CODE ON THE PREVENTION

of

MONEY LAUNDERING

&

TERRORIST FINANCING

intended for

MANAGEMENT COMPANIES

(Issued under Section 7(1)(a) of the Financial Services Development Act 2001 and Section 18(1)(a) of the Financial Intelligence and Anti-Money Laundering Act 2002)

15 July 2005

The Code on the Prevention of Money Laundering and Terrorist Financing intended for Management Companies was approved by the Board of the FSC on 20 July 2005.

The Code was issued on 22 July 2005 and comes into force on 01 August 2005.

Contents **Page**

Preface

The Financial Services Commission ("FSC") first issued its Codes on the Prevention of Money Laundering and Terrorist Financing in April 2003. Since that time, anti-money laundering and combating the financing of terrorism ("AML/CFT") initiatives have developed both nationally and internationally.

At the national level, a number of legislative changes have been introduced to enhance the existing AML/CFT legal framework. For instance, the Financial Intelligence and Anti-Money Laundering Regulations 2003 ('the Regulations') were enacted and came into operation in June 2003. Further, changes which affected the Financial Services Commission ('FSC') were made to the Financial Intelligence and Anti-Money Laundering Act 2002 (FIAML Act) by the Anti-Money Laundering (Miscellaneous Provisions) Act 2003. The FSC has thus been given statutory responsibility for supervising and enforcing compliance by licensees (including Management Companies) of the requirements imposed under the FIAML Act and regulations or guidelines which are made under the FIAML Act. Additionally, operational difficulties with respect to the implementation of the Codes have highlighted a number of areas where the Codes need to be strengthened, clarified or refined.

At the international level, the FATF announced the completion of its revision of the Forty Recommendations and produced a new comprehensive framework for combating money laundering and terrorist financing. In February 2004, the FATF adopted the AML/CFT Methodology 2004 - which will now be used in the assessment/evaluations of a country's compliance with the revised Recommendations of the FATF.

All these factors have made a review of the Codes desirable. For this purpose a working group (referred to as the AML/CFT Working Group) was established. The Working Group comprised representatives of the Association of Offshore Management Companies, the Port Louis Stockbroking Association, the Insurers' Association of Mauritius, and providers of custodial services. The objectives of the review included:-

- To make the requirements of the Codes consistent with the Revised FATF 40 Recommendations and the Eight Special Recommendations on Terrorist Financing;
- To remove any inconsistency between the requirements of the Codes and the national AML/CFT regulatory regime;
- To eliminate unnecessary duplication of obligations;
- To make the playing field as level as possible; and
- To balance the regulatory burden with the effectiveness of the requirements.

In October 2004, the FATF added another element to its counter-terrorist financing standards-Special Recommendation IX-which deals with cross-border movements of

currency and monetary instruments related to terrorist financing and money laundering.

One of the FSC's key imperatives is to ensure that the financial services sector in Mauritius is not used for money laundering and terrorist financing purposes. Achieving this objective will not be possible without the active assistance of all licensees. The FSC acknowledges with gratitude the substantial input of the AML/CFT Working Group's members and of other interested parties who have contributed to the review process-which has culminated in this updated Code.

This Code comes into force on 01 August 2005.

Financial Services Commission
15 July 2005

Introduction

The success of Mauritius as a centre for the provision of financial services depends (inter alia) upon the maintenance of its reputation of probity. It is therefore vital that all Licensees in Mauritius exercise appropriate care to avoid entering into a business relationship with anyone who is a criminal or whose intentions are to launder the proceeds of crime or to engage in terrorist financing.

Mauritius fully supports international initiatives to prevent money laundering and to combat terrorist financing. That being so, this Code takes account of all relevant international standards which include-

- the Financial Action Task Force's (FATF) Revised 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),
- IOSCO's Principles on Client Identification and Beneficial Ownership for the Securities Industry, and
- IAIS' Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities.

In addition to being committed to preventing the exploitation of the financial services industry in Mauritius by money launderers and terrorist financiers, the FSC wishes to play its part in preventing arbitrage between the anti-money laundering laws and practices of different jurisdictions.

The FSC believes that the implementation of, and adherence to, effective customer due diligence and vigilance procedures play a central role in the prevention of money laundering and terrorist financing by Licensees. In addition to reducing the risk of exposure to money laundering and terrorist financing, effective customer due diligence practices also protect Licensees against a range of other potentially damaging risks including reputational risk, legal risk and the risk of regulatory sanction.

This Code applies to all persons holding a Management Licence issued by the FSC under section 24(2) of the Financial Services Development Act 2001.

1 Purpose and Status of this Code

This Code is issued by the FSC pursuant to its functions and powers under sections 6(d) and 7(1)(a) of the Financial Services Development Act 2001 ("FSD Act") and section 18(1)(a) of the Financial Intelligence and Anti-Money Laundering Act 2002 ('FIAML Act'). The Code is intended to assist Licensees[1] to comply with the obligations contained within the FIAML Act.

The Code is designed to serve as a statement of minima criteria and to describe operational practices expected of Licensees. Non-compliance with the Code will expose the Licensee to regulatory action which may include a direction under section 7(1)(d) of the FSD Act to observe the Code. Failure to comply with the direction may lead to criminal sanction and to regulatory action under sections 7(1)(e) and 24 (5) of the FSD Act.

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 visits. As such, a Licensee's commitment to prevent the wrongful exploitation of its services by the implementation of policies, procedures, staff training and the creation of an effective internal compliance culture will be directly relevant to its ongoing status as a Licensee and to the assessment of the fitness and properness of its principals.

Where a Licensee has a particular difficulty in complying with any aspect of this Code, it should pro-actively advise the FSC - which will consider each case on its merits.

Licensees should note that compliance with the Code will not constitute a defence to a prosecution for an offence under the FIAML Act.

The FSC believes that the long term sustainability of the finance industry in Mauritius is best served by the implementation of best practice standards – such as those described in this Code.

Given that the Code provides "minima criteria", Licensees must consider what additional measures to adopt to prevent them and their services from being used to launder money or to finance terrorism.

Licensees should note that this Code will be subject to review and may be amended from time to time.

[1] For the purposes of this Code, "Licensee" means a management company or a corporate trustee holding a Management Licence issued by the Commission under section 24(2) of the FSD Act.

1.1 *Internal AML/CFT Framework*

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 that meet AML/CFT legal obligations are introduced and maintained.

The FSC believes that a Licensee's internal AML/CFT policies and procedures must at least cover the following core principles:-

- Licensees must, when establishing a business relationship with an Applicant for Business apply appropriate Customer Due Diligence measures including identifying and verifying the identity of the Applicant for Business.

- Licensees must appoint a Money Laundering Reporting Officer and have in place documented internal systems of suspicious transaction reporting.

- Licensees must implement effective on-going Customer Due Diligence measures and risk profiling procedures.

- Licensees must provide members of their staff with on-going AML/CFT training.

- Licensees must implement and maintain effective record keeping systems.

These core principles are developed in more detail in sections 4 to7 of the Code.

2. Money Laundering and Terrorist Financing

2.1. *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.

Money laundering is sometimes wrongly regarded as an activity that is associated only with organised crime and drug trafficking. It is not. It occurs whenever any person deals with another person's direct or indirect benefit from crime.

The term 'money laundering' is in fact a misnomer. Often it is not money that is being laundered but other forms of property that directly or indirectly represent benefit from crime. Any form of tangible or intangible property is capable of representing another person's benefit from crime.

Traditionally, money laundering has been described as a process that takes place in three stages as follows:

Placement – The stage at which property (usually in the form of cash) is introduced into the financial system;

Layering – The stage at which the property undergoes a series of transactions, thus concealing its origin and making it appear to be legitimate;

Integration – The stage at which the laundered money is utilised for the benefit of criminals within the legitimate economy.

In reality, the three stages often overlap and the benefit from many crimes including most financial crimes does not need to be 'placed' into the financial system. Licensees in Mauritius are most likely to be exposed at the layering and integration stages of the money laundering process.

Money laundering is a crime that is most often associated with banking and money remittance services. Whilst banks are often an essential part of successful laundering schemes, management companies and their client companies, including trust administration and related services that they offer are also highly vulnerable to abuse by money launderers. This is because of the opportunities that they present to conceal and disguise ownership and interest in criminally derived property by transferring legal ownership of such property to third parties. Beneficial ownership can then be further disguised by the use of nominees.

It is imperative for the protection of the financial services sector in Mauritius, that Licensees fully appreciate the money laundering vulnerabilities of the services that they offer.

2.2. *International AML/CFT initiatives*

The international community has taken and continues to take concerted action against money laundering and terrorist financing. The FSC wishes to draw Licensees' attention to some of the more influential initiatives with which Mauritius as a financial centre must comply.

2.2.1. Financial Action Task Force (FATF)

The FATF's Forty Recommendations and Nine Special Recommendations on Terrorist Financing are perhaps the most influential supra national initiatives in this arena. Mauritius has confirmed its adherence to the FATF Recommendations through its membership of the Offshore Group of Banking Supervisors ("OGBS"). Mauritius is also an active member of the Eastern and Southern African Anti-Money Laundering Group ("ESAAMLG"), which is an FATF style regional body ("FSRB"). FSRBs are important components of the global network of international organisations and bodies that combat money laundering and terrorist financing. These bodies are committed to implementing the FATF Recommendations.

In 1999, the FATF launched an initiative to examine the anti-money laundering laws and practices of non–member countries. One of the outcomes was the creation of a list of Non Co-operative Countries and Territories ("NCCTs"). A number of jurisdictions have gained the ignominious status of an FATF NCCT. As a result, the international reputation of such jurisdictions has suffered and in some cases, FATF member states have taken 'defensive action' against them by requiring businesses to exercise enhanced due diligence when dealing with individuals or businesses based within NCCTs.

The reputation of Mauritius as a leading centre for the provision of high quality financial services prevented it from being labelled by the FATF as a NCCT.

Further information on the FATF may be obtained from its website at www.fatf-gafi.org.

2.2.2. Basel Committee on Banking Supervision

Whilst its name suggests that the Basel Committee is concerned solely with the conduct of banking business, it has been highly influential in

shaping opinion on the importance of effective client due diligence across the financial sector. The Basel Committee's Paper on Customer Due Diligence clearly demonstrates the importance of Customer Due Diligence information in the management of risk.

Additional information on the Basel Committee including the full text of the Paper on Customer Due Diligence can be obtained by visiting the website of the Bank for International Settlements at www.bis.org

2.2.3. The Wolfsberg Group

Comprised of some of the world's leading private banks, the Wolfsberg Group has issued Global Anti-Money Laundering Guidelines and a Statement on the Suppression of the Financing of Terrorism.

More information may be obtained about the Wolfsberg Group from its website at www.wolfsberg-principles.com

2.2.4 International Organisation of Securities Commissions (IOSCO)

In 1992, IOSCO adopted a resolution inviting IOSCO members to consider issues relating to minimizing money laundering. More recently, in May 2004, IOSCO adopted a paper on Principles of Client Identification and Beneficial Ownership for the Securities Industry. The IOSCO Statement of Principles provides a comprehensive framework relating to Customer Due Diligence requirements that complements FATF's Recommendations and addresses the securities regulator's role in monitoring industry compliance with AML obligations.

More information may be obtained about IOSCO from its website at www.iosco.org.

2.2.5 International Association of Insurance Supervisors (IAIS)

The IAIS has given high priority to the fight against money laundering and terrorist financing. In October 2003, the IAIS revised and expanded its Insurance core principles and methodology. Compliance with these core principles is required for an insurance supervisory system to be effective. As part of this revision, new Insurance core principle 28, which deals specifically with anti-money laundering and combating the financing of terrorism, was introduced.

In October 2004, the IAIS adopted a new Guidance Paper on anti-money laundering and combating the financing of terrorism. This guidance paper replaces the anti-money laundering guidance paper for insurance supervisors and insurance entities which was issued in

January 2002. The new guidance paper takes into account the revised FATF 40+ 8 Special Recommendations and the Methodology for Assessing compliance with the FATF 40 recommendations and the 8 special recommendations issued in February 2004. The full text of the Paper can be obtained by visiting the website of the IAIS at www.iaisweb.org.

In addition to the initiatives highlighted above, other initiatives have been taken by the United Nations, the Commonwealth Secretariat, The International Monetary Fund, the World Bank and the OECD.

Licensees are reminded that Mauritius does not and cannot operate in isolation. The expectations of the international community cannot be ignored. Accordingly, the FSC is determined to ensure that Mauritius discharges its role as a member of the international financial community responsibly - by meeting international AML/CFT standards.

2.3. *Terrorist financing*

Acts of terror and the terrorist groups that commit them require funding in much the same way that criminal organisations require money to further their criminal activities. Since the events of September 11th in the United States, the prevention of the financing of terrorism by the financial sector has gained equal status with the prevention of the laundering of the proceeds of crime.

There are both similarities and differences between money laundering and terrorist financing. Differences include:

- Terrorist financing is an activity that supports future illegal acts, whereas money laundering generally occurs after the commission of illegal acts;

- Legitimately derived property is often used to support terrorism, whereas the origin of laundered money is illegitimate;

Similarities include:

- Terrorist groups are often engaged in other forms of criminal activity which may in turn fund their activities;

- Both money laundering and terrorist financing require the assistance of the financial sector.

The key to the prevention of both money laundering and terrorist financing is the adoption of adequate CDD measures by all Licensees both at the commencement of every relationship and on an on-going basis thereafter.

2.4 *Extra territorial powers of the United States*

Following the events of September 11th, the United States rapidly introduced a new piece of legislation, which has come to be referred to as the USA PATRIOT Act[2]. This legislation extended the extra territorial civil and criminal jurisdiction of the United States by amending existing US anti-money laundering legislation. Licensees should note that the United States' courts can now claim jurisdiction over any foreign person, including any financial institution authorised under the laws of a foreign country in circumstances where such a person commits any offence under US anti-money laundering laws. This means that any foreign person who conducts a transaction involving US dollars is subject to the jurisdiction of the US courts in respect of US anti-money laundering offences.

[2] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001

3. The Legislative Framework in Mauritius

3.1. *The Financial Intelligence and Anti-Money Laundering Act 2002*

The principal anti-money laundering legislation in Mauritius is the Financial Intelligence and Anti-Money Laundering Act 2002 (the "FIAML Act") which repealed the Economic Crime and Anti-Money Laundering Act 2000. The offences of money laundering are contained within Part II, Section 3 of the FIAML Act and may be summarised as follows:

3.1.1. Part II of the FIAML Act

Section 3(1)(a)

Engaging in a transaction involving property which represents the proceeds of any crime while suspecting or having reasonable grounds to suspect that the property derives from any crime.

Section 3(1)(b)

Receiving, possessing, concealing, disguising, transferring, converting, disposing or removing from or bringing to Mauritius property which represents the proceeds of any crime while suspecting or having reasonable grounds to suspect that the property derives from any crime.

Reference to property within both offences means any property which is in whole or in part, directly or indirectly the proceeds of any crime. Crime includes any crime in Mauritius as defined by the Criminal Code and any conduct committed outside Mauritius (whether or not it is regarded as a crime in the country in which it is committed), which if it had taken place in Mauritius would have constituted a crime in Mauritius.

Licensees should appreciate the following in relation to the offences:

- A person may be convicted of a money laundering offence notwithstanding the absence of any conviction of another person for any underlying predicate crime – the proceeds of which are allegedly laundered.

- The offences contain an important objective test of suspicion. The test means that it is possible for the offences to be committed in circumstances where a person ought to have reasonable grounds to suspect that property had derived from crime, even where they did not actually suspect that to be the case.

- The offences can be committed in relation to proposed as well as to actual transactions.

- A separate offence of conspiracy to commit an offence is contained within section 4 of the FIAML Act.

In addition to the offences of money laundering, section 3(2) of the FIAML Act makes it an offence to fail to take reasonable measures to ensure that neither the Licensee nor its services are capable of being used to launder money or to facilitate money laundering. In addition, section 17 of the FIAML Act imposes requirements upon Licensees to adopt specific anti-money laundering measures including-

- Verification of identity procedures; and

- Record keeping procedures.

Each of the offences within Part II of the FIAML Act is punishable by a maximum fine of 2 million rupees and 10 years imprisonment.

3.1.2. Part IV of the FIAML Act

Suspicious Transaction Reporting

Section 14 of the FIAML Act imposes an obligation upon all Licensees to report all suspicious transactions to the Financial Intelligence Unit ("FIU"). Licensees should note that failure to report a suspicious transaction is an offence under the FIAML Act. Failure to report can render a person liable to prosecution for the offence of failing to report under section 19 of the FIAML Act.

By prohibiting proceedings against any Licensee that reports in good faith or that provides information to the FIU upon the request of the latter, section 16 of the FIAML Act affords Licensees protection against liability resulting from making a suspicious transaction report. This protection is against both civil and criminal proceedings.

Tipping Off

Section 19 (1)(c) of the FIAML Act provides for the offence of 'tipping off' - which 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.

3.2. *The Financial Services Development Act 2001*

The FSD Act regulates the conduct of business by Licensees and makes provision for the regulatory and supervisory powers of the FSC. Pursuant to the FSD Act, the FSC has powers to enable it to discharge its functions, including those which arise under section 7(1) and under section 24(5)(a)(iii).

Further, section 18 (3) of the FIAML Act empowers the Commission to proceed against a Licensee under section 7 of the FSD Act on the grounds that it is carrying on its business in a manner which is contrary or detrimental to the interests of the public.

For the purposes of the exercise of this power, the FSC will have regard to the extent to which a Licensee takes positive action to protect itself against the threat of money laundering and terrorist financing by complying with this Code.

3.3 *Exchange of Information between the FSC and the FIU*

Section 21(1) of the FIAML Act empowers the FIU to pass on to the FSC any information which may be relevant to any of the FSC's functions.

Section 22 of the FIAML Act empowers the FSC to pass on to the FIU any information suggesting the possibility of a money laundering offence or suspicious transaction.

4. 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. Licensees must undertake effective CDD measures when-

- establishing a business relationship with an applicant for business;
- carrying out a one-off transaction or occasional transactions[3] where the total amount of the transactions which is payable by or to the applicant for business is above 350,000 rupees or an equivalent amount in foreign currency; or
- there is a suspicion of money laundering or terrorist financing.

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[4]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).

4.1 *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

[3] "occasional transactions"means two or more one-off transactions that are linked or appear to be linked.
[4] The FSC regards the beneficial owner as the natural person (s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

business in accordance with the measures outlined in paragraph 4.1.1. 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.

For the avoidance of doubt, principals of applicants for business include the following:

- Settlors or Contributors of capital (whether named or otherwise)
- Trustees
- Beneficiaries[5]
- Protectors
- Enforcers
- Company Directors[6]
- Controlling shareholders[7]
- Account signatories
- Significant Partners including Limited Partners[8]
- Any person operating under a Power of Attorney

Whether or not an applicant for business is a company or a trust or a partnership or a *société*, a Licensee must verify the identity of the ultimate individual principals of such applicants in the same way that they are expected to verify the identity of direct personal clients. This is in addition to verifying the existence of such legal persons or arrangements themselves.

[5] The FSC understands that in the case of discretionary trusts it is not always possible to expect a Licensee to obtain verification of identity of all class members. It can also be difficult to verify the identity of minor beneficiaries. In such cases, the FSC considers that verification of identity of such beneficiaries may be delayed until prior to the making of any distributions to them.

[6] The FSC expects Licensees to verify the identity of at least two directors of corporate applicants for business.

[7] The FSC regards as controlling shareholder- any person who is entitled to exercise, or control the exercise of, 20 per cent or more of the voting power at general meetings of the company or one which is in a position to control the appointment and/or removal of directors holding a majority of voting rights at board meetings on all or substantially all matters.

[8] The FSC regards as significant any partner owning or controlling 20 percent or more of a partnership.

4.1.1 Verification of identity of natural persons

Identity comprises the following elements:

- Name (including any former names and any aliases)
- Permanent residential address[9]
- Date of birth
- Place of birth
- Nationality

Primary identity documentation must be obtained and retained by all Licensees to verify the information provided by principals about their identity. The documentation must be pre-signed and must be either in an original form or must be certified appropriately - and should bear a photograph of the principal. The following types of primary identity documentation can be relied upon:

- Current valid passports

  Licensees should note that the FSC will expect them to cross refer copy passports with which they are unfamiliar in terms of look, style and format, to a passport reference Code.

- National Identity cards
- Current valid driving licences
- Armed forces identity cards

In addition to primary identity documentation, Licensees must also obtain additional verification of identity information (secondary identity documentation). Secondary documentation must be either in an original form or must be appropriately certified. The following types of secondary identity documentation can be relied upon:

- A recent original utility bill;
- A recent original bank or credit card statement; or

[9] PO Box addresses are not acceptable as permanent residential addresses of principals and may not be used in substitution thereof by Licensees.

[12] For the avoidance of doubt, reduced or simplified due diligence measures do not apply to applicants for business acting as trustees.

- A recent original bank reference.

Alternatively, additional verification may be achieved by:

- Obtaining a reference from a professional person who knows the principal. The reference must include the permanent residential address of the principal;

- Conducting a credit reference agency search;

- Checking a current register of electors;

- Utilising an address verification service; or

- Visiting the principal at the principal's permanent residential address.

4.1.2 Verifying the existence of a legal person or arrangement and identifying the principals thereof

Where an applicant for business is a legal person or arrangement, Licensees must verify and establish-

- the existence of the legal person or arrangement; and
- the identity of the principals of the legal person or arrangement.

These requirements can be achieved in a variety of ways depending upon the nature of the applicant - for example in relation to private companies, trusts, partnerships, and *société*:

Private companies

- Obtaining an original or appropriately certified copy of the certificate of incorporation or registration;

- Checking with the relevant companies registry that the company continues to exists;

- Obtaining details of the registered office and place of business;

- Verifying the identity of the principals of the company as above;

- Verifying that any person who purports to act on behalf of the company is so authorised, and identifying that person.

Trust

- Obtaining an original or appropriately certified copy of a trust deed or pertinent extracts thereof;
- Where the trust is registered - checking with the relevant registry to ensure that it does exist;
- Obtaining details of the registered office and place of business of the trustee;
- Verifying the identity of the principals of the trustee as above.

Partnerships

- Obtaining an original or certified copy of the partnership deed;
- Obtaining a copy of the latest report and accounts;
- Verification of the nature of the business of the partnership to ensure that it is legitimate;
- Verifying the identity of the significant partners as above;
- Verifying that any person that purports to act on behalf of the Partnership is so authorised, and identifying that person.

Sociétés

- Obtaining an original or certified copy of an *acte de société*;
- in the case of Mauritian *sociétés*, checking with the Registrar of Companies that the *société* continues to exist;
- in the case of foreign *sociétés* obtaining a certificate of good standing in relation to them;
- Verifying the identity of the principals, administrators or *gérants*;
- Verifying that any person that purports to act on behalf of the *société* is so authorised, and identifying that person.

4.2 *Appropriate certification*

Where a Licensee relies upon verification of identity documentation that are not in an original form, the documentation must be appropriately certified as true copies of the original documentation.

Where an employee of a Licensee meets an applicant for business or the principals thereof face-to-face and has access to original verification of identity documentation, he or she may take copies of the verification of identity documentation and certify them personally as true copies of the original documentation. In other cases, copies of the verification of identity documentation can be certified in accordance with the normal certification process of the jurisdiction where the applicant for business is based. Copies of the verification of identity documentation may, for example, be certified by one of the following:

- A lawyer, notary, actuary or an accountant holding a recognised professional qualification;
- A serving police or customs officer;
- A member of the judiciary;
- A senior civil servant;
- An employee of an embassy or consulate of the country of issue of identity documentation;
- A director or secretary (holding a recognised professional qualification) of a regulated financial services business in Mauritius or in an equivalent jurisdiction;
- A Commissioner of Oaths

4.3 *Reduced or simplified due diligence measures*

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 the national systems, it might be reasonable for Licensees to apply reduced or simplified due diligence measures when identifying and verifying the identity of the applicant for business.

Reduced or simplified CDD measures could be applied where applicants for business include-

- a regulated financial services business based in Mauritius or in an equivalent jurisdiction, provided that the Licensee is satisfied that the applicant for business is not acting on behalf of underlying principals[12]. Licensees must obtain and retain documentary evidence of the existence of the financial services business and of its regulated status[13].

- public companies listed on the Stock Exchange of Mauritius or on Recognised, Designated and Approved Stock/Investment Exchanges[14] or subsidiaries thereof. Licensees must obtain a copy of the annual report and accounts of such entities and must verify that the individuals that purport to act on behalf of such entities have the necessary authority to do so. Licensees must also obtain and retain documentary evidence of the existence of the public company and of its listed status.

- 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 scheme 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 Licensees must at a minimum identify and verify the identity of the employer and the trustees of the scheme (if any) as per the criteria set out in this Code.

Where Licensees determine that simplified or reduced CDD measures should apply to an applicant for business that does not fall within the examples above, Licensees should obtain FSC's prior approval[15] before applying such reduced or simplified measures.

4.4 Enhanced due diligence measures

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-

[13] Regulated for the purposes of this Code means that the entity must be licensed or registered and should be subject to the supervision of a public authority (empowered with either regulatory or criminal sanction) for AML/CFT purposes.

[14] A list of Recognised, Designated and Approved Stock/Investment Exchanges may be found at Appendix V

[15] In considering such applications, FSC will take into account the criteria established by Licensees for such risk determination and the extent to which Licensees are able to justify such criteria.

4.4.1 Politically Exposed Persons (PEPs)

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 and take appropriate measures to manage the increased risks of conducting business with PEPs.

4.4.2 Non-face-to-face business relationships

The FSC recognises that much of the business conducted by Licensees is conducted on a non-face to face basis with clients. Often, it is either impossible or impractical for Licensees to have or to obtain original primary or secondary documentary evidence of identity. Where this is the case, Licensees may rely upon copies that have been appropriately certified.

4.4.3 NCCTs and non-equivalent jurisdictions

When designing internal procedures, Licensees must have regard to the need for enhanced due diligence and additional monitoring procedures for transactions and business relationships involving NCCTs[16] and non-equivalent jurisdictions[17].

4.5 *Eligible and group introducers*

In recognition of the fact that a number of clients are introduced by intermediaries, Licensees find it necessary to place reliance upon eligible and group introducers in satisfying their obligation to undertake CDD measures.

Eligible introducers are persons or entities which refer business to Licensees and are regulated for money laundering purposes or/are subject to rules of professional conduct pertaining to money laundering. Eligible introducers must be either in Mauritius or in a jurisdiction that has in place anti-money laundering legislation that is at least equivalent to the legislation in Mauritius. Appendix II contains a list (which is subject to amendment) of such jurisdictions.

A group introducer is an entity that is part of the same group as the Licensee and is subject for money laundering purposes either to the consolidated supervision of a regulator in Mauritius or in an equivalent jurisdiction or is subject to the anti-money laundering regulation of a regulator in Mauritius or in an equivalent jurisdiction.

Licensees may rely on eligible or group introducers to perform the following CDD measures-

- Identifying and verifying the identity of the applicant for business using reliable, independent source documents, data or information;
- Identifying and verifying the beneficial owner 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.

[16] Licensees are reminded that the NCCT list is subject to amendment.

[17] Appendix II contains a list (which is subject to amendment) of equivalent jurisdictions, that is, jurisdictions having in place anti-money laundering legislation that is at least equivalent to the anti-money laundering legislation in Mauritius. Jurisdictions that do not appear on the list are considered by the FSC to be non-equivalent jurisdictions.

Whenever Licensees place reliance upon an eligible or group introducer, they should bear in mind that the ultimate responsibility to ensure that the CDD measures have been completed satisfactorily rests with the Licensee. Responsibility for undertaking CDD measures for applicants for business cannot be abdicated by Licensees to eligible or group introducers.

Licensees are entitled to rely on eligible/group introducers to perform their CDD obligations provided that the following criteria are met-

- Licensees must obtain evidence of a group or eligible introducer's status in the form of a completed Group Introducer Certificate (see specimen in Appendix III) or a completed Eligible Introducer Certificate (see specimen in Appendix IV). In addition, Licensees must satisfy themselves independently that the procedures followed by eligible and group introducers are sufficiently robust to ensure that the CDD measures are conducted in accordance with the requirements of this Code.

- Licensees and the eligible/group introducer must establish their respective responsibilities in writing. For these purposes, Licensees are required to establish clear procedures to determine an acceptable level of reliability on the eligible/group introducer.

- It is not necessary for Licensees to obtain copies of CDD documentation from the eligible/group introducer. Licensees should ensure that they have timely access to the CDD information maintained by the eligible/group introducer and that the CDD documentation will be made available from the eligible/group introducer **upon request without delay**.

- Licensees must ensure that their agreements with the eligible/group introducers include specific clauses relating to commitments that the eligible/group introducer will undertake all necessary CDD measures, will grant access to CDD information and will send copies of CDD documentation to the Licensee upon request without delay.

- Licensee's senior management or board of directors must conduct periodic independent testing of the arrangements by which Licensees may gain access to CDD information or obtain CDD documentation maintained by the eligible/group introducer to ensure that the arrangements work as designed.

- All copy documentation passed to Licensees by eligible or group introducers must be certified.

Licensees may rely upon existing CDD documentation in the possession of an eligible or group introducer provided that the information contained within the

documentation continues to be accurate at the time that it is relied upon by the Licensee.

Reliance may only be placed upon an eligible or group introducer in circumstances where an applicant for business is acting on its own behalf and not as a nominee or trustee on behalf of an undisclosed underlying principal.

The Licensee must undertake its own CDD measures if he has doubts about the introducer's ability to undertake appropriate CDD measures.

Paragraph 4.5 does not apply to outsourcing or agency relationships or relationships or transactions between the financial institutions for their clients.

4.6 *Omnibus Accounts*[18]

When establishing an omnibus account relationship with a regulated financial institution based in Mauritius or an equivalent jurisdiction, a Licensee should undertake CDD measures on the applicant for business, that is, the regulated financial institution, in the manner described in this Code.

In addition to identifying and verifying the applicant for business, the Licensee must:

- Gather sufficient information regarding the applicant for business (the financial institution) to understand its business and to determine from publicly available information its professional reputation;
- Assess the adequacy of the financial institution's CDD process;
- Ascertain whether the financial institution has a physical presence in the jurisdiction in which it is incorporated. The Licensee must neither establish nor maintain an omnibus account for a financial institution that has neither a physical presence in that jurisdiction nor is affiliated with a regulated financial group that has such a presence;
- Obtain approval of the Board of Directors before establishing new omnibus account relationships; and
- Document the respective responsibilities of each institution.

4.7 *Timing of verification of identity*

Licensees must take all reasonable measures to complete all CDD measures for all applicants for business prior to the establishment of a new client relationship and prior to providing any financial service. Where it is necessary to provide financial services to an applicant for business prior to completion of CDD measures, the decision to do so must be appropriately authorised by senior management and the reasons recorded in writing. The CDD measures must in

[18] "Omnibus accounts" has the same meaning as in the Financial Intelligence and Anti-Money Laundering Regulations 2003 (as amended).

any event be satisfactorily completed within thirty days of the establishment of the client relationship.

The Licensee must have precise procedures in place concerning the conditions under which a Licensee may act for an applicant for business before completion of the CDD measures. These procedures should (inter alia) limit the number and types of transactions that can be processed. The procedures should also include monitoring in general but monitoring large or complex transactions in particular during that period.

In the event that satisfactory CDD documentation has not been obtained, Licensees must have procedures in place to disengage from such relationships. Licensees should consider the potential risks inherent in engaging in any form of relationship with any applicant prior to satisfactorily completing CDD measures. Failure or inability to obtain satisfactory CDD documentation may in certain circumstances constitute a suspicion requiring a report to be made to the FIU.

5 Internal Controls and Handling of Suspicious Transactions

5.1 *Internal controls*

Licensees should have a system of internal controls to manage their AML/CFT risks and to provide a systematic and disciplined approach to assuring compliance with AML/CFT laws, codes and standards of good practice. AML/CFT risk management is most effective when a Licensee's culture emphasises high standards of ethical behaviour at all levels of the entity. The board of directors and senior management should promote an organisational culture which establishes through both actions and words the expectation of compliance by all employees with AML/CFT laws, codes, standards of good practice and internal policies and procedures when conducting the business of the Licensee.

The board of the Licensee should approve the Licensee's AML/CFT policy and must establish procedures and allocate responsibilities to ensure that AML/CFT policy and procedures are managed effectively and are in line with applicable laws, codes and standards of good practice.

5.2 *The appointment of a Money Laundering Reporting Officer*

Licensees must implement adequate internal reporting procedures to facilitate reporting of suspicious transactions by employees. Pursuant to Regulation 6(1) of the Financial Intelligence and Anti-Money Laundering Regulations 2003 Licensees must appoint a Money Laundering Reporting Officer ('MLRO') to whom all internal reports of suspicious transactions must be made. The MLRO must be a senior manager or a director of the Licensee with the relevant experience, competence, authority and independence to be able to discharge the reporting obligation effectively and autonomously. Licensees must advise the FSC of the identity of the MLRO within one month of that person assuming his/her responsibilities.

Where an employee makes a suspicious transaction report to an MLRO in accordance with a Licensee's internal procedures he/she will have discharged their legal obligation to report (pursuant to section 14 of the FIAML Act). Thereafter, the Licensee has a legal obligation to ensure that the employee's report is properly evaluated by the MLRO and where necessary a report should then be made to the FIU. In the event that the MLRO validates an internal suspicious transaction report, he/she has responsibility for ensuring that a report is made to the FIU. Where an MLRO fails to report a suspicion to the FIU

following an evaluation and validation of an internal report, the Licensee concerned may be liable.

Internal suspicious transaction reports must be made to the MLRO in writing. A sample internal report form is provided in Appendix I.

All internal reports by employees should be considered by the MLRO. It is not permissible for line managers or others within an organisation to prevent an internal report being made to, or considered by, the MLRO.

Adequate procedures should be implemented by Licensees to ensure that MLROs have access to all relevant business information and CDD documentation in order to properly evaluate internal suspicious transaction reports. MLROs must have autonomy in deciding whether suspicious transaction reports should be passed on to the FIU. MLROs may consult with colleagues as part of the evaluation process. However, the MLRO must be free to make his or her decision and without undue influence, pressure or fear of repercussions in the event that senior colleagues disagree with his/her decision.

A number of examples have shown that in addition to the accuracy of the detail of suspicious transaction reports, speed is also important in dealing with money laundering schemes and other types of financial crime. All Licensees should therefore take appropriate measures to ensure that the proper internal suspicious transaction reporting systems continue to function properly in the absence of the MLRO. It is for this reason that FSC requires the appointment of Deputy MLROs. The Licensee must advise the FSC of the identity of the Deputy MLRO within one month of his/her appointment.

It is imperative that all employees are made aware of the identity of the MLRO and Deputy MLRO. Licensees must ensure that employees know how to make suspicious transaction reports and when and why.

5.3 *Compliance monitoring*

The MLRO shall be responsible for implementing and monitoring the day-to-day operation of the Licensee's AML/CFT policy and procedures. The MLRO shall report to the board of directors of the Licensee or a committee of the board on any material breaches of the internal AML/CFT policy and procedures and of the AML/CFT laws, codes and standards of good practice.

The MLRO shall make annual reports and such other periodic reports as he/she deems necessary to the board of the Licensee or a committee of the board on the adequacy/shortcomings of internal controls and other procedures implemented to combat money laundering and financing of terrorism, the number of internal reports made by staff and the number of reports made to the

FIU. The report shall recommend any necessary action to remedy deficiencies identified by the MLRO.

The board of the Licensee must take all necessary action to remedy deficiencies identified by the MLRO in the report.

5.4 *Recognising suspicious transactions*

The FIAML Act 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.

This definition is not exhaustive. Licensees are reminded that the offence of money laundering can be committed in any circumstances where a person had reasonable grounds to suspect a transaction, even though he/she did not actually suspect it.

The number of possible examples of suspicious transactions precludes the FSC from replicating them all within this Code, although a list of indicators of potentially suspicious activity is provided in Appendix VI. FSC recommends that Licensees refer to the Egmont Group of Financial Intelligence Unit's

publication entitled "FIUs in Action – 100 Cases from the Egmont Group". This publication will provide examples and guidance to employees on suspicious activity. Licensees may also refer to the FATF Reports on Money Laundering Typologies.

Evidence of potential money laundering activity often occurs in the form of unusual or unexpected patterns of transactional activity. Adherence to satisfactory CDD measures provides the foundation for the recognition of such activity. In addition to helping Licensees to identify and manage the risks inherent in certain client relationships, adequate CDD measures enable Licensees to know enough about clients to be able to recognise unusual or unexpected activity as or before it occurs.

5.5 *CDD and risk profiling*

The need for Licensees to know their clients is essential to the prevention of money laundering and combating terrorist financing. CDD is the foundation upon which all internal anti-money laundering systems must be built. The concept of CDD extends beyond the identification and verification of the client- it includes the identification of the potential risks of a business relationship. In addition to the criminal risk of money laundering, such risks, for example, include the following:

- Reputational risk
- Legal risk
- Credit risk
- Fiduciary risk
- Regulatory risk
- Operational risk[20]

The extent to which a relationship will expose a Licensee to such risks will in turn depend upon numerous factors including the following:

- The identity of the client
- The occupation of the client[21]

[20] Further information on the role that effective CDD procedures can play in protecting organizations from risks is provided in the Basel Committee on Banking Supervision document ' Customer Due Diligence for Banks' – October 2001

[21] Details of the occupation of the principals must be obtained and recorded by Licensees.

- 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

Licensees must routinely consider the risks that all relationships pose to them and the manner in which those risks can be limited. To do so, Licensees must be able to demonstrate the effective use of documented CDD information. If a Licensee does not 'know a client' it will not be in a position to recognise and manage the risks inherent in the relationship.

5.6 *Source of funds/property*

Understanding the origin or provenance of property that forms part of any arrangement both at the outset of a client relationship and for its duration, is a necessary pre-requisite to identifying risk and preventing money laundering. Licensees must therefore take appropriate measures to obtain information about the source of property. Where the information received is consistent with the information that the Licensee already holds in relation to an applicant, and where the information provided does not indicate any abnormal or potentially suspicious activity within the context of the product or service being provided, there will be no requirement for the Licensee to verify the information supplied.

Questions that might be asked when determining whether incoming property or funds may be suspicious include the following:

- Is the volume and /or size of the transactions and/or value of the property consistent with the normal pattern of activity for the customer?

- Is the receipt of the property or transaction in the context of the customer's business or personal activities and their stated commercial objectives?

Where the type of product or service being offered makes it appropriate to do so, a Licensee should also consider obtaining information regarding an applicant's source of wealth.

5.7 *Suspicious activity*

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 FIAML Act 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.

5.8 *Complex arrangements*

The FSC is concerned to ensure that money launderers and terrorist financiers do not achieve their criminal objectives by deliberately concealing criminally derived property within complex arrangements or structures. Therefore Licensees must scrutinise all complex, unusual large transactions and all unusual patterns of transactions - especially those which have no apparent economic or visible lawful purpose. Licensees must pay close attention to any transactions which appear to be linked. The background and purpose of such transactions should, as far as possible, be examined and the findings recorded in writing.

5.9 *Constructive trusts*

Suspicion of certain types of criminal conduct on the part of clients can in certain circumstances render Licensees as constructive trustees. This situation may arise by operation of law when a Licensee knows or is on notice that the property that it handles on behalf of its client may in fact belong to identified or unidentified third parties, for example the victims of a fraud.

Where a Licensee is placed in the position of a constructive trustee it must be aware of the risk that it faces of breaching its fiduciary duties in the event that it dissipates the property or deals with it in a manner that is detrimental to the interests of a constructive beneficiary.

The duty to report suspicious transactions and to avoid committing the offence of 'tipping off' can occasionally lead to a conflict, particularly when a reported client requests information as to why his/her instructions have not been followed. On the one hand, the Licensee may not want to follow the client's instructions for fear of breaching its duties as a constructive trustee but on the other hand, it will not want to 'tip off' the client who may deduce that the reason for the inaction is that he is under suspicion.

Where a Licensee suspects criminality and is on notice that property may belong to a third party, the Licensee should include this information in the report that it makes to the FIU. If the Licensee is subsequently asked by a suspected client to give a reason for its inaction, it should refer to the FIU. The FIU may be able to offer guidance on how to avoid tipping off.

The FSC is of the opinion that the adoption of effective CDD measures will mitigate the risk of Licensees becoming involved in relationships that may give rise to constructive trust scenarios.

5.10 *Reporting suspicions to the FIU*

As stated in paragraph 5.2 above, employees of Licensees will discharge their legal obligations under the FIAML Act by disclosing their suspicions to the MLRO in accordance with the Licensee's internal procedures. Where the MLRO validates an internal suspicious transaction report, he or she must report it and the circumstances surrounding it as soon as possible to the FIU by utilising the form prescribed by the FIU.

The contact details of the FIU are as follows:

The Director
Financial Intelligence Unit
3rd Floor, Travel House

Corner Sir William Newton & Royal Streets
Port Louis
Tel: 213 1423-26
Fax: 213 1431
Email: contact@fiumauritius.org

In urgent cases disclosures may be made by telephone.

Once a suspicious transaction report is made, Licensees must take appropriate measures to ensure that the offence of tipping off is not committed.

Licensees must also ensure that any disclosure is made in good faith. An absence of good faith on the part of a Licensee (who for example makes a report maliciously and without reasonable grounds for doing so), renders the Licensee liable to be sued for breach of client confidentiality. Where a disclosure is made in good faith but proves to be groundless, the person disclosing may claim immunity from both civil and criminal action.

5.11 *Recording suspicious transaction reports*

Licensees must maintain a register of internal suspicious transaction reports received by the MLRO and of all reports made by the MLRO to the FIU. Where the MLRO has not deemed it appropriate to report a transaction reported by an employee, he or she should document the reasons for not submitting it to the FIU. The FSC will routinely inspect suspicious transaction report registers during the course of compliance visits.

6 Training and culture

Licensees must implement appropriate and on-going AML/CFT training for staff in general and for the MLRO in particular.

6.1 *Training*

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 FIAML Act.

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

6.2 *New employees*

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.

6.3 *Annual training*

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

6.4 *MLRO training*

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.

6.5 *Training methods*

The FSC does not wish to be prescriptive about the methods of training employed by Licensees - provided the method employed is effective in raising and maintaining the level of awareness of employees- but attending seminars does not per se constitute effective training.

6.6 *Training records*

Licensees must maintain records of all AML/CFT training delivered to employees. In the absence of evidence of sufficient training an employee may claim that their suspicion was not aroused (when it ought to have been) because (s)he had never been trained to be suspicious in such circumstances.

6.7 *Culture*

The FSC believes that internal procedures and staff training must be supported by an effective internal compliance culture. Cultural barriers commonly prevent organisations from taking appropriate measures in relationships involving criminally derived property. An inadequate compliance culture can manifest itself in a number of ways, for example:

- The attitude amongst junior employees that their suspicions and concerns are of no consequence. This is particularly dangerous as junior employees are in fact often exposed to the day to day transactional activity
- Failure to adequately and legibly document CDD information on file
- Management pressure to transact
- Over zealousness in the attraction of new business relationships
- Unwillingness to subject important clients to the same degree of vigilance.

Licensees must take appropriate measures to prevent these and other barriers from occurring. Licensees must encourage and support all members of staff to be vigilant and sensitive to any appearance of wrong-doing.

7 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.

7.1 *Records of suspicious transaction reports*

As outlined in paragraph 5.11 of this Code, 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. (See FSD Act section 14(4)).

7.2 *Transactional records*

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

7.3 *Identity records*

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.

7.4 *Training records*

As stated in paragraph 6.6, 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.

7.5 *Form of records*

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.

Appendices

Appendix I	–	Sample Internal Disclosure Form to MLRO
Appendix II	-	List of Equivalent Jurisdictions
Appendix III	-	Specimen Group Introducer Certificate
Appendix IV	-	Specimen Eligible Introducer Certificate
Appendix V	-	List of Recognised, Designated and Approved Stock/Investment Exchanges
Appendix VI	-	Indicators of Potentially Suspicious Activity
Appendix VII		Note on the Money Laundering Reporting Officer
Appendix VIII		Glossary
Appendix IX		Useful Websites

Appendix I

Sample Internal Disclosure Form to MLRO

1. Reporting Employee

Name :_____

Telephone No :_____

2. Client

Client Name :_____

Address :_____

Contact Name :_____

Contact Telephone No :_____

Date Client Relationship Commenced _____

Client reference :_____

3. Information/Suspicion

Suspected Information/ Transaction :_____

Reasons for Suspicion: _____

_____

_____

_____

_____

Please attach copies of any relevant documentation to this report.

Reporter's Signature :_____ Date: _____

It is an offence to advise the customer/client or anyone else of your suspicion and report.

This report will be treated in the strictest confidence.

MLRO Use:

Date received: ……Time received: …….. Ref:…….

FIU advised: Yes/No…..Date: …….. Ref:…….

Appendix II

List of Equivalent Jurisdictions

1. Australia
2. Austria
3. Bahamas
4. Bermuda
5. Belgium
6. Canada
7. Cayman Islands
8. Denmark
9. Finland
10. France
11. Germany
12. Gibraltar
13. Greece
14. Guernsey
15. Hong Kong
16. Iceland
17. Ireland
18. Isle of Man
19. Italy
20. Japan
21. Jersey
22. Luxembourg
23. Malta
24. Netherlands (excluding Netherlands Antilles)
25. New Zealand
26. Norway
27. Portugal
28. Republic of South Africa
29. Russian Federation
30. Singapore
31. Spain
32. Sweden
33. Switzerland
34. United Kingdom
35. United States

The criteria used by the FSC to determine whether a jurisdiction has equivalent anti-money laundering legislation in place includes the following:

- FATF Membership
- EU Membership
- Information available to the FSC about the AML/CFT laws of certain EU and FATF jurisdictions that are excluded from the list

- Information available to the FSC about the AML/CFT laws of certain non EU and FATF jurisdictions that appear on the list and are deemed by the FSC to have equivalent legislation in place.

Appendix III

Specimen Group Introducer Certificate

Date **……..**

Name of Applicant:……..…….

Address of Applicant: ……
(*including postcode)*
……

The above named is a *customer* of […….] located in [...……...] and a member of the [……] group of companies (the "Group"), subject to the consolidated supervision of […….……] located in [……..]

The *customer* wishes to establish a relationship with [……] in Mauritius

I/*we* hereby certify the following in respect of this *Applicant:*

1. The *Applicant* has been known to us for …… years, and all necessary Customer Due Diligence measures as required by Group standards and by local law for the purpose of combating money laundering and the financing of terrorism have been satisfactorily undertaken and completed.

2. There is sufficient information on file at the above group company to establish the ownership and control structure of the *Applicant* (if a corporate entity) or the *Applicant's* identity (if a natural person).

3. Original or certified copies of Customer Due Diligence documentation will be made available to [Name of Licensee in Mauritius] **upon request without delay**.

4 *I/we am/are* unaware of any activities of the Applicant that causes me/us to suspect that the *Applicant* is engaged in money laundering, terrorist financing or any other form of criminal conduct. Should *I/we* subsequently become so suspicious, *I/we* shall inform you immediately.

5. *I/we* undertake to advise the Group Company in Mauritius should *I/we* become aware of any material alteration in or adverse change in *my/our* opinion of the standing integrity or reputation of the above *Applicant*.

Signed: ……. Name:……...……

Position: ……. Group Company:……..

Appendix IV

Specimen Eligible Introducer Certificate

Name of Applicant: ……..

Address of Applicant: ……..
(*including postcode)*

……

I/We certify that in accordance with the provisions of the Financial Intelligence and Anti Money Laundering Act 2002 and the FSC's Code on the Prevention of Money Laundering and Terrorist Financing as amended from time to time, *or equivalent legislation:*

1 I/We have undertaken and completed Customer Due Diligence measures for the Applicant and confirm that I/we have in our possession sufficient information to establish the *ownership and control structure of the Applicant* (if a corporate entity) or the *Applicant's identity* (if a natural person).

2 Original or certified copies of Customer Due Diligence documentation will be made available to [Name of Licensee in Mauritius] **upon request without delay**.

AND

3 The Applicant(s) is/are applying on his/her own behalf and not as nominee, trustee or in a fiduciary capacity for any other person.

4 I/We am/are unaware of any activities of the Applicant that cause me/us to suspect either that the applicant is engaged in money laundering or any other form of criminal conduct.

Full Name of Regulated Introducer: …….

Name of Regulator: ……Country of Regulator: ……..….

Licence or Registration No: ……..

Signed: …….. Full Names: ……

Job Title: …….. Date: ……...

Appendix V

Recognised, Designated and Approved Stock/Investment Exchanges

1. Recognised Investment Exchanges

a) Recognised UK Investment Exchanges

London Stock Exchange (LSE)
London International Financial Futures & Options Exchange (LIFFE)
International Petroleum Exchange of London (IPE)
London Commodity Exchange (LCE)
London Metal Exchange (LME)
London Securities and Derivatives Exchange (OMLX)
Trade point Financial Networks PIc

b) Recognised Overseas Investment Exchanges

The National Association of Securities Dealers Incorporated (NASDAQ)
Sydney Futures Exchange Ltd (SFE)
Chicago Mercantile Exchange (GLOBEX)
Chicago Board of Trade (GLOBEX)
New York Mercantile Exchange (NYMEX).

c) The Channel Islands Stock Exchange

2. **Designated Investment Exchanges (DIEs) American Stock Exchange**

American Stock Exchange
Amsterdam Pork & Potato Terminal Market Clearing House (NLKKAS)
Amsterdam Futures
Australian Futures
Bolsa Mexicana de Valores
Chicago Board Options Exchange Chicago Mercantile Exchange
Coffee, Sugar and Cocoa Exchange, Inc
Commodity Exchange Inc
Copenhagen Stock Exchange (inc. FUTOP)
DTB Deutsche Terminborse
European Opinions Exchange
Finaciele Termijnmarkt, Amsterdam
Finnish Options Market
Hong Kong Futures Exchange
Hong Kong Stock Exchange
International Securities Market Association
Irish Futures and Options Exchange (IFOX)
Johannesburg Stock Exchange
Kansas City Board of Trade
Korea Stock Exchange

Marché des Options Négociables de Paris (MONEP)
Marché à Terme International de France
MEFF Renta Fija
MEFF Renta Variable
Midway Commodity Exchange
Mid America Commodity Exchange
Midwest Stock Exchange
Minneapolis Grain Exchange
Montreal Stock Exchange
New York Cotton Exchange (including Citrus Associates of the New York Cotton Exchange)
New York Futures Exchange
New York Mercantile Exchange
New York Stock Exchange
New Zealand Futures Exchange
New Zealand Stock Exchange OM Stockholm AB
Osaka Stock Exchange
Pacific Stock Exchange
Paris Stock Exchange
Philadelphia Board of Trade
Philadelphia Stock Exchange
Singapore International Monetary Exchange (SIMEX)
Singapore Stock Exchange
South African Futures Exchange (SAFEX)
Swiss Options and Financial Futures Exchange
Sydney Futures Exchange
Tokyo International Financial Futures Exchange (TIFFE)
Tokyo Stock Exchange
Toronto Futures Exchange
Vancouver Stock Exchange

3. **Approved Exchanges**

Amsterdam Stock Exchange
(Amsterdamse Effectenbeurs)
Antwerp Stock Exchange (Effectenbeurs vennootschap van Antwerpen)
Associacion de Intermediaros de Activos Financieros (Spanish Bond Market)
Athens Stock Exchange (ASE)
Barcelona Stock Exchange (Bolsa de Valores de Barcelona)
Basle Stock Exchange (Basler de Valores de Barcelona)
Belgium Futures & Options Exchange (BELFOX)
Berlin Stock Exchange (Berliner Borse)
Bergen Stock Exchange (Bergen Bors)
Bilbao Stock Exchange (Borsa de Valores de Bilbao)

Bologna Stock Exchange (Borsa Valori de Bologna)
Bolsa de Mercadorios & Futures (BM & F)
Bordeaux Stock Exchange (Bourse de Bordeaux)
Boston Stock Exchange
Bovespa (Sao Paulo Stock Exchange)
Bremen Stock Exchange (Bremener Wertpapierborse)
Brussels, Stock Exchange (Société de la Bourse des Valeurs MobilieresjEffecten Beursvennootschap van Brussels)
BVRJ (Rio de Janeiro Stock Exchange)
Cincinnati Stock Exchange
Copenhagen Stock Exchange (Kobenhavns Fondsbors)
Dusseldorf Stock Exchange (Rheinisch - Westfalische Borse zu Dusseldorf)
Florence Stock Exchange (Borsa Valori di Firenze)
Frankfurt Stock Exchange (Frankfurter Wertpapierborse)
Fukuoka Stock Exchange
Geneva Stock Exchange
Genoa Stock Exchange (Borsa Valori di Genoa)
Hamburg Stock Exchange (Hanseatische Vertpapier Borse Hamburg)
Hannover SE (Niedersachsische Borse zu Hannover)
Helsinki Stock Exchange (Helsingen Arvopaperiporssi Osuuskunta)
Kuala Lumpur Stock Exchange
Lille Stock Exchange
Lisbon Stock Exchange (Borsa de Valores de Lisboa)
Luxembourg Stock Exchange (Société de la Bourse de Luxembourg SA)
Lyons Stock Exchange
Madrid Stock Exchange (Borsa de Valores de Madrid)
Marseilles Stock Exchange
Mercato Italiano Futures (MIF)
Mid West Stock Exchange
Milan Stock Exchange (Borsa Valores de Milano)
Munich Stock Exchange (Bayerische Borse in Munchen)
Nagoa Stock Exchange
Nancy Stock Exchange (Bourse de Nancy)
Nantes Stock Exchange (Bourse de Nantes)
Naples Stock Exchange (Borsa Valori di Napoli)
New Zealand Stock Exchange
Oporto Stock Exchange (Bolsa de Valores do Porto)
Oslo Stock Exchange (Oslo Bors)
Palermo Stock Exchange (Borsa Valori di Palenno)
Rome Stock Exchange (Borsa Valori di Roma)
Stockholm Stock Exchange (Stockholm Fondbors)
Stuttgart Stock Exchange (Baden - Wurtembergische Wertpapierborse zu Stuttgart)
Taiwan Stock Exchange
Tel Aviv Stock Exchange

The Stock Exchange of Thailand
Trieste Stock Exchange (Borsa Valori di Trieste)
Trondheim Stock Exchange (Trondheims Bors)
Turin Stock Exchange (Borsa Valori de Torino)
Valencia Stock Exchange (Borsa de Valores de Valencia)
Venice Stock Exchange (Borsa Valori de Venezia)
Vienna Stock Exchange
Zurich Stock Exchange (Zurcher Borse)

4. **EFA Regulated Markets under Article 16 of the Investment Services Directive (93/22/EEC)**
(Note some listed below may also be included in the lists of DIEs or Approved Exchanges)

Austria
Vienna Stock Exchange
(Wiener WertpapieIborse)
Austrian Financial Futures and Options Exchange (Vienna)
(Osterreichische Termin-und Optionenborse Aktiengeselleschaft)

Belgium
De eerste en tweede markt van de effectenbeurs van Brussel/Le premier et Ie second marché et Ie nouveau marché de Ia bourse de valeurs mobilières de Bruxelles [Bourse de Bruxelles]
De Belgium future-en optiebeurs, afgekort Belfox/La bourse beige des futures et options, en abrégé Belfox.
De secondaire buiten-beursmarkt van de lineaire obligaties, der gesplitste effecten en de scharkistcertificaten/Le marche secondaire hors bourse des obligations linéaires, des titres scindés et des certificats de trésorerie.
EASDAQ

Denmark
The Copenhagen Stock Exchange (Kobenhavs Fondbors)

Finland
Hex Ltd Helsinki Securities and Derivatives Exchange, Clearing House

France

Le Matif
Le premier marché et Ie second marché de la bourse de Paris
Le nouveau marché
Le Monep

Germany
Berliner Wertpapierborse (Amtlicher Handel, Geregelter Markt) (Berlin Stock Exchange)

Wertpapierborse in Brenme (Amtlicher Handel, Geregelter Markt) (Bremen Stock Exchange Dusseldorf)
Rheinisch - Westfalische Borse zu Dusseldorf (Amtlicher Handel, Geregelter Markt) (Rhine - Westphalian Stock Exchange Dusseldorf)
Frankfurter Wertpapiernborse (Amtlicher Handel, Geregelter Markt) (Frankfurt Stock Exchange)
Deutsche Terminborse (DTB)
Hanseatische Wertpapierborse Hamberg (Amtlicher Handel, Geregelter Markt) (Hanseatic Stock Exchange Hamburg)
Niedersachsische Borse (Amtlicher Handel, Geregelter Markt) (Amstock Exchange of Lower Saxony (Hanover)) Bayerische Borse (Amtlicher Handel, Geregelter Markt) (Bavarian Stock Exchange (Munich))
Baden - Wurttembergische Wertpapierborse (Amtlicher Handel, Geregelter Markt) (Baden - Wurttemberg Stock Exchange (Stuttgart))
Neuer Markt

Greece
Athens Stock Exchange
Thessaloniki Stock Exchange Centes (TSEC)

Iceland
Iceland Stock Exchange (Verdbrefathing Islands) .

Ireland
Ireland Stock Exchange

Italy
Borsa Italiana SpA (Italian Stock Exchange, Milan)
Mercato ristretto
Mercato di borsa per la negoziazione degli strumenti previsti dall'articolo 1, cooma 1,lettere (f) e (i), del d.lgs. n.415/1996 (IDEM)
Mercato all'ingresso dei titoli di Stato di cui al decreto del Ministro del Tesoro 24 febbraio 1994 (MTS)
Mercato dei contratti uniformi a termine sui titoli di Stato di cui al decreta del Ministro del Tesoro 24 febbraio 1994 (MIF).

Luxembourg
Luxembourg Stock Exchange (Société de la Bourse de Luxembourg SA)

The Netherlands
Amsterdam Exchanges (Amsterdamse effectenbeurs)
EOE-optiebeurs

Norway
The Oslo Stock Exchange

Portugal
Mercado de Cotacoes Oficiais da Bolsa de Valores de Usboa (Market with Official Quotations of the Bolsa de Valores de Lisboa)
Segundo Mercado da Bolsa de Valores de Lisboa (Second Market of the Bolsa de Valores de Lisboa)
Mercato sem Cotacoes da Bolsa de Valores de lisboa (Market without Quotations of the Bolsa de Valores de Lisboa)
Bolsa de Derivados do Porto

Spain
La Bolsa de Valores de Barcelona
La Bolsa de Valores de Bilbao
La Bolsa de Valores de Madrid
La Bolsa de Valores de Valencia
Los mercados oficiales de futuros y opciones de Meff Sociedad Rectora del Mercado de Productos Financieros Derivados de Renta Fija, SA y Meff Sociedad Rectora del Mercado de Productos Financieros Derivados de Renta Variable, SA
AlAF, Mercado de Renta Fija, SA
Mercado de Deuda Publica en Anotaciones

Sweden
Stockholm Stock Exchange (Stockholm Fondbors AB)
Penningmarknadsinformation PmI AB
OM Stockholm AB

United Kingdom
The following four of the markets comprising the London Stock Exchange Limited: .

- The Domestic Equity Market
- The European Equity Market
- The Gilt-Edged and Sterling Bond Market
- The Alternative Investment Market

The London International Financial Futures and Options Exchange ('LIFFE')
OMLX, The London Securities & Derivatives Exchange Limited
Tradepoint Stock Exchange

Appendix VI

Indicators of Potentially Suspicious Activity

This list of indicators is by no means an exhaustive list of indicators of suspicious activity.

1. Any activity that casts doubt over the true identity of an applicant for business or the principals thereof

2. Any relationship or arrangement that appears not to have a clear commercial justification or rationale

3. Any unusual or unexplained transaction in the context of the normal pattern of activity for a particular relationship

4. Reluctance on the part of clients to respond to enquiries made by Licensees

5. Unusually linked transactions

6. Fund transfers to or from accounts in FATF NCCTs or countries that are known to be associated with drug trafficking or other serious crime

7. Any activity that appears to be inconsistent with the CDD information and profile of a particular client e.g. the client's apparent standing and means.

8. Clients who produce or demand for collection large quantities of cash

9. The request for use of intermediary client accounts as bank accounts

10. The settlement of transactions utilising cash or bearer instruments

11. Churning

12. Early redemption of single premium insurance products

Appendix VII

Note on The Money Laundering Reporting Officer

A *Appointment of the Money Laundering Reporting Officer*

- All Licensees must appoint a Money Laundering Reporting Officer ('MLRO').
- All Licensees should take appropriate measures to ensure the proper functioning of internal suspicious transaction reporting systems in the absence of the MLRO, by the appointment of a Deputy MLRO.

B *Profile of the Money Laundering Reporting Officer*

- The MLRO must be a senior manager or a director of the Licensee with relevant experience, competence, authority and independence to be able to discharge the reporting obligation effectively and autonomously.

C *Notification of the Appointment of the Money Laundering Reporting Officer*

- Licensees must advise the FSC of the identity of the MLRO within one month of that person assuming responsibility.
- Licensees must advise the FSC of the identity of the Deputy MLRO within one month of the appointment being made.

D *Suspicious Transactions Reporting*

- All employees must be made aware of the identity of the MLRO and Deputy MLRO and the manner in which employees are expected to make the MLRO aware of transactions about which they are suspicious.
- Within a Licensee, all reports concerning transactions about which staff are suspicious should be addressed to the MLRO and must be in writing.
- The Licensee has a legal obligation to ensure that a report submitted to a MLRO by an employee about a transaction which the employee considers to be suspicious is properly evaluated by the MLRO.
- A Licensee's Procedures Manual should show that it is not permissible for line managers or others within a licence holding company to prevent an internal report being made to or being considered by an MLRO.
- Adequate procedures should be implemented by Licensees to ensure that MLROs have reasonable access to all relevant information in order to properly evaluate internal reports that have aroused suspicion.

E ***Filing of STRs - Decision Making Process***

- MLROs must be autonomous in their decisions as to whether a suspicious transaction report should be made to the Financial Intelligence Unit ('FIU').

- MLROs may consult with colleagues as part of the evaluation process, the MLRO must be free to make his or her decision and without undue influence, pressure or fear of repercussions in the event that senior colleagues disagree with his/her decision.

- Where a MLRO validates an internal report about a transaction that has aroused suspicion, he/she has a legal obligation to make a report to the FIU.

F ***Compliance Monitoring***

- The MLRO shall be responsible for implementing and monitoring the day-to-day operation of the AML/CFT policy and procedures.

- The MLRO shall report to the Board of Directors or a committee of the Board on any material breaches of the internal AML/CFT policy and procedures and of the AML/CFT laws, codes and standards of good practice.

- The MLRO shall make annual reports and such other periodic reports as he/she deems necessary to the Board of the Licensee or a committee of the Board on the adequacy/shortcomings of internal controls and other AML/CFT procedures implemented, the number of internal reports made by staff and the number of reports made to the FIU.

- The report of the MLRO shall also recommend any necessary action to remedy deficiencies identified by the MLRO.

Appendix VIII

Glossary

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
Applicant for business	includes any natural person or legal person or arrangement-corporate or unincorporated that seeks to form a business relationship or to carry out a one-off transaction with a Licensee.
Beneficial owner	the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
Business relationship	an arrangement between an applicant for business and a licensee where the purpose or effect of the arrangement is to facilitate the carrying out of transactions between the applicant for business and the licensee on a frequent, habitual or regular basis
Controlling shareholder	Any person who is entitled to exercise, or control the exercise of, 20 percent or more of the voting power at general meetings of the company or one which is in a position to control the appointment and/or removal of directors holding a majority of voting rights at board meetings on all or substantially all matters.
Equivalent jurisdiction	A jurisdiction which has in place anti-money laundering legislation that is at least equivalent to the anti-money laundering legislation in Mauritius. See appendix II.
FATF	Financial Action Task Force
FIAML Act	Financial Intelligence and Anti-Money Laundering Act 2002
FIU	Financial Intelligence Unit
FSC	Financial Services Commission
FSD Act	Financial Services Development Act 2001

Licensee	a management company or a corporate trustee holding a Management Licence issued by the FSC under section 24(2) of the FSD Act.
Omnibus account	an account which is held with a Licensee in the name of a financial institution, or a bank, which is regulated under the FIAML Act or the Regulations, or any similar legislation in an equivalent jurisdiction and – (a) the assets of the customers of the financial institution or the bank are held in aggregate in such account; or (b) such account is held on behalf of pooled entities, including collective investment schemes, pension funds and such other bodies, plans or schemes as the Minister may designate.
One –off transaction	any transaction carried out other than in the course of a business relationship
Regulations	Financial Intelligence and Anti-Money Laundering Regulations 2003
Significant partner	any partner owning or controlling 20 percent or more of a partnership

Appendix IX

Useful Websites

Bank for International Settlements	www.bis.org
FATF	www.fatf-gafi.org
FIU	www.fiumauritius.org
FSC	www.fscmauritius.org
IAIS	www.iaisweb.org
IOSCO	www.iosco.org
Transparency International Corruption Perceptions Index	www.transparency.org
Wolfsberg Group	www.wolfsberg-principles.com