conviction to a fine of not less than $100,000 and not exceeding $500,000 and/or to imprisonment for a term of not less than 7 years and not exceeding 15 years
Section 6 of ATA	Provision of service for commission of terrorist acts	Conviction on indictment, liable to imprisonment for a term of 25 years.
Section 8 of ATA	Arrangements for retention or control of terrorist property	Conviction on indictment, liable to imprisonment for a term of 25 years.
Section 9 of ATA	Dealing with terrorist property	Conviction on indictment, liable to imprisonment for a term of 25 years

Appendix Three: Declaration of Source of Funds

for transactions exceeding EC$25,000.00 with a person engaged in other business activities

Name of Address of Business Activity						***Date of Transaction: (dd/mm/yy)***	
DECLARATION OF SOURCE OF FUNDS FORM **Section 21 of the Money Laundering (Prevention) Act**							
Customer/Client Information							
NAME							
Current Address:							
Resident Status:	**Resident**		**Non-resident**				
Date of Birth			**Place of Birth**		**Nationality**	**Occupation**	
Telephone Numbers			**Home:**		**Work:**	**Mobile:**	
Customer/Client Agent Information (if applicable)							
Name:							
Date of Birth			**Place of Birth**		**Nationality**	**Occupations**	
Telephone Numbers		**Home:**		**Work:**		**Mobile:**	
Resident Status:	**Resident**		**Non-resident**				
Identification: (Valid Picture ID required)							
National ID		***Passport***		***Driver's Licence***		***Other***	***Identification details:***
Description/Nature of Business Transaction							
Amount and Currency							
FINANCIAL INSTITUTIONS ARE REQUIRED BY LAW TO VERIFY THE SOURCE OF FUNDS BEING DEPOSITED BEFORE ACCEPTING DEPOSITS AND TO DISCLOSE SUCH INFORMATION TO LAW ENFORCEMENT AUTHORITIES IF REQUIRED. THE MAKING OF A FALSE DECLARATION AS TO THE SOURCE OF FUNDS CONSTITUTES AN OFFENCE UNDER SECTION 21(2) OF THE MONEY LAUNDERING (PREVENTION) ACT. I DECLARE THAT THE SOURCE OF FUNDS IS: (Show supporting evidence, e.g. Receipt, invoice, title deeds etc.)							
Transaction Approved:		**Yes** ☐		**No** ☐		**(If no state reason)**	
Customer's Signature:			**Transaction taken by: (signature and title)**			**Witness**	

Appendix Four: Suspicious Activity Report

FIA Ref:

ST. LUCIA FINANCIAL INTELLIGENCE AUTHORITY

Suspicious Activity Report

(In accordance with the Proceeds of Crime Act 3.02 and the Money Laundering (Prevention) Act, CAP 12.20 of the Revised Laws of Saint Lucia)

Reporting Business:	Date of Report:	Reporters Reference:
Address:		
SUBJECT DETAILS		
NAME (full name of person, business or company)		
ADDRESS (full address of person, business, registered office, etc.)		
DATE OF BIRTH / DATE OF INCORPORATION* (dd/mm/yyyy)	OCCUPATION / NATURE OF BUSINESS*	
EMPLOYER		
HOME TEL:	BUS TEL:	CELL:
ACCOUNT DETAILS (include details of all connected accounts)		
FORM(S) OF IDENTIFICATION PRODUCED (attach copies)		
REASON FOR SUSPICION & DETAILS OF TRANSACTION(S)		
(continue on reverse, if necessary)		
PERSON REPORTING	TEL NO:	BRANCH/DEPT*
SIGNATURE	POSITION HELD	

(* delete as necessary)

Completed forms and associated documentation should be forwarded without delay to:-

The Director, St. Lucia Financial Intelligence Authority, PO Box GM 959, Castries, St. Lucia. Tel 451 7126 Fax 453 6199.

UNAUTHORISED DISCLOSURE OF THIS INFORMATION TO THE SUBJECT OR ANY OTHER PERSON IS A CRIMINALOFFENCE WHICH CARRIES A PENALTY OF UP TO EC$250,000 OR IMPRISONMENT OF UP TO TEN YEARS.