



## Guide to Anti-Money Laundering and Anti-Terrorist Financing in Mauritius

## TABLE OF CONTENTS

Preface .....	2
1. Introduction .....	3
2. A. Legislative Framework .....	4
3. B. Anti-Money Laundering and Terrorist Financing .....	9
4. C. AML/ CFT Procedures .....	12
5. D. Customer Due Diligence .....	13
6. E. Suspicious Activity Reporting .....	19
7. F. Further Internal Policies and Procedures .....	20

## PREFACE

This is the first Edition of the Guide, which we have produced for the information of our clients and professional colleagues. This edition takes account of the main Legislations and Codes of Practice which regulates the Mauritius anti-money laundering and anti-terrorist financing framework.

This Guide is divided into six parts:

1. Legislative Framework
2. Anti-Money Laundering and Terrorist Financing
3. Anti-Money Laundering/Combating Financing of Terrorism Procedures
4. Customer Due Diligence
5. Suspicious Activity Reporting
6. Further Internal Policies and Procedures

Under the heading of Legislative Framework, we have outlined and elaborated on the different Acts, Regulations and Conventions that regulate the Anti-Money Laundering and Anti-Terrorist Financing framework in Mauritius. We have also dealt with matters such as explanation of terms like “Money Laundering”, “Terrorist Financing”, the different procedures regarding Anti-Money Laundering and Anti-Terrorist Financing procedures to be put in place. The different Customer Due Diligence requirements for individuals and other body corporate have also been outline. The Guide also comprise of the different procedures regarding Suspicious Activity Reporting.

It is recognised that this Guide will not completely answer detailed questions which clients and their advisers may have. It is intended to provide a sketch of Mauritius’ legal and regulatory environment in relation to exempted and permit companies. The Guide is, therefore, designed as a starting-point for a more detailed and comprehensive discussion of the issues.

Whilst we have made every effort to ensure the accuracy of the statements made herein, we accept no liability for any errors. In all cases expert legal advice from a qualified practitioner of Mauritius law should be obtained.

Appleby  
Port Louis, Mauritius  
August 2009

## **INTRODUCTION**

Over the past 7 years, Mauritius has continuously strived to enhance its anti-money laundering and anti-terrorist financing framework in order to bring itself into line with the recommendations of the International Monetary Fund (“IMF”), the Financial Action Task Force (“FATF”) and other international anti-money laundering standards. The anti-money laundering and combating the financing of terrorism framework was undertaken with the collaboration of the Ministry of Finance, Ministry of Justice, the Financial Services Commission (“Commission”), Bank of Mauritius (“BOM”) and other relevant stakeholders.

## PART A: LEGISLATIVE FRAMEWORK

### 1. Financial Intelligence and Anti-Money Laundering Act 2002 (“FIAMLA”) –

Refer to Annex A

#### a. Money-Laundering Offence

The principal anti-money laundering legislation in Mauritius is the Financial Intelligence and Anti-Money Laundering Act 2002 (“FIAMLA”). The Financial Intelligence and Anti-Money Laundering Act 2002 replaced the Economic Crime and Anti-Money Laundering Act 2000. The offences of money laundering are contained within Part II, section 3 of the FIAMLA and can be summarised as follows:

1. Concealing, disguising, converting or removing property to or from the jurisdiction knowing or having reasonable grounds to suspect that it is the proceeds of criminal conduct (either your own or another’s) with the intent to avoid prosecution or a confiscation order. Acquiring, possessing or using property, knowing that it represents the proceeds of criminal conduct.
2. Failing to disclose information coming to your attention at work leading you to know or suspect that another person is engaged in money laundering which related to the proceeds of crime. All suspicious transactions must be reported to the Financial Intelligence Unit.
3. Disclosing information likely to prejudice an investigation knowing or suspecting a report has been made to the Financial Intelligence Unit and there is or may be an investigation being conducted into money laundering.

The Financial Intelligence and Anti-Money Laundering Act (“FIAMLA”) defines “money laundering” as:

- (1) Any person who -
  - (a) engages in a transaction that involves property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime; or
  - (b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime, where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime, shall commit an offence.
- (2) A bank, financial institution, cash dealer or member of a relevant profession or occupation that fails to take such measures as are reasonably necessary to ensure that neither it nor any service offered by it, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence shall commit an offence.

The FIAMLA also provides that any person who makes or accepts any payment in cash in excess of 500,000 rupees or an equivalent amount in foreign currency, or such amount as may be prescribed, shall commit an offence.<sup>1</sup>

<sup>1</sup> However this does not apply to the following transactions:

- (a) between the Bank of Mauritius and any other person;
- (b) between a bank and another bank;
- (c) between a bank and a financial institution;

- (d) between a bank or a financial institution and a customer where –
- (i) the customer is, at the time the transaction takes place, an established customer of the bank or financial institution; and
  - (ii) the transaction consists of a deposit into, or withdrawal from, an account maintained by the Customer with the bank or financial institution, where the transaction does not exceed an amount that is commensurate with the lawful business activities of the customer; or
- (e) between such other persons as may be prescribed;

#### **b. Financial Intelligence Unit**

The Financial Intelligence Unit (“FIU”) was established in August 2002 as a result of the FIAMLA. The FIU replaces the Economic Crimes Office<sup>2</sup>. The FIU is responsible to deal with the Anti-Money Laundering (AML) Offences, Suspicious Transaction Reporting (“STRs”) and to exchange information on Anti-Money Laundering and Combating the Financing of Terrorism (“AML/CFT”).

The FIU is responsible for requesting, receiving, analyzing and disseminating disclosures of financial information concerning suspected proceeds of crime, alleged money laundering activities, suspected financing of any activities or transactions related to terrorism to the relevant investigatory<sup>3</sup> and supervisory authorities<sup>4</sup>.

The FIU also plays an integral part in the investigation and detection of financial crimes. It collects, processes, analyses and interprets all information disclosed to and obtained by it in the process of combating money laundering and terrorist financing.

Additionally, the FIU issued Guidance Notes on the way in which a suspicious transaction report should be made. The first Guidance Note was issued in January 2003. Same was recently replaced by Guidance Note 2 in August 2009.

The Mauritian FIU also became a member of the Egmont Group in July 2003. The Mauritius FIU was elected regional representative of African FIUs on the Egmont Committee in July, 2003 and was re-elected in that position for another period of two years until July, 2007. The Mauritius FIU also represents the Egmont Group in the ESAAMLG meetings as an official observer.

<sup>2</sup> The Economic Crimes Office was established under the Economic Crime and Anti-Money Laundering Act 2000

<sup>3</sup> "investigatory authorities" means the Commissioner of Police, the Comptroller of Customs and the Commission

<sup>4</sup> "supervisory authorities" means the Bank of Mauritius and the Financial Services Commission

<sup>5</sup> Refer to Annex B

#### **c. Reporting and other measures to combat money laundering**

The FIAMLA also contains provisions regarding the reporting obligations of banks, financial institutions, cash dealers and members of relevant professions or occupations whereby all reports should be lodged with the FIU. Additionally, the FIAMLA contains provisions relating to the legal consequences of reporting, measures to combat money laundering, regulatory action in the event of non-compliance and offences relating to obligation to report and keep records and to disclosure of information prejudicial to a request.

#### **d. National Committee for anti-money laundering and combating the financing of terrorism**

A National Committee for Anti-Money Laundering and Combating the Financing of Terrorism has been established under the FIAMLA. As per the FIAMLA the National

Committee consists of persons from several institutions in Mauritius. The functions of the National Committee is to:

- assess the effectiveness of policies and measures to combat money laundering and the financing of terrorism;
- make recommendations to the Minister for legislative, regulatory and policy reforms in respect of anti-money laundering and combating the financing of terrorism;
- promote co-ordination among the FIU, investigatory authorities, supervisory authorities and other institutions with a view to improving the effectiveness of existing policies to combat money laundering and the financing of terrorism;
- formulate policies to protect the international reputation of Mauritius with regard to anti-money laundering and combating the financing of terrorism;
- generally advise the Minister in relation to such matters relating to anti-money laundering and combating the financing of terrorism, as the Minister may refer to the National Committee.

**e. Provision and exchange of information in relation to money laundering and financial intelligence information**

The FIAMLA also provides for the Membership of international financial intelligence groups and provision of information to overseas financial intelligence units. The FIU shall be the only body in Mauritius which may seek recognition by any international group of overseas financial intelligence units which exchange financial intelligence information on the basis of reciprocity and mutual agreement. The FIU may also disseminate information to investigatory or supervisory authorities.

**2. The Financial Intelligence and Anti Money Laundering Regulations 2003**

The FIAMLA Regulations 2003 provides for appointment of a Money Laundering Reporting Officer and internal controls and procedures to be implemented by banks to combat money laundering and terrorist financing. Additionally, the Regulations also sets out circumstances in which verification of identity shall be carried out.

**3. The Financial Services Act 2007/Codes on the Prevention of Money Laundering and Terrorist Financing**

The Financial Services Act 2007 (“FSA”) governs the non-banking financial institutions in Mauritius. The FSA replaces the Financial Development Act 2001, under which the Financial Services Commission (“Commission”) was established. The objects of the Financial Services Commission are:

- to ensure the orderly administration of the financial services and global business activities;
- to ensure the sound conduct of business in the financial services sector and in the global business sector;
- to elaborate policies which are directed to ensuring the fairness, efficiency and transparency of financial and capital markets in Mauritius;
- to study new avenues for development in the financial services sector, to respond to new challenges and to take full advantage of new opportunities for achieving economic sustainability and job creation;
- to ensure, in collaboration with the Bank of Mauritius, the soundness and stability of the financial system in Mauritius; and
- to work out objectives, policies and priorities for the development of the financial services sector and global business and to make recommendations to the Minister.

One of the main powers of the Commission is to make FSC Rules, set standards and provide guidelines. As such the Commission has issued several Guidelines and those relevant to AML/CFT are:

- Codes on the Prevention of Money Laundering and Terrorist Financing intended for Insurance Entities<sup>6</sup>;
- Codes on the Prevention of Money Laundering and Terrorist Financing intended for Investment Businesses<sup>7</sup>;
- Codes on the Prevention of Money Laundering and Terrorist Financing intended for Management Companies<sup>8</sup>.

<sup>6</sup> Refer to Annex C

<sup>7</sup> Refer to Annex D

<sup>8</sup> Refer to Annex E

The Commission first issued its Codes on the Prevention of Money laundering and Terrorist Financing in April 2003. However, since that time there has been a lot of evolution in the anti-money laundering and combating the financing of terrorism initiatives both nationally and internationally. A review of the Codes was also desired so as to make the requirements of the Codes consistent with the revised FATF 40 Recommendations and the Nine Special Recommendations on Terrorist Financing.

The Codes takes into account all relevant international standards which include:

- the Financial Action Task Force's (FATF) Forty Recommendations 2003;
- the FATF's Nine Special Recommendations on Terrorist Financing;
- the Basel Committee's Paper on Customer Due Diligence, (which has been endorsed by the FATF); and
- the International Association of Insurance Supervisors' Guidance Paper on Anti- Money Laundering and Combating the Financing of Terrorism dated October 2004.

The Codes are intended to assist Licensees to comply with the obligations contained within the FIAMLA. The Code is designed to serve as a statement of minima criteria and to describe operational practices expected of licensees. Non-compliance with the Codes will expose the Licensee to regulatory action. Moreover, the extent to which a Licensee is able to demonstrate adherence to this Code will be considered by the FSC in the supervision of Licensees and in particular in the conduct of its compliance visit.

Moreover, the Commission has also issued a Guide to Compliance – refer to Annex F

#### **4. Bank of Mauritius Act 2004/Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institution (Refer to Annex G)**

The Bank of Mauritius (“BOM”) is the supervisory authority for banks, money changers and foreign exchange dealers. The BOM regularly issues and supervises compliance with codes and guidelines. The Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism are issued to financial institutions<sup>9</sup> by the Bank of Mauritius by virtue of powers conferred upon it by section 50(2) of the Bank of Mauritius Act 2004, section 100 of the Banking Act 2004 and section 18(1)(a) of the Financial Intelligence and Anti-Money Laundering Act 2002.

The Guidance Notes came into effect in June 2005, however same was reviewed in July 2008. The Guidance Notes are a statement of the minimum standard expected of ALL banks, non-bank deposit taking institution or cash dealer licensed by the BOM. The Bank of Mauritius, in the exercise of its

supervisory duties, will monitor adherence to the Guidance Notes and failure to measure up to the standard contained in the Guidance Notes will be dealt with, as appropriate, by the Bank. It is a criminal offence for financial institutions to fail to take measures to prevent their institutions or the services their institutions offer from being used to commit or to facilitate the commission of money laundering.

Note: As Appleby Management (Mauritius) Ltd has been licensed by the Financial Services Commission and falls part of the non-banking financial sector Part B to Part F of this Guide would be applicable to the non-banking financial sector.

<sup>9</sup> bank, non-bank deposit taking institution or cash dealer licensed by the central bank.

## **5. Prevention of Terrorism Act 2002 (“POTA”) – Refer to Annex H**

The POTA provides for measures to combat terrorism in general and empowers the legal system to adequately deal with the phenomenon of terrorism by providing for the prevention and suppression of terrorism, and by reinforcing intelligence gathering, investigatory and enforcement measures relating to terrorism offences.

## **6. The Convention for the Suppression of the Financing of Terrorism Act 2003 – Refer to Annex I**

Same provides for the offences relating to the financing of terrorism in line with the International Convention for the Suppression of the Financing of Terrorism.

## **7. Prevention of Corruption Act 2002 (“POCA”) – Refer to Annex J**

The POCA provides for the prevention and punishment of corruption and for the establishment of an Independent Commission Against Corruption (“ICAC”). It must be noted that matters in which the FIU establishes a prima facie case are referred for investigation and prosecution to the ICAC, which has extensive powers of investigation and enforcement in the AML/CFT field. ICAC can investigate any matter concerning the laundering of money or suspicious transactions referred to it by the FIU.

## **8. The Dangerous Drugs Act 2000**

The Dangerous Drugs Act is designed to improve provisions for the control of dangerous drugs, the treatment of addiction, the prevention, detection and repression of drug trafficking, the prevention of laundering of drug money and the sentencing of drug-trafficking.

## **9. The Mutual Assistance in Criminal and Related Matters Act 2003**

Makes provision for mutual assistance between Mauritius and a foreign state or an international criminal tribunal in relation to serious offences and to provide for related matters.

## **10. Conventions**

In addition, there are a series of anti-money laundering and terrorist financing Conventions which Mauritius are party to:

- On 14 December 2004, the UN Convention against Corruption known as the Merida Convention was ratified by Mauritius.

- On 11 December 2004, Mauritius ratified the International Convention for the Suppression of the Financing of Terrorism.
- On 18 April 2003, Mauritius ratified the United Nations Convention against Transnational Organised Crime known as the Palermo Convention.
- In March 2001, Mauritius acceded to the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances known as the Vienna Convention.
- On 4 June 2001, Government ratified the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, commonly known as the Vienna Convention.

Additionally, with regard to terrorism, Government has already ratified or acceded to, as the case may be, the following United Nations Conventions:

- The International Convention for the Suppression of the Financing of Terrorism was signed on 11 November 2001 and ratified on 14 December 2004.
- The Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf was acceded on 3 August 2004.
- The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation was acceded on 3 August 2004.
- The Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents was acceded on 24 December 2003.
- The International Convention for the Suppression of Terrorist Bombings was acceded on 24 January 2003.
- The Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation of 1971 was signed in Montreal on 24 February 1988 and ratified on 17 August 1989.
- The Convention on the Suppression of Unlawful Acts against the Safety of Civil Aviation was signed at Montreal on 23 September 1971 and ratified on 25 April 1983.
- The Convention on the Suppression of Unlawful Seizure of Aircraft was signed at the Hague on 16 December 1970 and ratified on 25 April 1983.
- The Convention on Offences and Certain Other Acts Committed on Board Aircraft was signed at Tokyo on 14 September 1963 and ratified on 5 April 1983.
- The International Convention against the Taking of Hostages was signed in New York on 18 June 1980 and ratified on 17 October 1980.

## **PART B: ANTI-MONEY LAUNDERING AND TERRORIST FINANCING**

### **1. Money Laundering**

#### **a. What is Money Laundering**

Money Laundering is a generic term used to describe any process that conceals the origin or derivation of the proceeds of crime so that the proceeds appear to be derived from a legitimate source. The term “money laundering” is a misnomer as very often it is not money that is being laundered but other forms of property that directly or indirectly represent benefit from crime.

Money laundering is the process by which criminals try to conceal the true origin and ownership of proceeds of criminal activities so as to make it appear legitimate. Criminals try to disguise the origins of money obtained through illegal activities so that it looks like it was

obtained from legal sources. Otherwise, they can't use the money because it would connect them to the criminal activity, and law-enforcement officials would seize it. Money laundering has been defined in the FIAMLA – refer to Part A point 1.

There are three stages of money laundering which are:

- **Placement**  
The stage at which property (usually in the form of cash) is introduced into the financial system. This is the riskiest stage of the laundering process because usually large amounts of cash are involved and banks are required to report high-value transactions.
- **Layering**  
Layering is the stage at which property undergoes a series of transactions so as to conceal its origin and making it appear legitimate. This may take the form of bank transfers, purchasing high value items, changing the money's currency. That is, making the dirty money as hard to trace as possible.
- **Integration**  
This is the stage at which the laundered money re-enters the mainstream economy in legitimate-looking form. In the integration stage the criminal can use the money without getting caught.

## **b. Offences**

### **I. Offence of Money Laundering**

As per section 8 of the FIAMLA any person who is guilty of the offence of money laundering shall on conviction be liable to a fine not exceeding 2 million rupees and to penal servitude for a term not exceeding 10 years.

### **II. Offences in relation to failure to report**

The FIAMLA imposes an obligation on every bank, financial institution, cash dealer or member of a relevant profession or occupation to report all suspicious transactions to the FIU. Any bank, financial institution, cash dealer or any director or employee thereof or member of a relevant profession or occupation who, knowingly or without reasonable excuse -

- fails to make a report, supply an information requested by the FIU under section 13(2) (of the FIAMLA) verify, identify or keep records, registers or documents, as required under section 17 (of the FIAMLA);
- destroys or removes any record, register or document which is required under this Act or any regulations;
- warns or informs the owner of any funds of any report required to be made in respect of any transaction, or of any action taken or required to be taken in respect of any transaction, related to such funds; or
- facilitates or permits the performance under a false identity of any transaction falling within this Part, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

### **III. Offences in relation to Tipping Off**

Any person who is guilty of the offence of tipping off shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

The Tipping Off offence is committed when a person warns or informs the owner of any funds of any report or any action that is to be taken in respect of any transaction concerning such funds.

## **2. Terrorist Financing**

Terrorism refers to acts of terror, and the terrorist/groups that commits them require funding in the same way that criminal organizations require to further their criminal activities.

The POTA provides for the following:

- 1) Any person who-
  - (a) does, or threatens to do, or does an act preparatory to or in furtherance of, an act of terrorism; or
  - (b) omits to do anything that is reasonably necessary to prevent an act of terrorism, shall commit an offence
  
- (2) In this section, "act of terrorism" means an act which-
  - (a) may seriously damage a country or an international organisation; and
  - (b) is intended or can reasonably be regarded as having been intended to-
    - (i) seriously intimidate a population;
    - (ii) unduly compel a Government or an international organisation to perform or abstain from performing any act;
    - (iii) seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation; or
    - (iv) otherwise influence such government, or international organisation; and
  - (c) involves or causes, as the case may be-
    - (i) attacks upon a person's life which may cause death;
    - (ii) attacks upon the physical integrity of a person;
    - (iii) kidnapping of a person;
    - (iv) extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property, likely to endanger human life or result in major economic loss;
    - (v) the seizure of an aircraft, a ship or other means of public or goods transport;
    - (vi) the manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;
    - (vii) the release of dangerous substance, or causing of fires, explosions or floods, the effect of which is to endanger human life;
    - (viii) interference with or disruption of the supply of water, power or any other fundamental natural resource, the effect of which is to endanger life.

The different offences with regard to Terrorism are provided in the POTA.

## **PART C: AML/CFT PROCEDURES**

### **1. Policies and Procedures**

The Regulations require that Applicable Institutions establish policies and procedures to forestall and prevent money laundering and terrorist financing. Such policies and procedures must cover the following:

- customer due diligence measures;
- ongoing monitoring;
- reporting;
- record keeping;
- internal control;
- risk assessment and management;
- monitoring and management of compliance with and the internal communication of such policies and procedures in order to prevent activities related to money laundering and terrorist financing, and;
- risk profiling procedures.

The nature and extent of such policies and procedures will depend on a variety of factors, including:

- The identity of the client
- The occupation of the client
- The nature and type of client
- The commercial rationale for the relationship
- The geographical location of the client's residence
- The geographical location of the client's business interests and/or assets
- The value of the assets concerned in the relationship
- The nature of the assets concerned in the relationship
- The need for any delegated authority e.g. powers of attorney or mixed boards
- The source of funds
- The client's source of wealth
- The role of any introducer and the introducer's regulated or professional status

The objective of the institution's AML/CTF policies and procedures must be to ensure that the institution is able to identify, assess, monitor and manage money laundering and terrorist financing risk. Furthermore, the policies and procedures must be comprehensive and proportionate to the nature, scale and complexity of the institution's business.

The board of the Licensee must adopt internal AML/CFT policies and must establish internal procedures and allocate responsibilities to ensure that AML/CFT policies and procedures are managed effectively and are in line with applicable laws, codes and standards of good practice.

### **2. Money Laundering Reporting Officer ("MLRO") and Compliance Officer**

Money Laundering Reporting Officer must be appointed to whom all internal reports of suspicious transactions must be made. The MLRO must be a senior manager or a director of the company with relevant experience, competence, authority and independence to be able to discharge the reporting obligation effectively and autonomously. The company must also appoint a Deputy MLRO. Regulations also require for the appointment of a Compliance Officer. Institutions should provide the Commission with the contact information of the MLRO and compliance person and notify them of any subsequent changes to these positions.

### **3. Risk Profiling System**

Institutions must put in place systems and controls which reflect the degree of risk associated with their business and customers. The institution's policies and procedures should then set out criteria and situations which by their nature can present a higher risk of money laundering or terrorist financing. Such situations may include where the customer has not been physically present for identification purposes; correspondent banking relationships; and business relationships and occasional transactions with politically exposed persons.

## **PART D: CUSTOMER DUE DILIGENCE**

### **1. What is Customer Due Diligence**

The need for Licensees to know their customers is essential to the prevention of money laundering and combating the financing of terrorism. Customer Due Diligence (CDD) is a key element of an internal AML/CFT system.

CDD measures that should be taken by Licensees include-

- Identifying and verifying the identity of the applicant for business using reliable, independent source documents, data or information;
- Identifying and verifying the identity of the beneficial owner<sup>4</sup> such that the Licensee is satisfied that he knows who the beneficial owner is.
- Obtaining information on the purpose and intended nature of the business relationship; and
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions throughout the course of the business relationship to ensure that the transactions in which the customer is engaged are consistent with the Licensee's knowledge of the customer and his business and risk profile (including where necessary, the source of funds).

### **2. Identifying and Verifying the identity of applicants for business**

The cornerstone of an effective anti-money laundering system of controls is the requirement for the verification of identity of the applicant for business. Licensees must have in place clear procedures on how they will identify and verify the identity of their customers. These procedures must be brought to the knowledge of all relevant staff. Where an applicant for business is a natural person, Licensees must identify and verify the identity of the applicant for business. However, where the applicant for business is a legal person or arrangement, Licensees must verify the existence of the legal person or arrangement itself and identify and verify the identity of the principals thereof, that is, those natural persons with a controlling interest and those who comprise the mind and management of the legal person or arrangement.

Applicants for business include any natural person or legal person or arrangement - corporate or unincorporate that seeks to form a business relationship or to carry out a one-off transaction with a Licensee.

A principal of an applicant for business is any person who is a beneficial owner of, or who has a beneficial interest in, or has direct or indirect control of any relationship established with a Licensee.

## **1. Individual Requirements**

In Mauritius, the following information should be recorded in relation to each individual for whom identity should be verified:

- Full name (including any former names and any aliases);
- Date of birth;
- Place of birth;
- Nationality;
- Specimen signature;
- Permanent residential address;

Additionally, the following primary documentation should be obtained to verify the information recorded pursuant to the above:

- A certified copy of the pages of the individual's current valid passport, identity document (e.g. national identity cards, current valid driving licence, armed forces identity card) , or other official document showing his or her photograph and the information detailed above. The copy must be clear and legible including the photograph and should not be reduced or enlarged.
- Certified documentary or original form evidence (secondary documentation) of the individual's permanent residential address. This evidence can take the form of a recent bank or credit card statement, recent utility bill, recent original bank reference, or can be confirmed in a reference letter from a respected professional, conducting a credit agency search, checking a current register of electors, utilizing an address verification service or visiting the principal at their permanent address.

Certification (that the document is a true copy of the original and that the photograph is a true likeness, where applicable) should be by a notary public, actuary, lawyer, accountant, serving police or customs officer, member of the judiciary, senior civil servant, an employee of an embassy or consulate of the country of issue of the identity document, a professionally qualified director or secretary of a regulated financial services business in Mauritius or in an equivalent jurisdiction and a commissioner of oaths. The name and contact details of the certifier should be clearly stated.

## **2. Corporate Requirements**

In relation to corporate entities whose identity must be verified, Appleby Mauritius requires the following information:

### **a. Private Companies**

1. Original or certified copy of the certificate of incorporation or registration;
2. Certified copies of the Memorandum and Articles of Association, Bye-Laws, or other constitutional documents;
3. Certificate of good standing;
4. Evidence of the authority to enter into the business relationship;
5. Description of the company's activities;
6. Certified copies of any Powers of Attorney granted in relation to the company;
7. Names and addresses of all authorised signatories on the company's accounts;
8. Certified copy of the Register of Members/Shareholders or equivalent;

9. Satisfactory evidence of identity for at least two Directors, authorised signatory and instructing party, as detailed in the Individual and Corporate Requirements sections, as appropriate; and,
10. Satisfactory evidence of identity for each beneficial owner, as detailed in the Individual and Corporate Requirements sections, as appropriate, for those holding a 20% or greater interest in the company.

**b. Societes**

1. Original or certified copy of the acte de société;
2. Certified copies of the Memorandum and Articles of Association, Bye-Laws, or other constitutional documents;
3. Certificate of good standing for foreign sociétés or if Mauritian check with the Registrar of Companies that the sociétés continues to exist;
4. Evidence of the authority to enter into the business relationship;
5. Description of the société's activities;
6. Certified copies of any Powers of Attorney granted in relation to the company;
7. Names and addresses of all authorised signatories on the company's accounts;
8. Certified copy of the Register of Principals, Administrators or Gerants or equivalent;
9. Satisfactory evidence of identity for all Principals, Administrators or Gerants, authorised signatory and instructing party, as detailed in the Individual and Corporate Requirements sections, as appropriate.

**c. Partnership Requirements**

Identification documents for all partners who own or control more than 20% of the partnership, as detailed above in the Individual and Corporate Requirements sections (as appropriate), should be obtained in Mauritius.

Additionally, the following information should be gathered:

1. Original or certified copy of the partnership deed;
2. Copy of the latest report and accounts;
3. Verification of the nature of the business of the partnership to ensure that it is legitimate;
4. Verification that any person that purports to act on behalf of the partnership is so authorised and identifying that person;

**d. Trust Requirements**

For all trusts, a certified copy of the trust deed and any amendments must be obtained.

Additionally, the following information should be gathered:

1. If the Trustee is regulated for money laundering purposes in an "approved country" (see below), verification of regulation and, if applicable, incorporation, existence and licensing of the trustee;
2. The same information as required above for an individual or corporate entity in respect of the following:
  - a. the Trustee (if not regulated);
  - b. the Settlor or original beneficial owner of the trust assets;

- c. depending on the terms of the trust, any named non-discretionary Beneficiaries; and
  - d. any Protector, Enforcer or other person on whose instructions or in accordance with whose wishes the Trustee is prepared or accustomed to act or who may appoint and/or remove the Trustee or investment advisor to the trust.
3. An explanation of the source of the funds comprised in the trust fund.

### **3. Timing of Verification**

Effective CDD measures should be undertaken when:

- establishing a business relationship with an applicant for business;
- carrying out a one-off transaction or occasional transactions where the total amount of the transactions which is payable by or to the applicant for business is above 500,000 rupees or an equivalent amount in foreign currency; or
- there is a suspicion of money laundering or terrorist financing.

### **4. Ongoing Monitoring**

Ongoing due diligence should be conducted on the business relationship and scrutiny of transactions throughout the course of the business relationship to ensure that the transactions in which the customer is engaged are consistent with the Licensee's knowledge of the customer and his business and risk profile (including where necessary, the source of funds).

### **5. Reliance on Third Parties**

In some situations, it may be appropriate to rely on client identification verification performed by a third party. In order to do so, Appleby Mauritius must obtain a written "eligible introduction" (see appendix IV in the Codes) from a regulated institution in an "approved country" or Appleby group introducers.

It is important to note that the responsibility for ensuring that satisfactory evidence of identity is obtained and that the appropriate records are retained rests with the financial services provider, not the introducer.

### **6. Simplified or Reduced Due Diligence**

In general, the full range of CDD measures should be applied to all applicants for business. However, where the risk of money laundering or the financing of terrorism is lower and where information on the identity of the applicant for business is publicly available or where adequate checks and controls exist elsewhere in national systems, it may be reasonable for Appleby Mauritius to apply reduced or simplified due diligence measures when identifying and verifying the identity of the applicant for business. Reduced or simplified measures could be applied where applicants for business include:

- Regulated financial institutions in Mauritius or "approved countries" (see below) provided that we are satisfied that the applicant for business is not acting on behalf of underlying principals such as trustees. Documentary evidence of the existence of the financial services business and regulated status must be obtained;
- 2. Companies that are publicly traded the Stock Exchange of Mauritius or on recognized exchanges (see Appendix V of the Codes) and their subsidiaries.

Documentary evidence of the existence of the public company and listed status must be obtained. In addition, a copy of the annual report and accounts must be obtained and verification that the individuals that purport to act on behalf of such entities have the authority to do so.

- Government administrations, or enterprises and statutory bodies;
- A pension, superannuation or similar scheme that provides retirement benefits to employees where contributions are made by way of deduction from wages and the schemes rules do not permit the assignment of a member's interest under the scheme. In all transactions undertaken on behalf of an employer sponsored scheme we must at a minimum identify and verify the identity of the employer and the trustees of the scheme as detailed in the Individual and Corporate Requirements sections, as appropriate. Where it is determined that simplified or reduced CDD measures should apply to an applicant for business that does not fall within the categories above, FSC approval must be obtained prior to applying such measures.

## **7. Equivalent Jurisdiction**

Below is the list of jurisdictions, as published in the Codes with legislation considered to be equivalent to that of Mauritius.

Australia  
Austria  
Bahamas  
Bermuda  
Belgium  
Canada  
Cayman Islands  
Denmark  
Finland  
France  
Germany  
Gibraltar  
Greece  
Guernsey  
Hong Kong  
Iceland  
Ireland  
Isle of Man  
Italy  
Japan  
Jersey  
Luxembourg  
Mexico  
Netherlands  
Netherlands Antilles  
New Zealand  
Norway  
Portugal  
Russian Federation  
Singapore  
South Africa  
Spain

Sweden  
Switzerland  
Turkey  
United States of America

If the customer is connected with a non-Equivalent Jurisdiction, it does not prevent the Applicable Institution from establishing a business relationship or carrying out an occasional transaction with the customer. It may mean, however, that the Applicable Institution will need to apply enhanced due diligence.

## **8. Enhanced Due Diligence**

Licensees should apply enhanced due diligence measures in all high risk business relationships, customers and transactions. These include both high risk business relationships assessed by the Licensee based on the customer's individual risk status and the following categories of business relationships-

- Politically Exposed Persons
- Non face-to-face business relationships
- NCCTs and non-equivalent jurisdictions

## **9. Politically Exposed Persons**

PEPs are individuals who are or who have been entrusted with prominent public functions (for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials). Licensees should be aware that business relationships with family members of PEPs are deemed to pose a greater than normal money laundering risk to Licensees by virtue of the potential for them to have benefited from corruption.

The nature of the parties concerned in PEP scandals attracts worldwide media attention. They can therefore be enormously damaging to the reputation of both the organisation and the jurisdictions concerned.

Licensees must know when they are in a relationship concerning a PEP and must be able to demonstrate the application of enhanced due diligence measures in conducting such relationships. Licensees must have appropriate risk management systems to determine whether an applicant for business is a PEP. In addition, Licensees must develop a clear policy on the acceptance of business relationships with such individuals. The approval of senior management should be obtained prior to establishing relationships with such applicants for business.

Licensees must take reasonable measures to establish the source of wealth and source of funds of a PEP. Lastly, Licensees must conduct enhanced ongoing monitoring of their business relationships with PEPs. The risks associated with PEPs differ according to the particular countries concerned. The risk of corruption in certain countries is higher than it is in others. Licensees should note the Transparency International Corruption Perceptions Index at [www.transparency.org](http://www.transparency.org) and take appropriate measures to manage the increased risks of conducting business with PEPs.

## **PART E: SUSPICIOUS ACTIVITY REPORTING**

### **1. Suspicious Transactions**

The FIAMLA defines a suspicious transaction as follows:

"...suspicious transaction" means a transaction which:-

- (a) gives rise to a reasonable suspicion that it may involve
  - (i) the laundering of money or the proceeds of any crime; or
  - (ii) funds linked or related to, or to be used for, terrorism or acts of terrorism or by proscribed organisations, whether or not the funds represent the proceeds of crime;
- (b) is made in circumstances of unusual or unjustified complexity;
- (c) appears to have no economic justification or lawful objective;
- (d) is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or
- (e) gives rise to suspicion for any other reason.

"transaction" includes:-

- (a) opening an account, issuing a passbook, renting a safe deposit box, entering into a fiduciary relationship or establishing any other business relationship, whether electronically or otherwise; and
- (b) a proposed transaction.

Not all unusual or unexpected activity is necessarily suspicious activity. As a first step, Licensees are expected as a result of effective CDD measures to be able to recognise unusual activity and then to analyse it in more detail to ascertain whether the activity is in fact suspicious. This may entail making discreet client enquiries (using a customer service approach).

Licensees are not under a duty to ascertain whether suspected conduct is in fact criminal conduct in the country in which it is committed. The issue for Licensees is whether the conduct would be a crime if it had been committed in Mauritius. Licensees need not know the exact nature of suspected criminal activity. Further, Licensees need not be certain that the particular property it is handling represents the proceeds of crime. The FIAMLA simply requires a person to suspect that the property may derive from crime.

In the event that an activity is found to be suspicious, a Licensee must report it and the circumstances surrounding it to the FIU. Licensees should bear in mind that in the event of a suspicion of money laundering, a suspicious transaction report should be made even where there has been no transaction by or through a Licensee.

### **2. Reporting Suspicious Transactions**

#### **a. Internal Suspicious Transaction Report (STR)**

Employees of Licensees will discharge their legal obligations under the FIAMLA by disclosing their suspicions to the MLRO in accordance with the Licensee's internal procedures.

The obligation to report knowledge or suspicion of possible money laundering or terrorist financing affects all employees of a Licensee. AML/CFT policies must require employees to make internal STRs to the MLRO where they have knowledge or suspicion that another person is engaged in money laundering or terrorist financing. The STR should be concise and provide all relevant

information to allow the MLRO to be able to determine if an external STR should be filed with the FIU.

#### **b. External Suspicious Transaction Report**

It is the responsibility of the MLRO or deputy MLRO to review all internal STRs and determine, in the light of all relevant information, whether or not the information or other matter contained in the report does give rise to such a knowledge or suspicion which should be reported to the FIU.

In making his determination, the MLRO must have access to and review all relevant information including the original customer due diligence. In some cases, it may be appropriate to obtain further information from the customer, however, care must be taken in such situations so as to avoid any possible tipping off of the customer.

Care should be taken when a filing is made prior to a transaction being completed that the filing does not lead to the unnecessary freezing of a customer's account, thus affecting other, non-suspicious transactions.

### **PART F: FURTHER INTERNAL POLICIES AND PROCEDURES**

#### **1. Staff Training and Awareness**

In order to facilitate recognition and handling of suspicious transaction reports, Licensees must make arrangements for on-going training of all employees. Training should cover recognition and handling of suspicious transactions and additional measures to maintain a high level of awareness and vigilance between training sessions. The FSC regards this as a "reasonable measure" under the FIAMLA.

Training must be relevant both to the role and the seniority of the employee and should take account of relevant financial services and products.

Within 14 days of being employed – but in any event before a new employee begins to engage in the provision of financial services, he/she must receive AML/CFT awareness training and training on the AML/CFT procedures that are in place within the organisation.

All employees should receive refresher AML/CFT training on an annual basis. The training should be relevant to the role that employees fulfill and should include the following:

- Legal obligations
- The money laundering/terrorist financing vulnerabilities of relevant services and products
- Internal controls and CDD measures
- Recognition and handling of suspicious transactions

As MLROs and Deputy MLROs have significant responsibility for the receipt, evaluation and where appropriate external reporting of suspicious transactions to the FIU, MLROs and Deputy MLROs should be given additional training in the recognition and handling of suspicious transactions.

MLROs and Deputy MLROs should familiarise themselves with the annual FATF Typology Reports that examine trends in money laundering activity. They should also know which countries comprise the current list of FATF NCCTs.

## 2. Record Keeping

Record keeping is an important control mechanism. Where a Licensee suspects an applicant for business, or where there is an investigation into the conduct of an applicant for business (whether in Mauritius or elsewhere), the records maintained by Licensees may prove to be very valuable.

Licensees are obliged to maintain records of internal suspicious transaction reports and suspicious transaction reports made to the FIU. These records should be retained for the duration of the client relationship and all records should be retained for a period of at least 7 years after the completion of the transaction to which they relate.

In order to assist law enforcement to follow audit trails should the need arise, Licensees must maintain records of all transactions undertaken during the course of a client relationship either in the form of original documents or copies of original documents. All transactional records should be retained for a period of at least 7 years after the completion of the transaction to which they relate.

Transactional records include records containing information on individual transactions as follows:

- source of funds including full remitter details
- volume of funds
- destination of funds
- instructions
- forms of authority
- counterparty details
- sale and purchase agreements
- service agreements
- date of transactions

Licensees must retain copies of all documentation used to verify the identity of all applicants for business. Identity records should be maintained for the duration of each relationship and for a period of at least seven years thereafter.

Licensees must maintain records of all AML/CFT training delivered to employees. Records should include details of content, dates, mode of delivery, and the names of trainees.

Records may consist of original hard copy documents, electronic data or documents maintained on microfiche. In any event, records should be capable of being easily and quickly retrieved by Licensees.

Records held by third parties are not considered to be in a readily retrievable form unless the Licensee is reasonably satisfied that the third party is itself an institution which is able and willing to keep such records and disclose them to it when required.

Licensees should consider whether they would be able to retrieve documents in the event of a disaster or in the event of the destruction of documents. Licensees should consider what contingency arrangements may be necessary to create or replace records in the event of a disaster.

For more specific advice on Anti-Money Laundering and Anti-Terrorist Financing in Mauritius, we invite you to contact one of the following:

Malcolm Moller  
Managing Partner – Mauritius  
+230 203 4301  
[mmoller@applebyglobal.com](mailto:mmoller@applebyglobal.com)

Gilbert Noel  
Partner, Mauritius  
+230 203 4302  
[gnoel@applebyglobal.com](mailto:gnoel@applebyglobal.com)

Appleby is the leading provider of offshore legal, fiduciary and administration services. With an unparalleled presence in the key offshore jurisdictions of Bermuda, the British Virgin Islands, the Cayman Islands, Isle of Man, Jersey, Mauritius and the Seychelles, the group offers advice on offshore law. We also have offices in the international financial centres of London, Hong Kong, Zurich and Bahrain.

Over 800 lawyers and professional specialists deliver sophisticated, specialised services, primarily in the areas of Corporate and Commercial; Litigation and Insolvency; Private Client and Trusts; and Property. We advise global public and private companies, financial institutions, and high net worth individuals, working with them and their advisers to achieve practical solutions, whether in a single location or across multiple jurisdictions.

This publication is intended only to provide a summary of the subject matter covered. It does not purport to be comprehensive or to provide legal advice. No person should act in reliance on any statement contained in this publication without first obtaining specific professional advice.

If this guide has been sent to you, and you would like to update your details or be removed from our marketing database, please contact the marketing department at Appleby or e-mail [info@applebyglobal.com](mailto:info@applebyglobal.com).

Bahrain  
Bermuda  
British Virgin Islands

Cayman Islands  
Hong Kong  
Isle of Man

Jersey  
London  
Mauritius

Seychelles  
Zurich