CODE ON THE PREVENTION

of

MONEY LAUNDERING

&

TERRORIST FINANCING

(Issued under Section 7(1)(a) of the Financial Services Act 2007 and Section 18(1)(a) of the Financial Intelligence and Anti-Money Laundering Act 2002)

March 2012
[Updated as at 25 May 2017]

The Code on the Prevention of Money Laundering and Terrorist Financing was approved by the Board of the FSC on 29 March 2012.

The Code was issued on 30 March 2012 and comes into force on 1 April 2012.

CHAPTER 1 – INTRODUCTION

Sections in this Chapter:

1.1 Background and Scope

The success of Mauritius as a centre for financial services depends inter alia upon the maintenance of its reputation of probity. It is therefore vital that all financial institutions[1] in Mauritius exercise appropriate care and diligence to ensure that neither it nor any services offered by it are used by anyone who is a criminal or whose intentions are to launder the proceeds of crime or to engage in terrorist financing.

The Financial Services Commission ('FSC') has the mandate to establish norms and standards in order to preserve and maintain the good repute of Mauritius in the financial services sector and inter alia ensure that the financial services sector in general, and its Licensees[2] in particular, are not used for money laundering and terrorist financing purposes. Pursuant to section 18(1)(c) of the Financial Intelligence and Anti-Money Laundering Act 2002 ('FIAML Act'), the FSC has a statutory duty to supervise and enforce compliance by its Licensees in respect of the requirements imposed under the FIAML Act and Regulations or guidelines which are made under the FIAML Act.

The FSC first issued its Codes on the Prevention of Money Laundering and Terrorist Financing in April 2003, which were consistent with the revised FATF 40 Recommendations and Eight Special Recommendations on Terrorist Financing and national AML/CFT strategies. Following a number of developments on both national and international fronts, the Codes of April 2003 was subsequently revised in July 2005.

The legislative framework has been set by the FIAML Act, followed by the Financial Intelligence and Anti-Money Laundering Regulations 2003 ('FIAML Regulations') which came into operation in June 2003. The FIAML Act has been amended over the years to ensure compliance with international standards.

Since September 2007, the FSC is governed by the Financial Services Act 2007 ('FS Act'). Together with the Insurance Act 2005 and the Securities Act 2005 (both of which came into operation in September 2007), the FS Act has brought about a streamlined and consolidated regime for financial services and a new conceptual approach to the global business sector.

[1] The term "financial institution" is defined under section 2 of the FIAML Act. [2] The term "Licensee" is defined in Appendix IX – Glossary.

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.

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 regulators and jurisdictions.

On the international front, the FATF completed the revision of the Forty Recommendations, resulting in a more comprehensive framework for combating money laundering and terrorist financing. For instance, in February 2007, the FATF adopted the revised AML/CFT Methodology 2004.

In 2007, Mauritius underwent a second Financial Sector Assessment Program (FSAP) of its AML/CFT regime using the AML/CFT assessment methodology 2004, as updated in February 2007, to assess Mauritius's level of compliance with the FATF 40+9 recommendations.

Further to the changes on both local and international fronts and with a view to adopting the recommendations made in the FSAP report 2007, the FSC initiated a review of the Codes. A major step in this review was to harmonise the requirements of the three Codes issued and come up with a single comprehensive Code on AML/CFT for all Licensees, with specific sectoral guidance as necessary. This approach is in line with the consolidated licensing and supervisory framework put in place by the FS Act.

Mauritius fully supports international initiatives to prevent money laundering and to combat terrorist financing. The present Code takes account of all relevant international standards, FSAP Recommendations and national commitments which include –

- the Financial Action Task Force's (FATF) Revised Forty Recommendations and the FATF's Nine Special Recommendations on Terrorist Financing[2];
- 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;
- IAIS' Anti-Money Laundering Guidance Notes for Insurance Supervisors and
- Insurance Entities;
- the recommendations made by IMF/World Bank Assessors in FSAP 2007 on how certain aspects of the system could be strengthened, using AML/CFT Methodologies of 2004;
- balancing the regulatory burden with the effectiveness of the requirements;

[2] In February 2012, the FATF has issued the revised Forty Recommendations, i.e. the International Standards on combating money laundering and the financing of terrorism & proliferation.

- providing a level playing field to all Licensees and eliminating unnecessary duplication of obligation; and
- aligning with other Codes issued to Financial Institutions i.e. Guidance Notes issued by Bank of Mauritius to ensure one form of language for enforceable measures and for guidance.

The Code not only caters for all financial service providers licensed under the FS Act, Insurance Act 2005 and Securities Act 2005, but it is also applicable to the designated non financial businesses and professions (DNFBPs) licensed by the FSC, namely Management Companies and Corporate Trustees.

Overseas branches or subsidiaries of Licensees may follow overseas regulatory requirements and guidance, as long as the regulatory requirements and guidance are consistent with those of the Code, or are otherwise consistent with the requirements of the FATF Recommendations.

This Code comes into force on 1 April 2012 and applies to all Licensees of the FSC.

Financial Services Commission
March 2012

1.2 Purpose and Status of the Code

In terms of regulatory hierarchy, the Code is a form of 'Guidelines' issued by the FSC pursuant to its functions and powers under sections 6(c) and 7(1) (a) of the FS Act and section 18(1) (a) of the FIAML Act. The Code is intended to assist Licensees 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. 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.

The FSC has adopted a Risk-Based Supervision Framework since 1 July 2009 which was implemented to assist the FSC to:

(i) monitor the progress of licensees in terms of their operational and compliance aspects which includes AML/CFT;
(ii) identify supervisory actions required in relation to the risk profile of entities;
(iii) focus on entities whose potential failure could lead to a systemic crisis; and
(iv) target and prioritise the use of its resources for supervision.

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", in compliance with the statutory requirements and in applying the Code, Licensees should as far as possible adopt an appropriate risk based approach to ensure that the measures in place correspond to the risks identified. This approach should be an essential foundation to the efficient allocation of resources. Licensees must consider what additional measures to adopt to prevent them and their services from being used to launder money or to finance terrorism.

A risk based approach[3] –

(i) Identifies that risks related to money laundering and financing of terrorism differ across customers, countries and territories, products and services and delivery channels;
(ii) Allows licensees to understand the nature of the customer based on its vulnerabilities in a way that matches its risk;
(iii) While having minimum standards, allows licensees to apply adequate internal controls and system, commensurate with the nature of its activities and arrangements; and
(iv) Assist licensees in the allocation of resources for the prudential conduct of business.

[3] Wolfsberg Statement, Guidance on a Risk Based Approach for Managing Money Laundering Risks, 2006

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

1.3 Sanctions for non-compliance with the Code

Non-compliance with the Code will expose the Licensee to regulatory action i.e. a direction under section 7(1)(b), section 46 of the FS Act or section 93 of the Insurance Act 2005 to observe the Code. Failure to comply with the direction shall amount to an offence under section 91 of the FS Act and may further lead to sanctions imposed by the Enforcement Committee pursuant to section 53 of the FS Act.

The sanctions available to the Enforcement Committee to look into breaches include:

- issuing a private warning;
- issuing a public censure;
- disqualifying a Licensee from holding a licence or a licence of a specified kind for a specified period; in the case of an officer of a Licensee, disqualifying the officer from a specified office or position in a Licensee for a specified period;
- imposing an administrative penalty; and
- revoking a licence.

Where a Licensee has difficulty in complying with any aspect of this Code, it should proactively advise the FSC. Nonetheless, Licensees should note that compliance with the Code will not constitute a defence to a prosecution for an offence under the FIAML Act and/or under FS Act.

1.4 Core AML/CFT Principles

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 have in place documented internal systems to prevent money laundering, report suspicious transactions and appoint a Money Laundering Reporting Officer;

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

- 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 explained in chapters 3 to 8 of the Code.

CHAPTER 2 - MONEY LAUNDERING AND TERRORIST FINANCING

Sections in this Chapter:

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 – This is the first stage in which illicit funds are separated from their illegal source. Placement involves the initial injection of the illegal funds into the financial system or carrying of cash across borders.

Layering – After successfully injecting the illicit funds into the financial system, laundering them requires creating multiple layers of transactions that further separate the funds from their illegal source. The purpose of this stage is to make it more difficult to trace these funds to the illegal source.

Integration – This is the final stage in a complete money laundering operation. It involves reintroducing the illegal funds into the legitimate economy. The funds now appear as clean income. The purpose of the integration of the funds is to allow the criminal to use the funds without raising suspicion that might trigger investigation and pursuit.

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, the financial and related services that Licensees offer are also vulnerable to abuse by money launderers.

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 Terrorist financing

Terrorist financing is the act of providing financial support to acts of terror, terrorists or terrorist organisations to enable them to carry out terrorist acts. Unlike other criminal organisations, the primary aim of terrorist groups is non-financial. Yet, as with all organisations, terrorist groups require funds in order to carry out their primary activities. This simple fact – the need for funds – is key in fighting terrorism. Follow the money. Follow the financial trail. This is the core objective of all measures that aim to identify, trace, and curb terrorist financing.

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 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.

2.3 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.

2.3.1 Financial Action Task Force (FATF)

The FATF's Forty Recommendations and Nine Special Recommendations on Terrorist Financing are 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.

Further information on the FATF may be obtained from its website at www.fatfgafi.org.

2.3.2 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 customer 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

2.3.3 The Wolfsberg Group

The Wolfsberg Group, which comprises some of the world's leading private banks, 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

2.3.4 International Organisation of Securities Commissions (IOSCO)

In 1992, IOSCO adopted a resolution inviting IOSCO members to consider issues relating to minimizing money laundering. 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.

2.3.5 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, the 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 replaced the anti-money laundering guidance paper for insurance supervisors and insurance entities which was issued in January 2002. The new guidance paper took 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.

2.4 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[4]. 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

[4] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct

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.

2.5 The Legal Framework in Mauritius

2.5.1 The Financial Intelligence and Anti-Money Laundering Act 2002 – "FIAML Act"

The principal anti-money laundering legislation in Mauritius is 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:

2.5.1.1 Part II of the FIAML Act

(i) 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.

(ii) Section 3(1) (b)

Receiving, possessing, concealing, disguising, transferring, converting, disposing or removing from or bringing into 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 (of any kind, nature or description, whether moveable or immoveable, tangible or intangible) which is in whole or in part, directly or indirectly the proceeds of any crime. The term is also defined under Section 2 of the FIAML Act.

Crime includes any crime in Mauritius as defined under Section 2 of the FIAML Act, any activity carried on outside Mauritius and any act or omission which occurred 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 the 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 penal servitude.

2.5.1.2 Part IV of the FIAML Act

(i) 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.

(ii) Tipping Off

Section 19 (1)(c) of the FIAML Act provides for the offence of 'tipping off' - which offence is committed when a person, knowingly or without reasonable excuse, warns or informs the owner of any funds of any report or any action that is to be taken in respect of any transaction concerning such funds.

2.5.2 The Prevention of Terrorism Act 2002 – "POTA"

The POTA aims at combating terrorism in general and empowers our legal system to adequately deal with the phenomenon of terrorism. This Act –

(i) provides for the prevention and suppression of terrorism;
(ii) reinforces intelligence gathering, investigatory and enforcement measures relating to terrorism offences; and
(iii) implements the international commitments of the Republic of Mauritius in respect of terrorism.

2.5.3 The Convention for the Suppression of the Financing of Terrorism Act 2003

The objective of this Act, which came into force in 2003, is to give force of law to the International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations on 9 December 1999, endorsed by Mauritius.

The Act provides for offences relating to the financing of terrorism as well as for the forfeiture of funds of convicted persons.

2.5.4 The Financial Services Act 2007 -"FS Act"

The FS Act regulates the conduct of business by Licensees and makes provisions for the regulatory and supervisory powers of the FSC. Pursuant to section 7(1) of the FS Act, the FSC has such powers as necessary to enable it to discharge its functions, including those which arise under section 7(1) and section 43 of the FS Act.

Further, section 18 (3) of the FIAML Act empowers the Commission to proceed against a Licensee under section 7 of the FS 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.

2.5.5 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 and section 83(7)(d) of the FS Act imposes an obligation on the FSC to pass on to the FIU any information suggesting the possibility of a money laundering offence or suspicious transaction.

In June 2004, the FSC and the FIU signed a Memorandum of Understanding (MOU) in order to facilitate the exchange of information between the two institutions.

CHAPTER 3 – INTERNAL CONTROLS AND MONEY LAUNDERING REPORTING OFFICER

Sections in this Chapter:

3.1 Internal controls

Regulation 9 of the FIAML Regulations 2003 requires all Licensees to implement a system of internal controls as well as other measures to combat money laundering and financing of terrorism. This would include programmes for assessing risk relating to money laundering and financing of terrorism as well as the formulation of a control policy that covers issues of timing, degree of control, areas to be controlled, responsibilities and follow-up actions.

Licensees must therefore 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. Licensees must establish written internal policies and procedures as well as comprehensive manual so that, in the event of a suspicious activity being discovered, all staff members are aware of the reporting chain and the procedures to follow. The manuals must be in line with applicable laws, regulations and guidelines and must be approved by the board of directors. They should be periodically updated to reflect any legislative changes.

The FSC is not prescriptive in the adoption of controls relevant to the business model and assessed risk of a licensee in a risk based approach regime. However, Licensees should be aware that the above does not exempt them from applying effective AML/CFT controls.

The board of directors and senior management has the responsibility to promote an organizational culture which establishes through both actions and words the expectation of compliance by all employees to observe the standards of good practices and ethical behaviours so as internal policies and procedures are adhered to.

Furthermore, Licensees are required to ensure that an adequately resourced and independent audit function is available to verify compliance (including sample testing) with these procedures, policies and controls.

Licensees should also incorporate in their internal control system appropriate policies to prevent the misuse of technological developments in money laundering or terrorist financing schemes. Licensees should ensure that staff is kept abreast of relevant technological developments and identified methodologies in money laundering and

terrorist financing schemes. Licensees may refer to the FATF Report on "Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites & Internet Payment Systems" as well as the FATF Typologies.

3.2 Appointment of the Money Laundering Reporting Officer (MLRO)

Pursuant to Regulation 6(1) of the FIAML Regulations 2003, Licensees must appoint a Money Laundering Reporting Officer (MLRO) to whom all internal report of suspicious transactions must be made (A sample Internal Disclosure Form to the MLRO is found at Appendix I). All Licensees must, at all times, have a MLRO, who should be of sufficiently senior status, with the relevant qualification, experience, competence, authority and independence to be able to discharge the reporting obligation effectively and autonomously.

Licensees should take appropriate measures to ensure that internal suspicious transaction reporting systems continue to function properly. In the absence of the MLRO, the FSC requires the appointment of an Alternate MLRO who should be of similar status, qualification and experience to the MLRO.

Where a person is appointed as MLRO or Alternate MLRO in various entities, Licensees must ensure that there are adequate measures in place to ensure that:

- they have adequate autonomy and independence;
- they have access to all relevant material in order to make an assessment as to whether the transaction/activity is suspicious or not; and
- there is adequate reporting to the board of the entities.

It is imperative that all Board members and employees of each Licensee are made aware of the identity of its MLRO and Alternate MLRO (as and when applicable).

3.3 Notification of the Appointment of the Money Laundering Reporting Officer

Licensees must inform the FSC of the identity of the MLRO within 21 days of his/her appointment. The appointment of an Alternate MLRO in the absence of the MLRO must be duly notified to the Commission.

3.4 Role of the Money Laundering Reporting Officer

Adequate procedures should be implemented by Licensees to ensure that their MLRO has timely access to customer identification data and other CDD information, transaction records, and other relevant information in order to properly evaluate internal suspicious transaction reports. MLROs must be autonomous in their decisions as to whether a suspicious transaction report should be made 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.

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.

The duties of the MLRO should at a minimum consist of the following:

- implementing and monitoring the day-to-day operation of the AML/CFT policy and procedures.

- reporting 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.

- preparing reports annually and such other periodic reports as he/she deems necessary to the Board of the Licensee or a committee of the Board dealing with:-

    - the adequacy/shortcomings of internal controls and other AML/CFT procedures implemented,
    - recommendations to remedy the deficiencies identified above, ○ the number of internal reports made by staff, ○ the number of reports made to the FIU.

The MLRO should be the main point of contact with the FIU in the handling of disclosures.

The Board of the Licensee should have regular contact with the MLRO so as to ensure that the Licensee is:

- complying with all the statutory obligations and provisions regarding AML/CFT; and
- taking sufficiently robust measures to protect itself against the potential risk of being used for money laundering and terrorist financing.

In the absence of the MLRO, the Alternate MLRO is expected to fulfill similar duties, as provided and explained above.

CHAPTER 4 – CUSTOMER DUE DILIGENCE

Sections in this Chapter:

4.1 Customer Due Diligence Measures – "CDD Measures"

AML/ CFT Principle:

Licensees must, when establishing a business relationship with an Applicant for Business and on an ongoing basis, using a risk based approach apply appropriate Customer Due Diligence measures on the business relationship, including identifying and verifying the identity of the Applicant for Business.

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

Section 17 of the FIAML Act requires Licensees to verify the true identity of all customers and other persons with whom they conduct transactions. Licensees must establish and verify the identity and the current address of the applicant for business as well as the nature of the applicant's business, his financial status and the capacity in which he is entering into the business relationship with the Licensee.

Regulation 3 of the FIAML Regulations 2003 prohibits financial institutions from opening anonymous or fictitious accounts. In this context, Licensees should not set up and maintain anonymous accounts or accounts which the Licensee knows or has reasonable cause to suspect, are in fictitious names.

Licensees must therefore undertake CDD measures and be satisfied of the results obtained –

- Prior to establishing any business relationship with an applicant for business and carrying out any business transaction for or on behalf of the applicant for business;

- In cases of one-off transactions or a series of occasional transactions[5] 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

- Whenever there is a suspicion of money laundering or terrorist financing at any point in time since the inception till the termination of the business relationship.

CDD measures that should be taken by Licensees using a risk based approach 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[6] 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 the source of funds).

Licensees must ensure that all documents, data or information collected under the CDD process are kept relevant and up-to-date by undertaking reviews of existing records, using a risk based approach particularly for higher risk categories of customers or business relationships.

If Licensees form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping off when performing the customer due diligence process. If the Licensee reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file Suspicious Transaction Report ('STR') to the FIU as per section 6.5 of the Code. Licensees should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

4.1.1 Identification and verification of applicants for business who are natural persons

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

[5] "Occasional transactions" means two or more one-off transactions that are linked or appear to be linked.

[6] 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.

have in place clear procedures on how they will identify and verify the identity of their customers. These procedures must be brought to the knowledge of all relevant staff.

Where an applicant for business is a natural person, Licensees must identify and verify the identity of the applicant for business in accordance with the measures outlined below:

Identification data for natural persons

A Licensee must collect relevant identification data on a natural person, which includes:

- Name (including any former names, any other names used and other aliases)
- Current residential address[7]
- Date and place of birth
- Nationality
- Any occupation, public position held and where appropriate the name of the employer

Verification of identity of natural persons

All identification data collected by the Licensees must be verified.

The identity documentation must be obtained and retained by all Licensees to verify the information provided by principals about their identity. The documentation must be presigned and must be either in an original form or must be certified appropriately - and should bear a photograph of the principal.

(a) Verification of the identity of the natural person

The following types of identity documentation can be relied upon:

- National Identity cards
- Current valid passports
- Current valid driving licences

(b) Verification of the address of the natural person

The following identity documentation[8] can be relied upon to verify the address of the applicant for business if he/she is a natural person:

- A recent utility bill issued;
- A recent bank or credit card statement dated; or

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

[8] The term 'recent' means within the last 6 months.

- A recent bank reference.

Alternatively, verification may be achieved by:

- Obtaining a reference from a professional person who knows the natural person. The reference must include the permanent residential address of the individual;
- Checking a current register of electors;
- Utilising an address verification service; or
- Visit the individual at his/her current residential address.

4.1.2 Identification and verification of applicants for business who are legal persons/arrangements

4.1.2.1 Legal persons

Legal persons include bodies corporate, partnerships, associations or any other body of persons other than legal arrangements.

(a) Verification of the existence of a legal person and identifying the principals thereof

Where an applicant for business is a legal person, Licensees must –

- take reasonable measures to understand the ownership and control structure of the applicant for business;
- verify and establish the existence of the legal person; and
- determine the identity of the principals of the legal person.

For avoidance of doubt, in the case of a legal person, principals of applicants for business include the following:

- Promoters
- Beneficial owners and ultimate beneficial owners
- Officers[7]
- Controllers[8]
- Company Directors[9]

[7] The term "officer" is defined under section 2 of the Financial Services Act 2007.
[8] The term "controller" is defined under section 2 of the Financial Services Act 2007.
[9] The FSC expects Licensees to verify the identity of at least two directors of corporate applicants for business.

Licensees must:

(i) identify and verify the identity of the legal person, including name, incorporation number, date and country of incorporation or registration;

(ii) identify and verify any registered office address and principal place of business (where different from the registered office);

(iii) verify the legal status of the legal person; and

(iv) identify and verify the identity of underlying principals (including beneficial owners, controllers, directors or equivalent) with ultimate effective control over the capital or assets of the legal person; and

(v) verify that any person who purports to act on behalf of the legal person is duly authorised and identify that person.

Where the underlying principals are not natural persons, Licensees must 'drill down' to establish the identity of the natural persons ultimately owning or controlling the business.

When seeking to identify and verify the identity of underlying principals, reference should be made to the identification and verification requirements for natural persons as outlined in section 4.1.1 of the Code.

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

(a) 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 exist;
- Reviewing a copy of the latest report and accounts if available (audited, where possible);
- Obtaining details of the registered office and place of business;
- Verifying the identity of the principals of the company as above;

(b) 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 principals as above;

(c) 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 Mauritian *sociétés*, checking with the Registrar of Companies that the *société* is registered and 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*;

4.1.2.2 Legal arrangements

Trusts do not have separate legal personality and therefore form business relationships through their business. It is the trustee of the trust who will enter into a business relationship on behalf of the trust and should be considered along with the trust as the customer.

(a) Verification of the existence of a legal arrangement and identifying the principals thereof

Where an applicant for business is a legal arrangement, Licensees must –

- take reasonable measures to understand the ownership and control structure of the applicant for business;

- verify and establish the existence of the legal arrangement; and

- determine the identity of the principals of the legal arrangement.

For avoidance of doubt, in the case of a legal arrangement, principals of applicants for business include the following:

- Settlors or Contributors of capital (whether named or otherwise)
- Trustees

- Beneficiaries[10]
- Protectors
- Enforcers

Licensees must:

(i) verify the legal status of the legal arrangement;

(ii) identify and verify the identity of the principals of the applicant for business, that is, those natural persons with a controlling interest and those who comprise the mind and management of the legal arrangement; and

(iii) obtain information concerning the name of trustee(s), its legal form, address and provisions binding the legal arrangement.

In relation to a trust, the above requirements can be achieved by:

- Obtaining an original or appropriately certified copy of the trust deed or pertinent extracts thereof;
- Where the trust is registered – checking with the relevant registry to ensure that the trust 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;

Whether an applicant for business is a company, a trust, a partnership, a *société* or any other body of persons, 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 customers who are natural persons (please refer to section 4.1.1 of the Code). This requirement is in addition to verifying the existence of the company, trust, partnership, *société* or any other body of persons (please refer to section 4.1.2 of the Code).

4.1.3 Acquisition of a Business or Block of customers

[10] The FSC takes note 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.

There are circumstances where a Licensee may acquire a business with established business relationships or a block of customers. Before taking on such type of business, a Licensee should undertake sufficient enquiries to determine whether the CDD policies, procedures and controls as described in the Procedure Manual of the other Licensee is satisfactory and in line with prevailing legislations to establish the level and the appropriateness of identification data held in relation to the customers and the business relationships of the business to be acquired.

A Licensee may rely on the information and documentation previously obtained where:

- the business relationships were established in equivalent jurisdictions;
- the CDD policies, procedures and controls which were in place were satisfactory; and
- the Licensee has obtained identification data for each customer acquired.

Where deficiencies in the identification data held are identified (either at the time of transfer or subsequently), the accepting Licensee must determine and implement a programme to remedy any such deficiencies.

4.2 Source of funds/property and source of wealth

In the identification of risk and prevention of money laundering, it is a pre-requisite for Licensees to understand the origin or provenance of funds or property underlying a business relationship with a customer. Therefore understanding the customer's source of funds/property and the customer's source of wealth is an important aspect of customer due diligence.

It is important to distinguish between the source of funds/property and the source of wealth. The "**source of funds**" is the activity or transaction which generates the funds for a customer while the "**source of wealth**" refers to the activities which have generated the total net worth of the customer.

Licensees must therefore use a risk based approach andby taking appropriate measures establish the source of funds for each applicant for business and when third party funding is involved, Licensees must make further enquiries as to the relationship between the person providing the funds and the applicant.

Licensees must ensure that there is consistency between the information they hold on the applicant for business and the nature of transactions or proposed transactions. Where there is any indication of abnormal or potentially suspicious activity within the context of the product or service being provided, the Licensee must take additional measures to verify the information obtained.

In such cases, a Licensee should also consider obtaining information regarding an applicant's or a customer's source of wealth. This is one of the enhanced CDD measures which must be applied in cases of high risk relationships.

4.3 Appropriate certification

Where a Licensee relies upon verification of identity documentation that is 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 by a suitable person, such as a lawyer, notary, actuary, an accountant or any other person holding a recognized professional qualification, director or secretary of a regulated financial institution in Mauritius or in an equivalent jurisdiction, a member of the judiciary or a senior civil servant.

The certifier should sign the copy document and clearly indicate his name, address and position or capacity on it together with contact details to aid tracing of the certifier.

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

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

4.4 Eligible and group introducers

In recognition of the fact that a number of customers are introduced to the Licensees by third parties/intermediaries, Licensees find it necessary to place reliance upon introducers in satisfying their obligations to undertake the CDD measures, as explained in section 4.1 above. In accordance with Regulation 4(6) of the FIAML Regulations, this Code provides for 2 types of introducers: Eligible introducers and Group introducers.

Eligible introducers are persons or entities which refer business to Licensees and –

(a) are regulated for money laundering purposes; or

(b) are subject to rules of professional conduct pertaining to money laundering; and

(c) 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 IV 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 and;

- Obtaining information on the purpose and intended nature of the business relationship.

Whenever reliance is placed upon an eligible or group introducer, Licensees should bear in mind that the ultimate responsibility to ensure that the CDD measures have been completed satisfactorily rests with them. Responsibility for undertaking CDD measures on 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 –

- Licensee must carry out appropriate due diligence on the introducers to ensure their eligibility. 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. In addition, Licensees must obtain evidence of an eligible or a group introducer's status in the form of a completed Eligible Introducer Certificate (see specimen in Appendix II) or a completed Group Introducer Certificate (see specimen in Appendix III).

- 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.

- Licensees should take the adequate steps to satisfy themselves that the eligible/group introducers have copies of identification data and other relevant documentation relating to the CDD requirements. 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.

- Licensees' senior management or board of directors must ensure that periodic independent testing of the arrangements are being conducted:

    (i) to ascertain that the Licensees gain access to CDD information or obtain CDD documentation maintained by the eligible/group introducer
    (ii) to ensure that the arrangements work as designed.

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

Licensees may rely upon existing CDD documentation in the possession of an eligible or a 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.

Where the introducer ceases to act as such for the Licensee, the latter must ensure that the appropriate procedures are in place to have access to all the CDD documentation collected and kept by the introducers when the CDD measures had been undertaken.

The Code recognises only Eligible Introducers and Group Introducers as bona fide Introducers of business to Licensees. Unregulated persons that offer business to Licensees are not recognised by the Code as Introducers.

Reliance may only be placed upon an eligible or a 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 eligible or group introducer's ability to undertake appropriate CDD measures.

Section 4.4 of the Code does not apply to outsourcing or agency relationships or relationships or transactions between the financial institutions for their customers.

4.5 Omnibus Accounts[11]

When establishing an omnibus account relationship with a regulated financial institution, 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:

[11] "Omnibus accounts" has the same meaning as in the FIAML Regulations 2003 (as amended).

- 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;
- Where the financial institution is a foreign entity, ensure that the country in which it is located is an equivalent jurisdiction with a view to determine whether the client has been subject to sufficient CDD standards.
- Obtain approval of the Board of Directors before establishing new omnibus account relationships; and
- Document the respective responsibilities of each institution.

4.6 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 customer 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 any event be satisfactorily completed, such that: -

(a) it occurs as soon as reasonably practicable;
(b) it is essential not to interrupt the normal conduct of business;
(c) the money laundering risks are effectively managed.

Examples of situations where verification of identity may be delayed provided that, inter alia, this does not interrupt the normal course of business are:

- Non face-to-face business.

- Securities transactions – in the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.

- Life insurance business – in relation to identification and verification of the beneficiary under the policy. This may take place after the business relationship with the policyholder is established, but in all such cases, identification and verification

should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

The Licensee must have appropriate and effective policies, procedures and controls in place, so as to manage the risk, which must include:

(a) establishing that the transaction is not a high risk relationship;
(b) monitoring by senior management of these business relationships to ensure that the verification of identity is completed as soon as reasonably practicable;
(c) ensuring funds received are not passed on to third parties;
(d) establishing procedures to limit the number, types and/ or amount of transactions that can be undertaken; and
(e) monitoring large or complex transactions.

In the event that satisfactory CDD documentation has not been obtained, Licensees must have procedures in place to disengage from or terminate such business relationships and consider making a suspicious transaction report. Licensees should consider the potential risks inherent in engaging in any form of relationship with any applicant for business prior to satisfactorily completing CDD measures. Where a Licensee is unable to comply with the CDD requirements with respect to an applicant for business, it should consider making a suspicious transaction report to the FIU.

4.7 Existing customers

The risk of money laundering to Licensees is not posed solely by future client relationship. Existing clients can also pose significant risks. Each Licensee is best placed to assess the risk of its own customer base and the extent and nature of the customer due diligence information held or of any additional documentation or information that may be required for existing customers in accordance with the criteria within this Code.

Licensees must apply CDD requirements to existing customers on the basis of materiality and risk and conduct due diligence on such existing relationships when necessary.

Where a Licensee had previously relied upon an introducer or an intermediary to verify the identity of an existing client, it may continue to do so provided that the introducer is an eligible or a group introducer as defined within this Code and the Licensee obtains from the introducer certified copies of the CDD documents held by them.

Below are examples of situations where it is desirable to conduct CDD checks on existing customers. Please note that this list is by no means prescriptive:

(a) a transaction of significance amount takes place,
(b) customer documentation standards change substantially,
(c) there is a material change in the way the account is operated,
(d) the Licensee becomes aware that it lacks sufficient CDD information about an existing customer.

Existing customers would also refer to those business relationships which existed prior to the coming into force of the FSC Codes in April 2003. In such cases, Licensees must ensure that its policies, procedures and controls which were in place, were appropriate and effective in relation to the CDD procedures.

Where the Licensee has doubts on the adequacy of the CDD conducted previously, the Licensee should consider application of the procedures set out in this Code.

CHAPTER 5: HIGH RISK AND LOW RISK RELATIONSHIPS

Sections in this Chapter:

5.1 Risk profiling[12]

The need to know the customers 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. As a result, Licensees are required to extend the concept of CDD beyond the usual process of identification and verification of the customer and must include the identification of the potential risks of a business relationship. Such risks would include criminal risk of money laundering, reputational risk, legal risk, credit risk, fiduciary risk, regulatory risk and operational risk[13] amongst others.

After the collection of the CDD documentation, the Licensee must make an initial assessment of the risk to which the business relationship will expose the Licensee and evaluate the customer accordingly. In this exercise, Licensees will take into consideration a number of factors, including but not limited to the following:

- The nature and type of customer
- The commercial rationale for the relationship
- The geographical location of the customer's residence
- The geographical location of the customer's business interests and/or assets
- The nature and value of the assets concerned in the relationship
- The customer's source of funds and where necessary the 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

[12] Licensees may refer to the FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing for further details.

[13] 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

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 to the relationship.

While a risk assessment should always be performed prior to entering a business relationship, for some customers, a comprehensive risk profile may only become evident once the customer has begun transacting through an account. Therefore on-going monitoring of customer transactions and on-going reviews are fundamental components of an appropriate risk-based assessment. A Licensee may also have to adjust its risk assessment of a particular customer based upon information received after the establishment of the relationship.

5.2 High risk relationship

Licensees should apply enhanced due diligence measures in all high risk business relationships, customers and transactions.

Where a Licensee has assessed that the business relationship or occasional transaction is a high risk relationship, based on the customer's individual risk status, that is, the nature of the customer, the business relationship, its location, or any other specificity of the business relationship, it must ensure that adequate policies, procedures and controls are in place to apply enhanced CDD measures as required under Regulation 9 of the FIAML Regulations.

5.3 Enhanced due diligence measures

Enhanced due diligence would imply taking additional steps in relation to identification and verification. This may include the following steps:–

(i) obtaining further customer due diligence information (identification and relationship information) from either the customer or independent sources (such as the internet, public or commercially available databases);

(ii) verifying additional aspects of the customer due diligence information obtained;

(iii) obtaining additional information required to understand the purpose and intended nature of such a business relationship;

(iv) taking appropriate and reasonable measures to establish the source of the funds and the wealth of the customer, any beneficial owner and underlying principal; and

(v) carrying out more frequent and more extensive ongoing monitoring on such business relationships with setting lower monitoring thresholds for transactions connected with such business relationships.

The nature of the measures to be applied will depend on the circumstances of the relationship or transaction and the factors leading to the customer being considered as higher risk.

5.3.1 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 PEPs, family members or close associates of PEPs are deemed to pose a greater than normal money laundering risk to Licensees by virtue of the possibility for them to have benefited from proceeds of corruption. Licensees are encouraged to consider the ongoing status of customers classified as PEPs on a case-to-case basis using a risk based approach.

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 organisations 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 or its beneficial owner is a PEP, a family member or a close associate of PEPs. Licensees must seek relevant information from the applicant as well as refer to publicly available information.

In addition, Licensees must:

- develop a clear policy on the acceptance of business relationships with such individuals;

- obtain the approval of senior management prior to establishing relationships with such applicants for business;

- where applicants have been accepted and the said applicant or its beneficial owner is subsequently found to be, or subsequently becomes, a PEP, obtain the approval of senior management to continue such business relationships;

- obtain similar approval from senior management in cases of family members or close associates of PEPs;

- take enhanced due diligence measures to establish the source of funds and source of wealth of applicants, beneficial owners, family members or close associates of PEPs;

- conduct enhanced ongoing monitoring of the business relationships involving PEPs, family members or close associates of 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 take note of the Transparency International Corruption Perceptions Index at www.transparency.org and take appropriate measures to manage the increased risks of conducting business with PEPs.

5.3.2 Non face-to-face business relationships

The FSC recognises that the business conducted by Licensees may also be conducted on a non-face to face basis with customers. Often, it is either impossible or impractical for Licensees to have or to obtain original documentary evidence of identity. However in such cases, Licensees should apply the following CDD procedures when dealing with non-face-to-face applicants for business:

(a) the certification of documents presented;

(b) the requisition of additional documents to complement those which are required for face- to-face applicant for business; and

(c) the initiation of an independent contact with the customer.

5.3.3 FATF Statements and non-cooperative 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 countries which are non-cooperative jurisdictions or which have been the subject of FATF Public Statements for deficiencies in their AML/CFT systems (Please refer to Appendix V).

5.4 Low Risk Relationships

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 simplified or reduced due diligence measures when identifying and verifying the identity of the applicant for business.

Licensees must ensure that when they become aware of circumstances which affect the assessed risk of the business relationship or occasional transaction, they must undertake a review of the CDD documentation and information held with a view to determine whether it is appropriate to continue applying simplified or reduced CDD measures.

Where Licensees take a decision to apply simplified or reduced CDD measures, documentary evidence which supports the decision must be retained.

5.5 Simplified or reduced Due Diligence Measures

Where the applicants for business consist of bodies as listed below, simplified or reduced CDD measures may be applied and the Licensee needs to obtain at a minimum the following information set out in the table below.

If Applicant for business is	CDD Documentation required
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[14][15].	Licensees must obtain and retain documentary evidence of the existence of the financial services business and of its regulated status[17].
A public company listed on the Stock Exchange of Mauritius or on Recognised, Designated and Approved Stock/ Investment Exchanges [16] or subsidiaries thereof. Government administrations or enterprises and statutory bodies	Licensees must obtain a copy of the annual report and accounts of that public company and must verify that the individuals who purport to act on behalf of such entity 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. Licensees must obtain and retain documentary evidence of identification and verification of identity.
A pension, superannuation or similar scheme which 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.

However simplified CDD measures will not be acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

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

[15] 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.

[16] A list of Recognised, Designated and Approved Stock/Investment Exchanges may be found at Appendix VI.

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[17] before applying such reduced or simplified measures, in order to ensure that the reduced CDD measures are consistent with this Code.

Where any aspect of the relationship or occasional transaction expose the Licensee to an increased level of risk (for example, by virtue of the country; territory; or value of the relationship), then simplified or reduced CDD measures must not be applied.

[17] 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.

CHAPTER 6 – ON-GOING MONITORING, RECOGNISING AND REPORTING SUSPICIOUS TRANSACTION / ACTIVITY

Sections in this Chapter:

6.1 On-Going Monitoring

Once the identification procedures have been completed and the business relationship has been established with the customer, Licensees should monitor the relationship to ensure that it is consistent with the nature of business stated at the establishment of the relationship.

Licensees are required to monitor business relationships so that money laundering or terrorist financing may be identified and prevented. This may involve requesting additional customer due diligence information.

As mentioned previously, for some business relationships, a complete customer profile and an appropriate risk assessment may only become evident once the relationship has been established thus making monitoring of the relationship key to obtaining a complete understanding of business relationships.

For example, in relation to the the source of funds/property, the following questions might be asked when determining whether incoming funds/property may be suspicious:

- 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?

Monitoring of customer's activities and transactions would entail periodic reviews using a risk-based approach of the existing records and ensuring that up-to-date information is held in relation to the business relationship. Periodic reviews of the customer's activity and transactions can also be used as a basis to identify patterns of unusual customer activity or transactions. Licensee must also pay attention to information or instructions received from customers before or as they are being processed. Where monitoring indicates possible

money laundering or financing of terrorist activity and contact with the customer is made without due care, this could unintentionally lead to the customer being tipped off.

6.2 Complex arrangements

The FSC aims at ensuring 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. The records of such findings should be kept for a period of at least 7 years and, upon request, be made available to the FSC and auditors.

6.3 Recognising suspicious transaction and activity

Section 2 of the FIAML Act defines a suspicious transaction as *"... 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.

The word "transaction" is also defined in the section 2 of the FIAML Act, as follows: -

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 attention must be paid to cases of unusual pattern of activity within a particular business relationship. An unusual activity may be one which is inconsistent with the normal business activities for the type of product or service that is being delivered. It follows that an important precondition for recognition of a suspicious transaction or activity is that the Licensee should know enough about the business relationship to recognise that the transaction or activity is unusual. This may indicate money laundering or terrorist financing activity where the activity has no apparent economic or visible lawful purpose.

Although not all unusual or unexpected activity is necessarily suspicious, employees are expected to be able to recognise unusual activity as a result of effective CDD checks conducted on an on-going basis. Suspicion need not only be based on transactions or activities within the business relationship, but also on information from other sources, including the media, intermediaries, or the customer himself. Employees must analyse the transaction/activity in more detail to ascertain whether it is suspicious.

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 VII. 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 and ESAAMLG 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 customer relationships, adequate CDD measures enable Licensees to know enough about customers, to be able to recognise unusual or unexpected activity, as or before it occurs.

6.4 Obligation and failure to report

Section 14 of the FIAML Act provides the following:

"Every bank, financial institution, cash dealer or member of a relevant profession or occupation shall forthwith make a report to the FIU of any transaction which the bank, financial institution, cash dealer or member of a relevant profession or occupation has reason to believe may be a suspicious transaction."

Licensees therefore have the obligation to report any suspicious transaction to the FIU. As described in Chapter 3 of the Code, it is the role of the MLRO to validate any internal report on a suspicious transaction/activity made by the employees of the Licensee. As a result, it is essential that the Licensee has in place appropriate and effective internal reporting policies, procedures and controls to ensure that:

(a) all employees of the Licensee know to whom and in what format their suspicions must be reported; and
(b) all suspicion reports are considered by the MLRO and where the MLRO makes a decision not to make a report to the FIU, the reasons for such a decision must be documented and retained with the Licensee.

Appropriate and effective policies, procedures and controls should be implemented by Licensees to ensure that:

(a) each suspicion is reported to the MLRO regardless of the amount involved;
(b) the MLRO promptly considers the internal suspicion report referred to in part (a) above and determines whether there is suspicion or reasonable grounds for suspecting that a person is engaged in money laundering or terrorist financing;
(c) where the MLRO has validated the internal suspicion report, he should lodge a suspicious transaction report with the FIU; and
(d) where, during the CDD process, a Licensee knows or suspects that a person is engaged in money laundering or terrorist financing, a suspicious transaction report is made to the FIU.

Failure to report a suspicious transaction constitutes an offence and on conviction, a Licensee shall be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

6.5 Reporting suspicions to the FIU

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 using the form prescribed by the FIU.

The contact details of the FIU are as follows:

The Director
Financial Intelligence Unit
7th Floor, Ebène Heights
34, Ebène Cybercity
Ebène
Republic of Mauritius
Tel: (230) 454 1423
Fax: (230) 466 2431
Email: fiu@fiumauritius.org

In urgent cases disclosures may be made by telephone.

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 customer confidentiality. However, where a disclosure is made in good faith, the person disclosing such information may claim immunity from both civil and criminal action.

6.6 Communicating with customers and Tipping off

Once an internal suspicion report to a MLRO or a suspicious transaction report has been submitted to the FIU, it is an offence 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. When a suspicious transaction report has been made to the FIU with respect to a particular customer, Licensees must ensure that due care is taken during subsequent enquiries so as not to alert the customer about the disclosure. Appropriate measures must be taken by Licensees to ensure that the offence of tipping off is not committed.

When a suspicious transaction report is made under section 14 of the FIAML Act, the Director of the FIU may request for further information relating to the suspicious transaction from the Licensee who made the report or any other person or any Licensee who is, or appears to be, involved in the transaction. Section 16 of the FIAML Act also provides that no person directly or indirectly involved in the reporting of a suspicious transaction is allowed to inform any person involved in the transaction or an unauthorized third party that the transaction has been reported or that information has been supplied to the FIU on request.

6.7 Constructive trusts

The concept of constructive trust, as per the Trust Act 2001, arises where a profit is made due to a breach of trust or a property is obtained from such a breach. The law provides that a beneficiary may apply for an order to Court so that the profit or property obtained from the breach be traced and recovered to him.

For money laundering purposes, constructive trusts may arise due to the conflict of 'tipping off'. This will be best explained through an example. For instance, a Licensee has received funds from a customer, who shortly after, requests a payment be made to a third party. Since this transaction seems suspicious, the Licensee has two options:

(i) to refuse following the customer's instructions and at the same time run the risk of 'tipping off' the customer; or
(ii) to allow the transaction but report it to the FIU, which implies risking a constructive trust claim from the beneficiaries for breach of fiduciary duties.

The Licensee is therefore faced with a dilemma in taking a decision in such cases. The Licensee must be aware of the consequences it may face for breaching its fiduciary duties, especially in the event that it dissipates the property or deals with it in a manner which is detrimental to the interests of a constructive beneficiary.

Where a Licensee suspects criminality and is on notice that property may belong to a third party, such information must be included in its report to the FIU. If the Licensee is subsequently requested by a suspected customer to provide a reason for its inaction, it should refer to the FIU.

CHAPTER 7 – TRAINING AND CULTURE

Sections in this Chapter:

7.1 Awareness and training

Regulation 9 of the FIAML Act clearly specifies that all employees should be made aware of the Licensee's internal controls, policies and procedures. Licensees must have appropriate measures in place to make employees aware of:

- Licensee's policies, procedures and controls manual for AML/CFT;
- Legal obligations of employees, the implications of failing to report information in accordance with the established procedures and the potential criminal liability and those of the Licensee under the AML/CFT laws, regulations and guidelines;
- Developments on the money laundering and financing of terrorism techniques, methods and trends.

Employees must be informed of the identity of the MLRO as well as the responsibilities of the latter. Licensees need to ensure that employees who have been provided with the Licensee's AML/CFT policies, procedures and controls manual, fully understand them and their importance. This will enable the employee to understand the procedures for the filing of a suspicious transaction report.

Licensees must provide appropriate training to enable employees to perform their duties in respect of AML/CFT, in particular to assess adequately the information for them to judge whether the activity or business relationship is suspicious. Training should cover recognition and handling of suspicious transactions and additional measures and aims at maintaining a high level of awareness and vigilance between training sessions.

7.2 Screening and hiring of employees

To assist in the prevention and detection of money laundering and terrorist financing, one of the most important tools available to a Licensee is to have an alert staff to identify

money laundering and terrorist financing risks. Licensees must therefore put in place appropriate procedures to ensure that its staff is competent and of high integrity.

Licensees must ensure that, when hiring employees, appropriate screening measures are applied, which may include:

- obtaining references and confirming them when recruiting new employees;
- confirming employment history and the qualifications;
- requesting details of any disciplinary action taken against the individual or the absence of such action by previous employers or any professional body; and
- requesting details of any criminal convictions (or the absence of such convictions) and verifying where possible.

New employees should receive an introductory training on money laundering and terrorist financing and should also receive a clear indication of the importance placed on money laundering and terrorist financing issues. Licensees must ensure that the employees are aware of the legal requirements for reporting a suspicious transaction/activity as well as the procedures for reporting to the MLRO, prior to them becoming actively involved in day to day operations.

7.3 Relevant employees

It is important to demarcate those employees whose duties relate to the handling of business relationships or transactions from the Licensee's overall staff. They would accordingly be referred to as "relevant employees".

When determining whether an employee is a relevant employee, the Licensee may take into consideration the following:

(a) whether the employee is undertaking any customer facing functions or is responsible for the handling of business relationships or transactions; or

(b) whether the employee is directly supporting a colleague who carries out any of the functions mentioned in (a) above.

The Board and senior management are responsible for the effectiveness and appropriateness of the Licensee's policies, procedures and controls to counter money laundering and terrorist financing. As such, directors, managers and the MLRO would also be considered as relevant employees, to whom ongoing training must be given so that they remain competent to give informed and adequate consideration to the evaluation of the effectiveness of those policies, procedures and controls.

7.4 On-going training

Licensee must ensure that relevant employees receive on-going trainings. The training should be relevant to the role and responsibilities of the employees and may include:

- legal obligations as well as all aspects of the AML/CFT laws, regulations and guidelines;

- the money laundering and terrorist financing vulnerabilities of the products and services offered by the Licensee;
- the CDD requirements and the requirements for the internal and external reporting of suspicion;
- recognition and handling of suspicious transactions/activities;
- the criminal sanctions in place for failing to report information;
- new developments including information on current money laundering and terrorist financing techniques, methods, trends and typologies; and
- information on the changing behaviour and practices amongst money launderers and those of financing terrorism.

The frequency of training should be determined on a risk-based approach, with those employees with responsibility for the handling of business relationships or transactions receiving more frequent training. However there should be a minimum of at least one training session annually.

7.5 MLRO training

As MLROs and Alternate MLROs have significant responsibility for the receipt, evaluation and where appropriate external reporting of suspicious transactions to the FIU, MLROs and Alternate MLROs should be given additional training. The additional training must be in-depth and specific with regard to:

(a) the recognition and handling of suspicious transactions;
(b) liaising with law enforcement agencies; and
(c) the management of the risk of tipping off.

MLROs and Alternate MLROs should familiarise themselves with the FATF Reports on Money Laundering Typologies that examine trends in money laundering activity. They should also be aware of those countries designated by FATF as having deficiencies in their AML/CFT systems.

7.6 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. The precise approach will depend on the size, nature and complexity of the Licensee. The training should equip the employees in respect of their responsibilities.

7.7 Culture

The FSC believes that internal procedures and staff training must be supported by an effective internal compliance culture. The prevailing culture of an organisation may create certain barriers, which may lead to dealing inappropriately with 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 customers 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.

CHAPTER 8 – RECORD KEEPING

Sections in this Chapter:

8.1 General requirements

Pursuant to section 17(b) of FIAML Act, a Licensee must keep such records, registers and documents as prescribed in Regulation 8 of the FIAML Regulations. Furthermore section 29 of the FSA requires every Licensee to keep and maintain internal records of the identity of each customer as well as full and true written records of all transactions relating to his business activities. The records maintained by Licensees may prove to be very valuable 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).

Licensees are expected to have appropriate and effective policies, procedures and controls in place to ensure that records are prepared, kept for the stipulated retention period and in a readily retrievable form so as to be available on a timely basis to the FSC upon request.

8.1.1 Customer due diligence information

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 the stipulated period thereafter. The records will include the following:

(a) copies of the identification data obtained to verify the identity of all customers, beneficial owners and underlying principals; and
(b) copies of any customer files, account files, business correspondence and information relating to the business relationship; or
(c) information as to where copies of the identification data and other files may be obtained.

8.1.2 Transactions

In order to assist law enforcement to follow audit trails should the need arise, Licensees must maintain records of all transactions undertaken on behalf of the customer during the course of a business relationship either in the form of original documents or copies of original documents.

All transactional records should be retained for the stipulated period after the completion of the transaction to which they relate. Transactional records are records containing information on individual transactions, set out as follows:

(a) the name and address of the customer, beneficial owner and underlying principal;
(b) if a monetary transaction, the currency and amount of the transaction;
(c) source and destination of funds including full remitter details (instructions, forms of authority)
(d) account name and number or other information by which it can be identified;
(e) details of the counterparty, including account details;
(f) sale and purchase agreements as well as service agreements; (g) the nature of the transaction; and (h) the date of the transaction.

In every case, sufficient information must be recorded to enable the reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

8.1.3 Internal and external suspicious reports

Licensees are required to maintain the following records on the suspicious reports being filed:

(a) the internal suspicion reports received by the MLRO;
(b) records of actions taken under the internal and external reporting requirements;
(c) when the MLRO has considered information or other material concerning the reports, but has not made a disclosure of suspicion to the FIU, a record of the information or material that was considered and the reason for the decision; and
(d) all reports made by the MLRO to the FIU.

8.1.4 Training

In line with Chapter 7 of the Code, Licensees must maintain records of all AML/CFT training delivered to employees. Records should include:

(a) the dates AML/CFT training was provided;
(b) the nature of the training, including details of contents and mode of delivery; and
(c) (c) the names of the employees who received training.

8.1.5 Compliance monitoring

With a view to ascertain that compliance is being monitored at all level of the Licensee, records must be kept to ensure that appropriate policies, procedures and controls are in place and are being properly adhered to. Such records will also help management in reviewing the compliance policy, procedures and internal controls and maintaining an adequately resourced audit function. Records must include:

(a) reports by the MLRO to the Board and senior management;
(b) records of consideration of those reports and of any action taken as a consequence; and
(c) any records made within the Licensee or by other parties in respect of compliance of the Licensee with the relevant AML/CFT laws and guidelines.

8.2 Forms of record and record retrieval

Records may consist of original hard copy documents as well as data or documents maintained electronically. In any event, Licensees should be able to retrieve records easily and quickly. Also Licensees must periodically review the ease of retrieval of, and condition of, paper and electronically retrievable records.

Licensees are required to make records available to the FSC in a timely manner. They must therefore consider the implications for meeting this requirement where documentation, data and information is held overseas or by third parties or where reliance is placed on introducers. The FSC reminds Licensees that 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 and disclose them such records when so required.

Licensees should also 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 put in place contingency arrangements that it deems necessary to create or replace records in the event of a disaster.

8.3 Period of retention

The Companies Act 2001 and the FS Act prescribe a period of seven years. Therefore all records must be kept for a stipulated period of at least seven years.

8.4 Inspection of records

Licensees are made aware that during the course of on-site visits, the FSC will inspect the above mentioned records, to ensure that they are maintained in line with the requirements set out in this Code.

CHAPTER 9 – INDUSTRY/ SECTOR SPECIFIC GUIDANCE

Sections in this Chapter:

9.1 Management Companies/ Trustees

When dealing with customers wishing to set up global business companies and/or trusts, Licensees must be in a position to adequately assess the associated AML/CFT risks.

Who is the Applicant for business?

When setting up a company, the applicant for business refers to the customer upon whose instructions the company is established. This may be a proposed shareholder or a promoter.

Where Licensees create trusts for their customers, the applicant for business will be the settlor(s).

Identification and verification of identity

When companies are set up, in addition to identifying and verifying the identity of the applicant for business, the Licensee must obtain the following:

(i) The nature of the proposed company's business and the source of funds
(ii) Evidence of the identity of each of the proposed principals

Where a Licensee provides corporate or other services to companies it administers, the Licensee must conduct CDD on all the principals of the companies.

Similarly, in the case of a trust being created, the Licensee must conduct due diligence on all principals involved in the trust being formed. The Licensees must make appropriate inquiry as to the source of the assets of the settlor which will be the trust property. This exercise will vary according to the types of trusts created, the trust property and the objectives of the settlor as well as the duration of the trust. The Licensees must ensure that the same CDD procedures are followed as and when there is a change in the trust property by the settlor(s).

With a view to identify and verify the principals of the company being set up or trust being created, the Licensee should apply provisions of sections 4.1.1 and 4.1.2 of the Code, as appropriate.

It is recognised however that in such businesses, Licensees may at times use introducers to conduct CDD. In such cases, where introducers are involved, Licensees should refer to section 4.4 of the Code.

Change in Management Company and Additional or Change in Trustee

Customers have the right to choose which management company should administer their businesses and to change to others if they so wish. However Licensees should communicate with each other and make appropriate enquiries as to the reason for the transfer of business. All documentation pertaining to the due diligence of the customer should be duly transferred to the new management company and the latter should be satisfied of the CDD conducted previously. If this is not the case, the new management company may adopt additional measures to comply with the provisions of this Code.

When there is an additional or a change in trustees, the new trustee must ensure that the CDD measures have been conducted on the settler(s) at the time of creation of the trusts, as well as whenever there has been change in the trust property. All the relevant due diligence documentation such as the verification of the settlor's identity and source of funds must be made available. Where the trustee believes that the documentation available is not adequate for the CDD measures, it may wish to enquire from the settlor. However where the settlor is no more alive, the trustee may enquire from existing or previous trustees as well as from the beneficiaries, especially in cases of family trusts.

Service Providers

Licensees should understand the purposes and activities of their customer companies to which they provide services. Suspicion could be raised if the Licensees are unable to obtain adequate explanation of any of the following features, which may include but is not limited to:

- complex networks of trusts and/or nomineeships and/or companies
- transactions which lack economic purpose (for example, sales or purchases at undervalued or inflated prices; payments or receipts being split between a large number of bank accounts or other financial services products; companies consistently making substantial losses)
- transactions which are inconsistent (for example, in size or source) with the expected objectives of the structure
- arrangements established with the apparent objective of fiscal evasion;
- clarity about beneficial ownership or interests or difficulties in verifying identity of persons with ownership or control;
- unwillingness to disclose the source of assets to be received by a trust or company.

9.2 Capital Market

The nature of businesses conducted in the capital market makes it fundamental for Licensees operating in this segment to adopt the appropriate AML/CFT measures to ensure that their businesses/services offered are not being used to commit money laundering or terrorist financing.

The capital market has witnessed many sophisticated products/services which may attract money launderers and terrorist financiers. The liquidity of the markets also allows funds to move quickly and easily from one product/service to another and thus there is a risk that illicit proceeds are mixed with lawful proceeds in order to integrate them into the legitimate economy.

As such, it is more likely that a Licensee will come into contact with the layering and integration stages of a money laundering operation than the placement of cash. The money launderer's intention is to complicate the audit trail in the event of an investigation and this may be achieved by carrying out a series of transactions.

Complying with the procedures set out in this Code plays an important part in combating money laundering and terrorist financing and helps in constituting an important audit trail. This section will be of guidance not only to the securities or capital market intermediaries, the collective investment schemes (CIS) and closed-end funds and the CIS functionaries and professionals, but also to the financial service providers and the specialised financial institutions[18].

Who is the applicant for business?

Where the Licensee is:	**The Applicant for Business is:**
Securities or Capital Market Intermediaries	
an investment dealer or a representative of an investment dealer	the person who is giving instructions to execute the securities transactions
an investment adviser or representative of an investment adviser	the investor or potential investor
CIS, CIS Functionaries and Professionals	
a CIS or a closed-end fund	the investor or potential investor
a CIS manager	the CIS
a CIS administrator	the CIS (and the investor or potential investor, where CDD has been delegated to the administrator)
Financial Service Providers	the person who is giving instructions to the service provider for execution of a
	transaction **[the customer]**
Specialised Financial Institutions	the person who is giving instructions to the service provider for execution of a transaction **[the customer]**

[18] Please refer to the Financial Services (Consolidated Licensing and Fees) Rules 2008 for details on the categories of service providers.

How and when should identity be verified?

If the Applicant for Business is a natural person, the Licensee should apply provisions of section 4.1.1 of the Code.

If the Applicant for Business is a corporate body or other legal arrangement, then provisions of section 4.1.2 of the Code would apply.

Licensees must ensure that adequate procedures are in place to verify the identity of the applicants for businesses as soon as reasonably practicable after an initial contact has been made between the two parties. Satisfactory evidence of the identity must be obtained by the Licensees before the provision of any financial service.

Where the Licensee has not been able to complete the CDD measures prior to the provision of the financial service, it must ensure that this is done in conformity with section 4.6 of the Code, where the approval of senior management must be sought and recorded in writing.

If a Licensee acquires the customers/accounts of another Licensee, the Licensee acquiring the new customers must be satisfied that the verification of identity procedures have been undertaken accordingly. When this is not the case, the Licensee has to undertake verification of identity of all the transferred customers as soon as practicable. The procedures set out in section 4.1.3 of the Code must be complied with.

When is it possible to rely on third parties to verify identity?

Customers may at times be introduced to Licensees by way of third parties, i.e. the Introducers, with whom business relationships are already established. Thus the Licensees may rely on the appropriate evidence of customer verification provided by the Introducer, as provided under section 4.4 of the Code.

The latter may provide:

(i) the primary documentation relating to the identity of the customer; or
(ii) a written confirmation that the required CDD provisions are satisfactorily met.

What records need to be kept?

In the case of a CIS, maintaining records is usually done by the CIS administrator on behalf of the CIS. CIS administrators must ensure that they have evidence of customer verification and where other functions are delegated to them by the CIS manager, to maintain records accordingly. The provisions are set out in Chapter 8 of the Code.

9.3 Insurance

Licensees operating in the insurance business should be constantly vigilant in deterring criminals from making use of them for the purposes of money laundering or terrorist financing. By understanding the AML/CFT risks, Licensees are in a position to determine

what can be done to control these risks and which procedures and measures can be implemented effectively and efficiently.

Licensees should put in place adequate control system to assess the risks associated with each business relationship. The concept of customer due diligence goes beyond the identification and verification of the only the policyholder – it extends to the identification of the potential risks of the whole business relationship.

Insurers, reinsurers as well as insurance service providers may refer to the guidance provided below with a view to ensure compliance with the provisions of this Code.

The principal obligation to perform CDD checks remains with each Licensee in respect of the parties with which it directly transacts, i.e. its own applicants for business.

Who should be treated as the Applicant for Business?

Where the Licensee is:	The Applicant for Business is:
an insurer	the policyholder or proposed policy holder, the insurance agent and the insurance salesperson
an insurance manager	the policyholder and the insurer
an insurance broker	the policyholder
an insurance agent	the policyholder

How and when should identity be verified?

In principle, identification and verification of policyholders and beneficial owners should take place when the business relationship with that person is established. This means that the policyholder (or its owner / controller) needs to be identified and their identity verified before, or at the very latest at the moment when, the insurance contract is concluded or when the financial service is being provided.

If the policyholder is a natural person, the Licensee should apply provisions of section 4.1.1 of the Code.

If the policyholder is a corporate body or other legal arrangement, then provisions of section 4.1.2 of the Code would apply.

Where the Licensee has not been able to complete the CDD measures prior to the conclusion of insurance contract or provision of the financial services, it must ensure that this is done in conformity with section 4.6 of the Code, where the approval of senior management must be sought and recorded in writing.

In any case, identification and verification must occur at or before the time of claims settlement, premium refunds or the time when the beneficiary intends to exercise vested rights under the policy or any other instruments.

What additional information might be requested and when?

In insurance, various transactions or 'trigger events' occur after the contract date and indicate where due diligence may be required. These trigger events include claims notification, surrender requests and policy alterations, including changes in beneficiaries.

Insurance Products

Redemptions/Surrenders

When a client redeems an investment (wholly or partially), and verification of identity has not been undertaken, it will be considered reasonable for a Licensee to establish evidence of identity without the requirement for further verification where payment is made:

- To the legal owner of the insurance product by means of a cheques crossed "Account Payee" or
- To a bank account held (solely or jointly) in the name of the legal owner of the investment
- To a bank account beneficially owned by the legal owner of the investment held with a financial institution in one of the countries listed in Appendix IV or to a Stock/Investment Exchange listed in Appendix VI at the request of the legal owner of the investment.

Switch transactions

A switch transaction involves moving the value of one insurance product to a different insurance product (from product A to product B).

A switch transaction does not give rise to a requirement of verification if it is a switch in which all of the proceeds are directly paid to another policy of insurance offered by an insurer within the same group as the Insurance Entity provided that before payment or surrender the identity of the applicant for business is fully verified.

Payments from one policy of insurance to another - for the same applicant for business

A number of insurance vehicles offer customers the facility to have payments from one policy of insurance fund the premium payments of another policy of insurance. The use of such a facility within the same group should not be seen as a new business relationship and the payments under such a facility should not be treated as a transaction that triggers the requirement of additional verification provided the identity of the applicant for business has been verified in accordance with this Code.

Savings schemes

For regular savings schemes in which money invested is used to acquire insurance policies registered in the name, or to be held to the order of a third party beneficiary, both the party

who funds the savings scheme and the third party beneficiary must be treated as applicants for business for verification of identity purposes.

Policy Cancellation Reports

The reason Policy Cancellation Reports should be maintained is to provide audit trails should the need arise to identify all policies cancelled within a specific time period.

The Reports must detail the amount of the value of cash surrender value, the currency paid, the identity of the sales agent, the actual term of the policy and reasons for cancellation.

APPENDICES

Appendix I –	Sample Internal Disclosure Form to MLRO
Appendix II –	Specimen Eligible Introducer Certificate
Appendix III –	Specimen Group Introducer Certificate
Appendix IV –	List of Equivalent Jurisdictions
Appendix V –	List of non-cooperative countries and territories and countries with deficiencies in their AML/CFT regime
Appendix VI –	Recognised, Designated, Approved Stock/Investment Exchanges
Appendix VII –	Indicators of Potentially Suspicious Transaction/Activity
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

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 III

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: …….

Registration No: ……

Signed: …….. Full Names: ……

Job Title: …….. Date: ……

Appendix IV

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. India
18. Ireland
19. Isle of Man
20. Italy
21. Japan
22. Jersey
23. Luxembourg
24. Malta
25. Netherlands (excluding Netherlands Antilles)
26. New Zealand
27. Norway
28. Portugal
29. Republic of South Africa
30. Russian Federation
31. Singapore
32. Spain
33. Sweden
34. Switzerland
35. United Kingdom
36. United States

Appendix V

List of non-cooperative countries and territories and countries with deficiencies in their AML/CFT regime

NON-COOPERATIVE COUNTRIES AND TERRITORIES

The FATF recommends that special attention should be given to business relations and transactions with persons, including companies and financial institutions, from the non-cooperative countries and territories (NCCT).

As of 13 October 2006, there are no countries and territories which have been designated as NCCTs by the FATF.

COUNTRIES WITH DEFICIENCIES IN THEIR AML/CFT REGIME

1. Iran
2. Democratic People's Republic of Korea (DPRK)
3. Bolivia
4. Cuba
5. Ethiopia
6. Ghana
7. Indonesia 8. Kenya
9. Myanmar
10. Nigeria
11. Pakistan
12. São Tomé and Príncipe
13. Sri Lanka
14. Syria
15. Tanzania
16. Thailand
17. Turkey

Licensees are required to check the FATF website for regular updates on the above countries.

Appendix VI

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
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 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) Bangalore Stock Exchange Ltd.
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)
Bhubaneswar S.E. Assoc. Ltd.*
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) Calcutta Stock Exchange Assoc. Ltd.
Cincinnati Stock Exchange
Cochin Stock Exchange Ltd.*
Copenhagen Stock Exchange (Kobenhavns Fondsbors) Delhi Stock Exchange Assoc. Ltd.
Dusseldorf Stock Exchange (Rheinisch - Westfalische Borse zu Dusseldorf)
Florence Stock Exchange (Borsa Valori di Firenze)
Frankfurt Stock Exchange (Frankfurter Wertpapierborse)
Fukuoka Stock Exchange
Gauhati Stock Exchange Ltd.*
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)
Inter-connected Stock Exchange of India*
Jaipur Stock Exchange Ltd.*
Kuala Lumpur Stock Exchange
Lille Stock Exchange
Lisbon Stock Exchange (Borsa de Valores de Lisboa)
Ludhiana Stock Exchange Assoc. Ltd.*
Luxembourg Stock Exchange (Société de la Bourse de Luxembourg SA) Lyons Stock Exchange Madras Stock Exchange Ltd.
Madrid Stock Exchange (Borsa de Valores de Madrid)
Madhya Pradesh Stock Exc Ltd. 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)
National Stock Exchange of India Ltd
New Zealand Stock Exchange
Oporto Stock Exchange (Bolsa de Valores do Porto)
Oslo Stock Exchange (Oslo Bors)
OTC Exchange of India*
Palermo Stock Exchange (Borsa Valori di Palenno)
Pune Stock Exchange Ltd.*
Rome Stock Exchange (Borsa Valori di Roma)

Stockholm Stock Exchange (Stockholm Fondbors)
Stock Exchange of Mauritius
Stuttgart Stock Exchange (Baden - Wurtembergische Wertpapierborse zu Stuttgart)
Taiwan Stock Exchange
Tel Aviv Stock Exchange
The Stock Exchange, Ahmedabad
The Stock Exchange, Mumbai
The Stock Exchange of Thailand
Trieste Stock Exchange (Borsa Valori di Trieste)
Trondheim Stock Exchange (Trondheims Bors)
Turin Stock Exchange (Borsa Valori de Torino)
Uttar Pradesh Stock Exchange*
Vadodara Stock Exchange Ltd.*
Valencia Stock Exchange (Borsa de Valores de Valencia)
Venice Stock Exchange (Borsa Valori de Venezia)
Vienna Stock Exchange
Zurich Stock Exchange (Zurcher Borse)

**All the exchanges marked are recognised by the Commission as long as they hold valid recognition from the Stock Exchange Board of India.*

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 VII

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 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 VIII

Glossary

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
applicant for business	includes any natural or legal person or arrangement – whether corporate or unincorporated - that seeks to form a business relationship or to carry out a one-off transaction with a Licensee.
associate	means – (i) in relation to a relationship with an individual – (A) a spouse, a person living "*en concubinage*" under the common law, any child or step child or any relative residing under the same roof as that person; (B) a succession in which the person has an interest; (C) a partner of that person; (ii) in relation to a relationship with any person – (A) any company in which the person directly or indirectly holds 10 per cent of the voting rights or an unlimited right to participate in earnings and in the assets upon winding up; (B) any controller of that person; (C) any trust in which the person has a substantial ownership interest or in which he fulfils the functions of a trustee or similar function; (D) any company which is a related company.
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
controller	has the same meaning as in the FS Act
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 VI.
FATF	Financial Action Task Force
FIAML Act	Financial Intelligence and Anti-Money Laundering Act 2002
FIU	Financial Intelligence Unit
FSC	Financial Services Commission
FS Act	Financial Services Act 2007
Licensee	has the same meaning as the FIAML 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
relevant Acts	has the same meaning as in the FS Act
regulations	Financial Intelligence and Anti-Money Laundering Regulations 2003

Appendix IX

Useful Websites

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