BANK OF MAURITIUS

GUIDANCE NOTES ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

FOR

FINANCIAL INSTITUTIONS

JUNE 2005

[Updated as at July 2017]

TABLE OF CONTENTS

1. INTRODUCTION

1. INTRODUCTION

1.01 The State of the Republic of Mauritius has through numerous initiatives demonstrated its firm willingness to combat money laundering and terrorist financing. On 23 December 1997, Mauritius committed itself to the 40 Recommendations of the Financial Action Task Force (FATF) and to the Mutual Evaluation procedure. Further, on 20 October 2000, Mauritius committed itself to the United Nations Minimum Performance Programme standards agreed at the Global Programme Against Money Laundering Plenary held in Cayman Islands.

1.02 On 4 June 2001, Government ratified the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, commonly known as the Vienna Convention and on 18 April 2003, Government ratified the United Nations Convention against Transnational Organised Crime, the Palermo Convention.

1.03 In June 2000, Government also enacted a legislation against money laundering, the Economic Crime and Anti-Money Laundering Act 2000 which became operative in Mauritius on 7 July 2000. The Economic Crime and Anti-Money Laundering Act 2000 captured under its umbrella, fraud and corruption. To stay in pitch with fast evolving developments in money laundering, the Economic Crime and Anti-Money Laundering Act 2000 was soon repealed and replaced by the Financial Intelligence and Anti-Money Laundering Act 2002, giving explicit powers to gather, analyse and disseminate information to a Financial Intelligence Unit (FIU). This Act is operative in Mauritius since 10 June 2002. It provides, inter alia, that financial institutions should submit suspicious transaction reports directly to the FIU whereas the practice heretofore had been for those institutions to make suspicious transaction reports to the Bank of Mauritius. The corruption component of the Economic Crime and Anti-Money Laundering Act 2000 was, however, not carried over in the Financial Intelligence and Anti-Money Laundering Act 2002. It was taken on board in the Prevention of Corruption Act 2002 which also provided for the investigation of money laundering offences to be undertaken by an Independent Commission Against Corruption created under that Act.

1.04 On 19 June 2003, Regulations (G.N. No. 79 of 2003), which are operative in Mauritius as from 21 June 2003, were promulgated under the Financial Intelligence and Anti-Money Laundering Act 2002 to provide among other things, for verification of identity and record keeping. These Regulations have, however, been amended by the Financial Intelligence and Anti-Money Laundering (Amendment) Regulations 2005 (G.N. No. 117 of 2005) and the Financial Intelligence and Anti-Money Laundering (Amendment) Regulations 2006 (G.N. No. 127 of 2006) to make better provision for, inter alia, eligible and group introducers.

1.05 Further, on 16 September 2003, an Anti-Money Laundering (Miscellaneous Provisions) Act was enacted in Parliament. The Act was the result of recommendations made by the Financial Sector Assessment Program (FSAP) mission of the International Monetary Fund and the World Bank. The Act brought certain changes to the institutional and regulatory framework which obtained in Mauritius as regards anti-money laundering.

1.06 Mauritius is a founder member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). The ESAAMLG is now an associate member of the FATF.

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

(i) The Convention on Offences and Certain Other Acts Committed on Board Aircraft was signed at Tokyo on 14 September 1963 and ratified on 5 April 1983.

(ii) The Convention on the Suppression of Unlawful Seizure of Aircraft was signed at the Hague on 16 December 1970 and ratified on 25 April 1983.

(iii) The Convention on the Suppression of Unlawful Acts against the Safety of Civil Aviation was signed at Montreal on 23 September 1971 and ratified on 25 April 1983.

(iv) The International Convention against the Taking of Hostages was signed in New York on 18 June 1980 and ratified on 17 October 1980.

(v) The Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation of 1971 was signed in Montreal on 24 February 1988 and ratified on 17 August 1989.

(vi) The International Convention for the Suppression of the Financing of Terrorism was signed on 11 November 2001 and ratified on 14 December 2004.

(vii) The International Convention for the Suppression of Terrorist Bombings was acceded on 24 January 2003.

(viii) The Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents was acceded on 24 December 2003.

(ix) The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation was acceded on 3 August 2004.

(x) The Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf was acceded on 3 August 2004.

1.08 On 19 February 2002, Parliament enacted a Prevention of Terrorism Act 2002 to combat terrorism generally. The Act is fully operative in Mauritius since 16 March 2002. Subsequently, two sets of regulations were made under that Act by the Honourable Minister responsible for the subject of national security, namely the Prevention of Terrorism (Special Measures) Regulations 2003 and the Prevention of Terrorism (Special Measures) (Amendment) Regulations 2003.

1.09 On 16 September 2003, Parliament enacted the Convention for the Suppression of the Financing of Terrorism Act to give force of law to the International Convention for the Suppression of the Financing of Terrorism.

1.10 A Combating of Trafficking in Persons Act was also enacted on 8 May 2009 effective from 30 July 2009, to

(a) give effect to the United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons;

(b) prevent and combat trafficking in persons; and

(c) protect and assist victims of trafficking.

1.11 In March 2005, Mauritius signed an Agreement with India on Cooperation to combat Terrorism.

1.12 Further, in September 2009, Government set up a Counter Terrorism Unit for terrorism monitoring under the aegis of the Prime Minister's Office. Its aim is to act as the agency of the Government of Mauritius in the prevention and combating of terrorism and related matters both locally and internationally.

1.13 Conventions and statutory instruments would remain dead letters if they are not properly enforced. The Bank of Mauritius and all stakeholders in the financial services sector have to shoulder their part of the responsibilities. Accordingly, the Bank of Mauritius, in recognition of the risks, including reputational risks, to which the laundering of the proceeds of criminal activities and the financing of terrorist activities may expose the financial sector of Mauritius and also mindful of the need to continue to maintain Mauritius as a clean jurisdiction, has, after consultation with the Mauritius Bankers Association Limited, the Association of International Banks, non-bank deposit taking institutions, cash dealers and the Financial Intelligence Unit, issued these Guidance Notes.

1.14 The Guidance Notes set out the broad parameters within which financial institutions should operate in order to ward off money laundering and terrorist financing risks. Financial institutions should, on their part, maintain updated anti-money laundering and terrorist financing deterrence policies, including regular update and training of concerned staff to keep up with new emerging typologies.

1.15 Any enquiries pertaining to these Guidance Notes should be addressed to :

The First Deputy Governor
Bank of Mauritius
Sir William Newton Street
Port Louis
Tel : 202 3962
Fax : 212 0313
e-mail : fdg@bom.mu

2. PURPOSE, APPLICATION AND STATUS OF THESE GUIDANCE NOTES

2. PURPOSE, APPLICATION AND STATUS OF THESE GUIDANCE NOTES

2.01 These Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism are issued to financial institutions by the Bank of Mauritius by virtue of powers conferred upon it by section 50(2) of the Bank of Mauritius Act 2004, section 100 of the Banking Act 2004 and section 18(1)(a) of the Financial Intelligence and Anti-Money Laundering Act 2002.

2.02 These Guidance Notes supersede the Guidance Notes issued by the Bank under cover of the Bank's letter BD 888 Vol. 3 dated 19 December 2003 and came into effect on 7 June 2005.

2.03 The Guidance Notes outline the requirements, as appropriate, of the Financial Intelligence and Anti-Money Laundering Act 2002 as amended by the Anti-Money Laundering (Miscellaneous Provisions) Act 2003, the Financial Intelligence and Anti-Money Laundering Regulations 2003 as amended by the Financial Intelligence and Anti-Money Laundering (Amendment) Regulations 2005 and the Financial Intelligence and Anti-Money Laundering (Amendment) Regulations 2006, the Prevention of Corruption Act 2002, the Prevention of Terrorism Act 2002, the Convention for the Suppression of the Financing of Terrorism Act 2003, the Prevention of Terrorism (Special Measures) Regulations 2003 and the Prevention of Terrorism (Special Measures) (Amendment) Regulations 2003.

2.04 For the purposes of these Guidance Notes and unless specified otherwise, "financial institution" shall include bank[1], non-bank deposit taking institution[2], cash dealer[3], and money lender[4] licensed by the Bank of Mauritius under the Banking Act 2004.

2.05 The Guidance Notes are a statement of the minimum standard expected of ALL financial institutions. The Guidance Notes therefore are not intended to provide an exhaustive list of systems and controls to counter money laundering and the financing of terrorism. In complying with statutory requirements and in applying the Guidance Notes, financial institutions should as far as possible adopt an appropriate and intelligent risk based approach and always consider additional measures that could be necessary to prevent its exploitation, and that of its products and services, by persons seeking either to launder money or to finance terrorism. A risk based approach –

Under the Banking Act 2004:

[1] "bank" means a company incorporated under the Companies Act, or a branch of a company incorporated abroad, which is licensed under section 7(5) of the Banking Act to carry on any of the following: banking business, Islamic banking business, private banking business.

[2] "non-bank deposit taking institution" means an institution other than a bank that has been authorised by the central bank to conduct deposit taking business.

[3] "cash dealer" means a person licensed by the central bank to carry on the business of foreign exchange dealer or money-changer. A money changer is a body corporate licensed as such under the Banking Act to carry on solely the business of (a) buying and selling of foreign currency notes, coins and travellers' cheques; (b) replacement of lost or stolen traveller's cheques; and (c) encashment under credit cards. A foreign exchange dealer is a body corporate licensed as such by the central bank to carry on the business of: (a) buying and selling foreign currency, including spot and forward exchange transactions and wholesale money market dealings; (b) a money changer; (c) money or value transfer services.

4 "moneylender" means a person, other than a bank or a non-bank deposit taking institution, whose business is that of moneylending or who provides, advertises or holds himself out in any way as providing that business, whether or not he possesses or owns property or money derived from sources other than the lending of money, and whether or not he carries on the business as a principal or as an agent.

(i) recognises that the money laundering and financing of terrorism threat to a financial institution varies across customers, countries and territories, products and delivery channels;

(ii) allows a financial institution to differentiate between customers in a way that matches its risk;

(iii) while establishing minimum standards, allows a financial institution to apply its own approach to systems and controls, and arrangements in particular circumstances; and

(iv) helps financial institutions produce a more cost effective system.

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

2.07 It is recognised that for the Guidance Notes to be effective, they need to be reviewed on a regular basis to reflect changing circumstances and experience. Revisions and updates will be communicated to all financial institutions as and when necessary.

3. MONEY LAUNDERING AND TERRORIST FINANCING

3. MONEY LAUNDERING AND TERRORIST FINANCING

PART A – ANTI-MONEY LAUNDERING

3.01 The main pieces of legislation relating to money laundering are the Financial Intelligence and Anti-Money Laundering Act 2002 as amended by the Anti-Money Laundering (Miscellaneous Provisions) Act 2003, the Financial Intelligence and Anti-Money Laundering Regulations 2003 as amended by the Financial Intelligence and Anti-Money Laundering (Amendment) Regulations 2005 and the Financial Intelligence and Anti-Money Laundering (Amendment) Regulations 2006, and the Prevention of Corruption Act 2002 [POCA].

3.02 Money laundering offences relate to the proceeds of crime generally.

WHAT IS MONEY LAUNDERING?

3.03 Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it allows them to maintain control over those proceeds and, ultimately provides them with a legitimate cover for the source of their income.

3.04 Money laundering is a global phenomenon that affects all countries to varying degrees. By its very nature it is a hidden activity and therefore the scale of the problem, and the amount of criminal money being generated either locally or globally each year, is impossible to measure accurately. However, failure to prevent the laundering of the proceeds of crime permits criminals to benefit from their actions, thus making crime a more attractive proposition.

THE NEED TO COMBAT MONEY LAUNDERING

3.05 It is vital in the fight against crime that criminals be prevented, whenever possible, from legitimising the proceeds of their criminal activities by converting funds from ‘dirty’ to ‘clean’.

3.06 The ability to launder the proceeds of criminal activity through the financial system is a key element to the success of criminal operations. Those involved in money laundering need to exploit the facilities of the world's financial sector businesses if they are to benefit from the proceeds of their activities. The unchecked use of the financial systems for this purpose has the potential to undermine individual financial institutions and, ultimately, the entire financial sector. The increased integration of the world's financial systems, the removal of barriers to the free movement of capital and the expansion of electronic banking have enhanced the ease with which criminal money can be laundered and simultaneously complicated the tracing process.

3.07 The long term success of any of the world's financial sectors depends on attracting and retaining legitimately earned funds. Criminally earned money is invariably transient in nature. It damages reputation and the integrity of banking systems and deters the honest depositor. Any person or institution that becomes involved in a money laundering scandal will risk likely prosecution, and the loss of his good market reputation.

STAGES OF MONEY LAUNDERING

3.08 The laundering process is generally accomplished in three stages, as follows, which may comprise numerous transactions by the launderers that could trigger suspicion on money laundering.

a) Placement - the physical disposal of the initial proceeds derived from illegal activity
b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity
c) Integration - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three basic steps may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminals.

3.09 Certain points of vulnerability have been identified in the laundering process, which the money launderer finds difficult to avoid and where his activities are therefore more susceptible to being recognised, specifically:

- entry of cash into the financial system
- transfers within and from the financial system.

VULNERABILITY OF FINANCIAL SECTOR BUSINESSES TO MONEY LAUNDERING

3.10 Historically, efforts to combat money laundering have to a large extent concentrated on the deposit-taking procedures of financial sector businesses where the launderer's activities are most susceptible to recognition. Criminals have, however, over the recent years recognised that cash payments made into financial sector businesses can often give rise to additional enquiries. Other means have therefore been sought to convert the illegally earned cash or to mix it with legitimate cash earnings before it enters the financial system, thus making it harder to detect at the placement stage. These include the use of ‘smart’ cards and wire transfers which are not easily amenable to tracking. Financial institutions should, accordingly, consider the money laundering risks posed by the products and services they offer, particularly where there is no face-to-face contact with the customer.

3.11 All financial institutions, as providers of a wide range of money transmission, are vulnerable to being used in the layering and integration stages of money laundering as well as the placement stage. Electronic funds transfer systems increase the vulnerability by enabling the cash deposits to be switched rapidly between accounts in different names and different jurisdictions.

3.12 Some financial institutions will additionally be susceptible to the attention of the more sophisticated criminal organisations and their 'professional money launderers'. Such organisations, possibly under the disguise of front companies and nominees, will create large scale but false international trading activities in order to move their illicit monies from one country to another. They will create the illusion of international trade using falsely inflated invoices to generate apparently legitimate international wire transfers, and will use falsified bogus letters of credit to confuse the trail further. Many of the front companies may even approach their bankers for credit in order to fund the business activity. Financial institutions offering international trade services should be on their guard for laundering by these means.

THE FORTY RECOMMENDATIONS OF THE FINANCIAL ACTION TASK FORCE (FATF)

3.13 The international standard setter with respect to money laundering is the Financial Action Task Force (FATF). The FATF was established by the G-7 Summit in Paris in July 1989. In 1990, it issued its Forty Recommendations setting out the basic framework for anti-money laundering efforts. The Forty Recommendations were first revised in 1996 and then in June 2003, to take into account changes in money laundering methods, techniques and trends that have developed as counter-measures to combat this crime and again in February 2012[5] following the revision of the FATF Standards in the document entitled *"International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation".* The FATF Standards aims at strengthening global safeguards and further protect the integrity of the financial system.

PART B - TERRORIST FINANCING

3.14 The main pieces of legislation relating to terrorist financing are the Convention for the Suppression of the Financing of Terrorism Act, the Prevention of Terrorism Act 2002, the Prevention of Terrorism (Special Measures) Regulations 2003 (G.N. No. 14 of 2003), the Prevention of Terrorism (Special Measures) (Amendment) Regulations 2003 (GN No. 36 of 2003) and the Financial Intelligence and Anti-Money Laundering Act 2002.

ENHANCING EXISTING DUE DILIGENCE REQUIREMENTS

3.15 Terrorist activities and the means that are used to further those activities require financing and wittingly or unwittingly the services of financial institutions may be used to hide or move terrorist funds.

3.16 While financial gain is generally the objective of other types of criminal activities, the goal of terrorism may be different, but terrorists still require financial support in order to achieve their aims. A successful terrorist group, like any criminal organisation, is therefore necessarily one that is able to build and maintain an effective financial infrastructure. For this it must develop sources of funding, a means of laundering those funds and then finally a way to ensure that the funds can be used to obtain material and other logistical items needed to commit terrorist acts.

[5] The FATF Recommendations issued in February 2012 are available at the website address of the FATF www.fatf-gafi.org.

3.17 Financial institutions should, therefore, protect themselves from being used as a conduit for such activities and make use of their already existing due diligence requirements, along with current policies and procedures on money laundering and enhance them where necessary to detect transactions that may involve terrorist funds. Financial institutions should review their practices in this area as part of their general internal and external audit processes. Financial institutions are encouraged to consider the risks identified by the FATF in its Report "Emerging Terrorist Financing Risks" issued in October 2015, when reviewing their policies and procedures and due diligence requirements. They should pay special attention to the terrorist financing methods and techniques identified in the Report and enhance their systems and controls accordingly.

SOURCES OF TERRORIST FUNDS

3.18 Terrorist financing may be derived from two primary sources, although there are other sources which are no less important. The first major source is the financial support provided by States or organisations with large enough infrastructures to collect funds and then make them available to terrorist organisations and also by individuals with sufficient financial means.

3.19 The second major source of funds for terrorist organisations is income derived directly from various "revenue-generating" activities. As with criminal organisations, a terrorist group's income may be derived from crime or other unlawful activities such as large-scale smuggling, various types of fraud, thefts and robbery, and narcotics trafficking.

3.20 Funding of terrorist groups may, unlike criminal organisations, however, also include income derived from legitimate sources such as donations or from a combination of lawful and unlawful sources. Indeed, this funding from legal and apparently legitimate sources is a key difference between terrorist groups and traditional criminal organisations. The FATF has highlighted that several law enforcement investigations and prosecutions have found a nexus between a commercial enterprise, including used car dealerships and restaurant franchises, and terrorist organisations, where revenue from the commercial enterprise was being routed to support a terrorist organization.

3.21 Community solicitation and fundraising appeals are one very effective means of raising funds to support terrorism. Often such fundraising is carried out in the name of organisations having the status of a charitable or relief organisation. In many cases, the charities to which donations are given are in fact legitimate in that they do engage in some of the work they purport to carry out. Most of the members of the organisation, however, have no knowledge that a portion of the funds raised by the charity is being diverted in a distinct pattern to terrorist causes. Some of the specific fundraising methods might include: collection of membership dues and/or subscriptions; sale of publications; cultural and social events; door-to-door solicitation within the community; appeals to wealthy members of the community; and donations of a portion of their personal earnings.

LAUNDERING OF TERRORIST RELATED FUNDS

3.22 The methods used by terrorists and their associates to generate funds from illegal sources differ little from those used by traditional criminal organisations. Although funding from legitimate sources need not be laundered, there is nevertheless often a need for terrorists to obscure or disguise links between it and its legitimate funding sources. It follows then that terrorists must find ways to launder these funds in order to be able to use them without drawing the attention of authorities. In examining terrorist related financial activity, FATF experts have concluded that terrorists and their support organisations generally use the same methods as criminal groups to launder funds. Some of the particular methods detected with respect to various terrorist groups include: cash smuggling, deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments (travellers' cheques, bank cheques, money orders), use of credit or debit cards, and wire transfers. The terrorist's ultimate aim is not to generate profit from his fundraising mechanisms but to obtain resources to support his operations. Thus, the direction taken by fund transfers would be particularly relevant to the tracking down of terrorist financing. A view may be taken in this regard on the basis of repetitive similar transactions either from a sole account or from a number of accounts maintained in the same institution by different parties.

3.23 When terrorists obtain their financial support from legal sources (donations, sales of publications, etc.), there are certain factors that make the detection and tracing of these funds more difficult. For example, charities or non-profit organisations and other legal entities have been cited as playing an important role in the financing of some terrorist groups. At first sight, the apparent legal source of this funding may mean that there are few, if any, indicators that would make an individual financial transaction or series of transactions stand out as linked to terrorist activities.

3.24 Other important aspects of terrorist financing that make its detection more difficult are the size and nature of the transactions involved. Several FATF experts have mentioned that the funding needed to mount a terrorist attack does not always call for large sums of money, and the associated transactions are usually not complex and many involve the movement of small sums through wire transfers.

3.25 Enhanced due diligence techniques are therefore required for tracking down terrorist financing.

3.26 Terrorist financing, while an offence in itself, is also a predicate offence for money laundering.

THE NINE SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING

3.27 In October 2001 the FATF expanded its mandate, which was until then limited to money laundering, to deal with the issue of the financing of terrorism, and took the important step of creating the Eight Special Recommendations on Terrorist Financing. These Recommendations contain a set of measures aimed at combating the funding of terrorist acts and terrorist organisations, and are complementary to the Forty Recommendations.

3.28 Further, in October 2004 the FATF added a key element to the world's counter-terrorist financing defences by issuing a new measure, Special Recommendation IX on Cash Couriers, which calls on countries to stop cross-border movements of currency and monetary instruments related to terrorist financing and money laundering and confiscate such funds.

3.29 In February 2012, the FATF's nine Special Recommendations on terrorist financing have been integrated fully within the Forty Recommendations, reflecting both the fact that terrorist financing is a long-standing concern, and the close connections between anti-money laundering measures and measures to counter the financing of terrorism. [6]

PROLIFERATION FINANCING

3.30 The issue of proliferation[7] received international attention for several years. A number of international conventions provide for measures to detect and prohibit proliferation, especially with regard to nuclear materials (such as the Nuclear Non-Proliferation Treaty). These treaties do not, however, consider the aspect of financing proliferation. In 2004, the UN Security Council issued Resolution 1540, requiring states to put in place a number of measures in order to prevent the proliferation of nuclear, chemical or biological weapons. Subsequently, the FATF started in 2007 to consider the threats related to proliferation financing and its interconnection with terrorism and terrorism financing.

3.31 The interconnection is based on the fact that proliferation might be a means for supporting the undertaking of terrorist activities. Its disruption is therefore essential for the prevention of terrorist acts. Moreover, the practical undertaking of proliferation financing often uses the same channels as terrorist financing. Measures to be applied in order to disrupt proliferation financing would therefore often be similar to the measures applied to counter terrorist financing.

3.32 Such measures are included in Recommendation 7 of the revised 2012 FATF Recommendations. It requires countries to put in place to implement the UNSC Resolutions concerning the prevention, suppression and disruption of proliferation of weapon of mass destruction (WMD) and its financing.

---

[6] The FATF Standards issued in February 2012 are available at the website address www.fatf-gafi.org

7 The FATF defines "proliferation" as the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials. This could include, inter alia, technology, goods, software, services or expertise.

3.33 The FATF has developed a working definition for financing of proliferation as set out in *Combating Proliferation Financing: A Status Report on Policy Development and Consultation*[8]*:*

"Financing of proliferation" refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

3.34 The United Nations Security Council Resolution ("UNSCR") has designated certain individuals and entities involved in the proliferation of weapons of mass destruction and its financing. The relevant information and full listings of persons designated by UNSCRs may be found on the UN website[9].

3.35 Financial institutions should rely on its CDD measures (including screening measures) to detect and prevent proliferation financing activities and transactions. It is important to ensure that name screening by financial institutions is performed against the latest UN listings as they are updated from time to time. Financial institutions should have in place policies, procedures and controls to continuously monitor the listings and take necessary follow-up action within a reasonable period of time, not to proceed with the transaction and to immediately report the matter to the Bank.

3.36 Financial institutions should also have policies and procedures to detect attempts by its employees or officers to circumvent the above requirement by, namely —

(a) omitting, deleting or altering information in payment messages for the purpose of avoiding detection of that information by the financial institution itself or other institutions involved in the payment process; and

(b) structuring transactions with the purpose of concealing the involvement of designated persons.

3.37 The financial institution should have policies and procedures to prevent such attempts, and take appropriate measures against such employees and officers.

Potential Indicators of Proliferation Financing

3.38 Financial institutions should develop indicators that would alert it to customers and transactions (actual or proposed) that are possibly associated with proliferation financing-related activities, including indicators such as whether —

(a) the customer is vague and resistant to providing additional information when asked;

(b) the customer's activity does not match its business profile or the end-user information does not match the end-user's business profile;

---

[8] available at http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf

9 https://www.un.org/sc/suborg/en/s/res/1737-(2006) and https://www.un.org/sc/suborg/en/sanctions/1718.

(c) the transaction involves designated persons;

(d) the transaction involves higher risk countries or jurisdictions which are known to be involved in proliferation of weapons of mass destruction or proliferation financing activities;

(e) the transaction involves other financial institutions with known deficiencies in AML/CFT controls or controls for combating proliferation financing;

(f) the transaction involves possible shell companies (e.g. companies that do not have a high level of capitalisation or display other shell company indicators);

(g) the transaction involves containers whose numbers have been changed or ships that have been renamed;

(h) the shipment of goods takes a circuitous route or the financial transaction is structured in a circuitous manner;

(i) the transaction involves the shipment of goods inconsistent with normal geographic trade patterns (e.g. the country involved would not normally export or import such goods);

(j) the transaction involves the shipment of goods incompatible with the technical level of the country to which goods are being shipped (e.g. semiconductor manufacturing equipment shipped to a country with no electronics industry); or

(k) there are inconsistencies in the information provided in trade documents and financial flows (e.g. in the names, companies, addresses, ports of call and final destination).

3.39 The FATF has also provided guidance on measures to combat proliferation financing and it is recommended that financial institutions refer to the FATF website (www.fatf-gafi.org) for additional information.

4. THE LEGISLATIVE FRAMEWORK OF MAURITIUS

4. THE LEGISLATIVE FRAMEWORK OF MAURITIUS

PART A - ANTI-MONEY LAUNDERING

THE FINANCIAL INTELLIGENCE AND ANTI-MONEY LAUNDERING ACT 2002

4.01 The first specific legislation to address the risks of money laundering in Mauritius was known as the Economic Crime and Anti-Money Laundering Act 2000.

4.02 The Economic Crime and Anti-Money Laundering Act was repealed on 1 April 2002 on the coming into force of the Prevention of Corruption Act 2002 and another legislation against money laundering known as the Financial Intelligence and Anti-Money Laundering Act 2002 was enacted by Parliament on 27 February 2002 and came into force on 10 June 2002. The Financial Intelligence and Anti-Money Laundering Act 2002 was itself, in the light of the assessment of our jurisdiction made by the joint IMF/World Bank Financial Sector Assessment Program Mission, amended by the Anti-Money Laundering (Miscellaneous Provisions) Act 2003. The Financial Intelligence and Anti-Money Laundering Act 2002 as amended by the Anti-Money Laundering (Miscellaneous Provisions) Act 2003 is hereinafter referred to as the FIAML.

THE TRANSITION FROM THE ECONOMIC CRIME AND ANTI-MONEY LAUNDERING ACT 2000 TO THE FIAML

4.03 Under the Economic Crime and Anti-Money Laundering Act 2000, financial institutions were required to report suspicious transactions of money laundering to the Bank of Mauritius. Under the FIAML, all suspicious transactions of money laundering are now required to be reported directly to the Financial Intelligence Unit.

4.04 The Economic Crime and Anti-Money Laundering Act 2000 provided for the investigation of money laundering offences to be carried out by the Economic Crime Office which was also created under that Act. Responsibility for investigations of money laundering offences has, under the Prevention of Corruption Act 2002, been vested in the Independent Commission Against Corruption.

4.05 The FIAML provides a complete mechanism for the dissemination of information to other regulatory and law enforcement bodies and contains provisions for regulatory bodies to report to the Financial Intelligence Unit suspicious transactions which they come to know in the course of their supervisory functions, a procedure which was not available under the Economic Crime and Anti-Money Laundering Act 2000.

4.06 The definition of suspicious transaction in the FIAML expressly mentions that it includes transactions related to terrorism.

THE FINANCIAL INTELLIGENCE UNIT (FIU)

4.07 Financial institutions are required to report suspicious transactions to the Financial Intelligence Unit.

4.08 The Financial Intelligence Unit was established on 10 June 2002 under the FIAML.

4.09 The Financial Intelligence Unit is headed by a Director and is administered by a Board which consists of a chairperson and two other members.

4.10 The FIU is the central agency in Mauritius responsible for receiving, requesting, analysing and disseminating to the investigatory and supervisory authorities disclosures of financial information –

(a) concerning suspected proceeds of crime and alleged money laundering offences;

(b) required by or under any enactment in order to counter money laundering; or

(c) concerning the financing of any activities or transactions related to terrorism.

4.11 The Financial Intelligence Unit is essentially an intelligence-gathering entity which collects and compiles information on money laundering and terrorism. It acts as the central repository of financial information in connexion with suspected or actual money laundering activities and terrorist financing.

4.12 The Financial Intelligence Unit became a member of the EGMONT Group on 23 July 2003 and is the representative of African FIUs on the EGMONT Committee. The Financial Intelligence Unit benefits from mutual assistance in money laundering matters from members of the Group. The EGMONT Group, which at present regroups Financial Intelligence Units from 151 countries, has the objective of improving support to its members' national anti-money laundering programmes which involves, inter alia, the sharing of financial intelligence information.

4.13 The address of the Financial Intelligence Unit is currently :

The Director
Financial Intelligence Unit
7th Floor, Ebène Heights
34, Ebène Cybercity
Ebène
Republic of Mauritius

Telephone: (230) 454 1423
Fax: (230) 466 2431
Email: fiu@fiumauritius.org

MONEY LAUNDERING OFFENCES

4.14 In the interpretation section of the FIAML, money laundering is defined as an offence under Part II of the Act.

Under Part II of the FIAML, the following offences are money laundering offences:-

"3. Money laundering

(1) Any person who -

(a) engages in a transaction that involves property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime; or

(b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime,

where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime, shall commit an offence.

(2) A bank[10], financial institution[11], cash dealer or member of a relevant profession or occupation that fails to take such measures as are reasonably necessary to ensure that neither it nor any service offered by it, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence or the financing of terrorism shall commit an offence.

(3) Reference to concealing or disguising property which is, or in whole or in part, directly or indirectly, represents, the proceeds of any crime, shall include concealing or disguising its true nature, source, location, disposition, movement or ownership of or rights with respect to it.

4. Conspiracy to commit the offence of money laundering

Without prejudice to section 109 of the Criminal Code (Supplementary) Act, any person who agrees with one or more other persons to commit an offence specified in section 3(1) and (2) shall commit an offence.

---

[10] 'bank' as defined under the Financial Intelligence and Anti-Money Laundering Act 2002, has the same meaning as under the Banking Act 2004 and includes a moneylender, a credit union, any person carrying on non-bank deposit taking business licensed under the Banking Act.

[11] "Financial institution" as defined under the Financial Intelligence and Anti-Money Laundering Act 2002 does not have the same meaning as under the Banking Act 2004. Under the Financial Intelligence and Anti-Money Laundering Act 2002, "financial institution" means an institution, or a person, licensed or registered or required to be licensed or registered under –
(a) section 14 or 77 of the Financial Services Act;
(b) the Insurance Act; or
(c) the Securities Act.

5. Limitation of payment in cash

(1) Notwithstanding section 37 of the Bank of Mauritius Act 2004, but subject to subsection (2), any person who makes or accepts any payment in cash in excess of 500,000 rupees or an equivalent amount in foreign currency, or such amount as may be prescribed, shall commit an offence.

(2) Subsection (1) shall not apply to an exempt transaction."

4.15 The Intermediate Court has jurisdiction to try any offence under the Act or regulations made thereunder and may, on conviction, in addition to any penal sanction that it may impose, namely a fine not exceeding 2 million rupees and to penal servitude for a term not exceeding 10 years, order the forfeiture of assets. Any property belonging to or in the possession or under the control of, any person who is convicted of a money laundering offence is deemed to be derived from a crime and the Court may order its forfeiture.

4.16 The term 'crime' as defined in the Act

(a) means an offence punishable by -
  (i) penal servitude;
  (ii) imprisonment for a term exceeding 10 days;
  (iii) a fine exceeding 5,000 rupees;

(b) includes an activity carried on outside Mauritius and which, had it taken place in Mauritius, would have constituted a crime; and

(c) includes an act or omission which occurred outside Mauritius but which, had it taken place in Mauritius, would have constituted a crime.

SUSPICIOUS TRANSACTIONS

4.17 The definition of suspicious transaction in the Act is as follows :-

"Suspicious transaction" means a transaction[12] 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 a crime;

(b) is made in circumstances of unusual or unjustified complexity;

---

[12] "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.

(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.

4.18 The standard imposed on suspicion and also on money laundering offences is the objective standard. Accordingly, if the circumstances warranted the appropriate officer of a financial institution to have reasonable suspicion but he did not actually suspect, the offence may be committed. Those officers should therefore be very familiar with the 'Know Your Customer Principle', which is dealt with under section 6 of these guidance notes.

LIMITATION ON PAYMENT IN CASH AND EXEMPT TRANSACTIONS

Limitation on Payment in Cash

4.19 With a view to secure an audit trail and as a preventive measure against the laundering of the proceeds of crime, a limit on cash payments has been imposed under the Act. Accordingly, apart from certain exempt transactions, described below, transactions in cash in excess of 500,000 rupees are prohibited altogether.

Exempt Transactions

4.20 Exempt transactions are transactions for which the limit of 500,000 rupees does not apply and are generally transactions between (i) the Bank of Mauritius and any other person, (ii) a bank and another bank, (iii) a bank and a financial institution, (iv) a bank or a financial institution and a customer, where (a) the transaction does not exceed an amount that is commensurate with the lawful activities of the customer, and 1) the customer is, at the time the transaction takes place, an established customer of the bank or financial institution; and 2) the transaction consists of a deposit into, or withdrawal from, an account of a customer with the bank or financial institution; or b) the chief executive officer or chief operating officer of the bank or financial institution, as the case may be, personally approves the transaction in accordance with any guidelines, instructions or rules issued by a supervisory authority in relation to exempt transactions; or (v) between such other persons as may be prescribed.[13]

[13] For the purposes of this paragraph, 'financial institution' has the same meaning as under the Financial Intelligence and Anti-Money Laundering Act 2002, i.e. "financial institution" means an institution, or a person, licensed or registered or required to be licensed or registered under –
(a) section 14, 77, 77A or 79A of the Financial Services Act;
(b) the Insurance Act;
(c) the Securities Act; or
(d) the Captive Insurance Act 2015.

OBLIGATIONS OF FINANCIAL INSTITUTIONS

4.21 In order to combat money laundering and the financing of terrorism, every financial institution must take measures to ensure that neither it nor any services offered by it is capable of being used to commit or facilitate the commission of a money laundering offence.

4.22 In addition, financial institutions have, in terms of the FIAML, a duty to verify the true identity of the customers and other persons with whom they conduct transactions. Under the Banking Act 2004, financial institutions may open accounts for deposits of money only where they are satisfied that they have established the identity of the person in whose name the funds are to be credited.

4.23 Financial institutions are also required to adopt internal reporting procedures, including the appointment of a Money Laundering Reporting Officer and to implement internal controls and other procedures to combat money laundering and the financing of terrorism.

REPORTING REQUIREMENTS

Lodging of Reports of Suspicious Transactions

4.24 Every financial institution must under section 14 of the FIAMLA, as soon as practicable, but not later than 15 working days, make a report to the FIU of any transaction which the financial institution has reason to believe may be a suspicious transaction. The FIU has devised a form to that effect. Financial institutions are required to use the form which is available at the FIU to report suspicious transactions.

Contents of the Report

4.25 Every report lodged with the Financial Intelligence Unit must include the following –

- The identification of the party or parties to the transaction;
- The amount of the transaction, the description of the nature of the transaction and all the circumstances giving rise to the suspicion;
- The business relationship of the suspect to the financial institution;
- Where the suspect is an insider, any information as to whether the suspect is still affiliated with the financial institution;
- Any voluntary statement as to the origin, source or destination of the proceeds;
- The impact of the suspicious activity on the financial soundness of the reporting institution or person; and
- The names of all the officers, employees or agents dealing with the transaction.

Duty of the FIU to provide feedback

4.25A Following the receipt of a report, the FIU will provide a feedback in writing on the outcome of the report to the relevant financial institution and to the Bank of Mauritius.

Inadmissibility of STR as evidence

4.25B No report of a suspicious transaction is admissible as evidence in any proceedings.

Powers of the FIU to request additional information, pursuant to a Suspicious Transaction Report made to it.

4.26 Following a Suspicious Transaction Report made to the FIU by a financial institution, the Director of the FIU is empowered to request additional information from the financial institution in respect of that suspicious transaction and also from any other financial institution who is or appears to be involved in the transaction.

4.26A Where a financial institution receives a request for further information from the Director of the FIU, it shall, as soon as practicable, but not later than 15 working days, furnish the FIU with the requested information.

4.27 This power of the Director of the FIU is, however, subject to two provisos:-

(i) the additional information may be sought only for the purposes of assessing whether the information should be disseminated to investigatory or supervisory authorities.

(ii) the additional information sought should be in relation to the suspicious transaction report made by the financial institution.

Legal Consequences of Reporting

Customer Confidentiality

4.28 The legislation protects those reporting or receiving reports of suspicious transactions of money laundering or additional information thereon from claims in respect of any alleged breach of client confidentiality or for disclosure of confidential information.

4.29 The legislation also provides immunity from suit for reports made in good faith, even though the suspicion ultimately proves not to be well founded.

Tipping Off

4.30 The Act expressly prohibits a person who is directly or indirectly involved in the reporting of a suspicious transaction from divulging to any person involved in the transaction or to any unauthorised third party, that the transaction has been reported. In the event that a person is found guilty of tipping off he may, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

4.31 In practice, preliminary enquiries in respect of an applicant for business, either to obtain additional information to confirm true identity, or to ascertain the source of funds or the precise nature of the transaction being undertaken, will not trigger a tipping off offence. Great care should, however, be taken where a suspicious transaction has already been reported and it becomes necessary to make further enquiries, to ensure that customers do not become aware that their names have been brought to the attention of the FIU. In cases where the financial institution forms a suspicion of money laundering or terrorist financing, and the financial institution reasonably believes that performing the CDD process will tip-off the customer, the financial institution shall not pursue the CDD process and shall instead file an STR with the FIU.

Failure to Report

4.32 Any financial institution or any director or employee thereof who knowingly or without reasonable excuse fails to (i) supply any information requested by the FIU under section 13(2) or 13(3) of the FIAMLA within the date specified in the request; (ii) make a report under section 14 of the FIAMLA; or (iii) verify, identify or keep records, registers or documents, as required under section 17 of FIAMLA shall on conviction be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Sanctions

4.33 Where it appears to the Bank of Mauritius that any financial institution subject to its supervision has failed to comply with any requirement imposed by FIAML or any regulations applicable to that financial institution and that the failure is caused by a negligent act or omission or by a serious defect in the implementation of any such requirement, the Bank of Mauritius, in the absence of any reasonable excuse, may -

(a) in the case of a bank, proceed against it under sections 11 and 17 of the Banking Act 2004 on the ground that it is carrying on business in a manner which is contrary to the interest of the public;

(b) in the case of a cash dealer or a person licensed to carry on deposit taking business, proceed against him under sections 16 and 17 of the Banking Act 2004 on the ground that he is carrying on business in a manner which is contrary to the interest of the public.

4.33A The Bank of Mauritius may, for the sole purpose of discharging its compliance function, request the FIU to provide it with a copy of the suspicious transaction report made under section 14(1) of the FIAMLA.

THE FINANCIAL INTELLIGENCE AND ANTI-MONEY LAUNDERING REGULATIONS 2003

4.34 The Financial Intelligence and Anti-Money Laundering Regulations 2003 were enacted on 19 June 2003 and became operative on 21 June 2003. These Regulations have, however, been amended by the Financial Intelligence and Anti-Money Laundering (Amendment) Regulations 2005 and the Financial Intelligence and Anti-Money Laundering (Amendment) Regulations 2006.

4.35 The Regulations as amended set out the circumstances in which verification of identity shall be carried out, the basic documents required, requirements as to record keeping, the adoption of internal reporting procedures including the identification and appointment of a Money Laundering Reporting Officer, the implementation of internal controls and other procedures for combating money laundering and the financing of terrorism, as well as reliance by financial institutions on eligible and group introducers.

THE PREVENTION OF CORRUPTION ACT 2002

4.36 The Prevention of Corruption Act 2002 was enacted on 27 February 2002 and became operative on 1 April 2002.

4.37 The Prevention of Corruption Act 2002 creates an Independent Commission Against Corruption which is vested under the Act with powers to, inter alia, investigate money laundering offences.

4.38 The Prevention of Corruption Act 2002 also provides among other things for the Independent Commission Against Corruption to co-operate with all other statutory corporations which have as object the betterment of the social and economic life of Mauritius and international institutions and with international institutions and agencies involved in the fight against money laundering.

PART B – TERRORIST FINANCING

THE CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM ACT 2003

4.39 The suppression of the financing of terrorism which was formerly dealt with under the Prevention of Terrorism Act 2002 is now addressed under the Convention for the Suppression of the Financing of Terrorism Act 2003. Sections 11, 13 and 14 of the Prevention of Terrorism Act 2002 in that respect have been repealed by the Convention for the Suppression of the Financing of Terrorism Act 2003. The offences relating to the financing of terrorism created in the Convention for the Suppression of the Financing of Terrorism Act 2003 are in line with the International Convention for the Suppression of the Financing of Terrorism.

4.40 The offence regarding the financing of terrorism created in the Act is as follows:-

4. Financing of terrorism

(1) Any person who, by any means whatsoever, wilfully and unlawfully, directly or indirectly, provides or collects funds[14] with the intention or knowledge that it will be used, or having reasonable grounds to believe that they will be used, in full or in part, to commit in Mauritius or abroad -

(a) an offence in breach of sections 4, 5, 6 and 6A of the Civil Aviation (Hijacking and Other Offences) Act and section 12 of the Prevention of Terrorism Act 2002; or

(b) an act of terrorism,

shall commit an offence.

(2) For an act to constitute an offence under subsection (1), it shall not be necessary that the funds were actually used to carry out the offence in breach of sections 4,5,6 and 6A of the Civil Aviation (Hijacking and Other Offences) Act and section 12 of the Prevention of Terrorism Act 2002 an act of terrorism, as the case may be.

(3) Any person who commits an offence under subsection (1) shall, on conviction, be liable to penal servitude for a term of not less than 3 years.

4.41 The Court is empowered under the Act to order the forfeiture of funds of a convicted person.

THE PREVENTION OF TERRORISM ACT 2002

4.42 The Prevention of Terrorism Act 2002 (POTA) was enacted on 19 February 2002 and is fully effective in the Republic of Mauritius as from 16 March 2002.

4.43 The Act proscribes terrorism in general and empowers our legal system to adequately deal with the phenomenon of terrorism. The Act, inter alia, contains provisions for -

(a) the prevention, suppression and combating of terrorism[15];

---

[14] "Funds", for the purposes of the Convention for the Suppression of the Financing of Terrorism Act 2003,
- (a) means assets of every kind, whether tangible or intangible, movable or immovable, however acquired;
- (b) includes legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including but not limited to, bank credits, travellers' cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit.

[15] Under the Prevention of Terrorism Act 2002, Acts of Terrorism are defined as acts which :-
- (a) may seriously damage a country or an international organisation; and
- (b) is intended or can reasonably be regarded as having been intended to-
  - (i) seriously intimidate a population;
  - (ii) unduly compel a Government or an international organisation to perform or abstain from performing any act;
  - (iii) seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation; or
  - (iv) otherwise influence such government, or international organisation; and

(b) new offences relating to terrorism generally;

(c) reinforcing intelligence gathering, investigatory and enforcement measures for the above; and

(d) implementing the international commitments of the Republic of Mauritius in respect of terrorism.

4.44 Section 15 of the Act, reproduced hereunder, is of particular relevance, the more so as it deals with terrorist property which includes money.

15. Dealing in terrorist property

(1) Any person who enters into, or becomes concerned in, an arrangement which facilitates the retention or control by, or on behalf of, another person of terrorist property[16], in any manner, including -

(a) by concealment;
(b) by removal from the jurisdiction; or
(c) by transfer to any other person,

shall commit an offence.

(2) It shall be a defence for a person charged under subsection (1) to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.

4.45 The Commissioner of Police may apply to the Judge in Chambers for the tracking and attachment of terrorist property.

(c) involves or causes, as the case may be-
(i) attacks upon a person's life which may cause death;
(ii) attacks upon the physical integrity of a person;
(iii) kidnapping of a person;
(iv) extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property, likely to endanger human life or result in major economic loss;
(v) the seizure of an aircraft, a ship or other means of public or goods transport;
(vi) the manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;
(vii) the release of dangerous substance, or causing of fires, explosions or floods, the effect of which is to endanger human life;
(viii) interference with or disruption of the supply of water, power or any other fundamental natural resource, the effect of which is to endanger life.

[16] Under the Prevention of Terrorism Act 2002, "terrorist property" means property which -
(a) has been, is being, or is likely to be used for any act of terrorism;
(b) has been, is being, or is likely to be used by a proscribed organisation;
(c) is the proceeds of an act of terrorism; or
(d) is gathered for the pursuit of, or in connection with, an act of terrorism.

PREVENTION OF TERRORISM (SPECIAL MEASURES) REGULATIONS 2003

4.46 The Prevention of Terrorism (Special Measures) Regulations 2003 were enacted on 25 January 2003 and became operative on the same date to cater for, among other things, the freezing of funds of terrorists. The definition of "funds" in those regulations was similar to the definition of "funds" in the Convention for the Suppression of the Financing of Terrorism Act 2003. On 19 March 2003, however, the definition of "funds" in those regulations was amended by the Prevention of Terrorism (Special Measures) (Amendment) Regulations 2003 to reflect certain exemptions contained in United Nations Security Council Resolution 1452 with regard to payments for basic necessities of terrorists. Those exemptions are contained in Section (b) of the definition of "funds", reproduced hereunder.

"funds"

(a) means assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form including electronic or digital, including title to, or interest in, such assets, including, but not limited to, bank credit, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit;

(b) does not include funds and other financial assets or economic resources that have been determined by the Minister to be –

(i) necessary for basic expenses, including payments for foodstuffs, rent or mortgage, medicines and medical treatment, taxes, insurance premiums, and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services, or fees or service charges for routine holding or maintenance of frozen funds, other financial assets or economic resources, after notification to the Committee of the intention to authorize, where appropriate, access to such funds, assets or resources and, in the absence of a negative decision by the Committee within 48 hours of such notification;

(ii) necessary for extraordinary expenses, provided that such determination has been notified to, and approved by, the Committee.

4.47 Regulations 7 and 8 of the Prevention of Terrorism (Special Measures) Regulations 2003, as amended by the Prevention of Terrorism (Special Measures) (Amendment) Regulations 2003, with respect to, inter alia, dealing in terrorist property or funds, provide as follows :-

"7. (1) No person shall -

(a) deal, directly or indirectly, in any property that is owned or controlled by or on behalf of any listed terrorist,

including funds derived or generated from property owned or controlled, directly or indirectly, by any listed terrorist;

(b) enter into or facilitate, directly or indirectly, any financial transaction related to a dealing in property referred to in sub-paragraph (a); or

(c) provide any financial or other related services in respect of any property referred to in sub-paragraph (a) to, or for the benefit of, or on the direction or order of, any listed terrorist.

(2) Reference in paragraph (1) to a listed terrorist shall be deemed to include reference to an entity owned or controlled by any listed terrorist.

8. (1) No person shall -

(a) make available any funds or other financial assets or economic resources; or
(b) make available any financial or other related services for the benefit of any listed terrorist.

(2) Reference in paragraph (1) to a listed terrorist shall be deemed to include reference to -

(a) any entity owned or controlled by any listed terrorist; or

(b) any person or entity acting on behalf, or at the direction of any listed terrorist or of any entity owned or controlled by any listed terrorist."

4.48 A listed terrorist has been defined in the regulations as an international terrorist group or a suspected international terrorist. In this respect, the Bank is, on the publication in the Government Gazette of a declaration by the Prime Minister listing those suspected international terrorists or international terrorist groups, empowered to direct by notice that funds and property held by financial institutions for those listed terrorists be frozen and to subsequently refer the matter to the police for investigation.

THE FIAML COMPLEMENTS THE PREVENTION OF TERRORISM ACT 2002, REGULATIONS MADE THEREUNDER AND THE CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM ACT 2003

4.49 The Convention for the Suppression of the Financing of Terrorism Act 2003, the Prevention of Terrorism Act 2002 and regulations made thereunder are further complemented by the FIAML. Under the FIAML, dealings in the proceeds of any crime are money laundering offences. Accordingly, the laundering of funds involved in the offences contained in the Convention for the Suppression of the Financing of Terrorism Act 2003, the POTA and regulations made thereunder would also be a money laundering offence under the FIAML.

4.50 Under the FIAML, a suspicious transaction is defined as a transaction which, inter alia, 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 a crime.

4.51 Section 10 of the FIAML further provides that the FIU shall be the central agency in the Republic of Mauritius responsible for receiving, requesting, analysing and disseminating to the investigatory and supervisory authorities disclosures of financial information, inter alia, concerning the financing of any activities or transactions related to terrorism.

PART C – ASSET RECOVERY

THE ASSET RECOVERY ACT 2011 AS AMENDED

4.52 The Asset Recovery Act (the Act) was passed by the National Assembly on 5 April 2011 and became operative on 1 February 2012 upon proclamation. The Act has subsequently been amended by the Asset Recovery (Amendment) Act 2012 in November 2012 and the Asset Recovery (Amendment) Act 2015 which, however, came into operation on 26 January 2016.

4.53 The Act prescribes the procedure to enable the State to recover assets which are proceeds or instrumentalities of crime or terrorist property, (i) where a person has been convicted of an offence (i.e. conviction based confiscation) or (ii) where there has been no prosecution but it can be proved on a balance of probabilities that property represents proceeds or instrumentalities of an unlawful activity, or terrorist property (i.e. non-conviction based, or civil, asset forfeiture).

4.54 It also creates a comprehensive asset recovery framework which applies not only to drug offences but also to all offences against the laws of Mauritius which are punishable by a maximum term of imprisonment of not less than 12 months. It also applies to any offence committed in a foreign State which, if committed in Mauritius, would constitute an offence in Mauritius.

4.55 The Act applies to any offence committed, and any property obtained, within 10 years before the commencement of the Act.

Enforcement Authority

4.56 Part II of the Act establishes an independent Enforcement Authority (EA). Since 26 January 2016, the EA is vested on the FIU. Prior thereto, the EA was the Director of Public Prosecutions or any law officer to whom he shall have delegated his powers.

4.57 The Enforcement Authority may exercise any of the powers vested in it by the Act, *inter alia*, applying to a Judge of the Supreme Court for a confiscation or Recovery Order, or for a Restraining or Restriction Order from the Judge in Chambers in relation to property.

4.58 The Enforcement Authority may also :

(a) seek from the Judge in Chambers an Ancillary Order, which may be a Search and Seizure Order or an Account Monitoring Order;

(b) by written notice, require any person to produce or disclose any information or material, other than privileged material or customer information;

(c) by written notice, require a financial institution to provide such customer information as it may have relating to a person specified in the notice.

Customer Information

4.59 The customer information which financial institutions may be required to submit to the Enforcement Authority under the Act are:

(a) information as to whether a person holds or has held an account at financial institutions solely or jointly with another person;

(b) information relating to any evidence obtained by the financial institution under or for the purposes of an enactment relating to money laundering; and

(c) such particulars, relating to the account or its holder as are, in the opinion of the Enforcement Authority, relevant.

Account Monitoring Order

4.60 An Account Monitoring Order is an Order that a financial institution specified in the application for the Order shall, for the period stated in the order[17], provide account information[18] of the description specified in the Order to the Enforcement Authority in the manner, and at or by the time, stated in the Order.

4.61 The Enforcement Authority may make an application before the Judge in Chambers for an Account Monitoring Order and the financial institution shall comply with the Order and provide to the Enforcement Authority the account information specified in the Order.

4.62 The application for the Account Monitoring Order may specify information relating to –

(a) all accounts held by the person specified in the application for the Order at the financial institution so specified;
(b) a particular description, or particular descriptions, of accounts so held; or
(c) a particular account, or particular accounts, so held.

17 The period stated in an Account Monitoring Order shall not exceed the period of 90 days beginning with the day on which the Order is made.

18 Under the Act, "account information" means information relating to an account held in a financial institution by a person solely or jointly with another.

4.63 Under the Act, a statement made by a financial institution in response to an Account Monitoring Order may not be used in evidence against the financial institution in any proceedings.

Asset Recovery Investigative Division

4.63A An Asset Recovery Investigation Division (ARID) has been set up within the FIU. The ARID replaces the former Investigative Agency set up under the office of the Director of Prosecution. The ARID shall, with the approval of the Director of the FIU, consist of law enforcement agents, one of whom shall be designated by the Director to be the Chief Investigating Officer. A law enforcement agent shall have and exercise such powers and duties as the Enforcement Authority may determine.

4.63B. In furtherance of the functions of the FlU under the Asset Recovery Act, the Director of the FIU shall consult with, and seek such assistance from, such persons in Mauritius concerned with combating money laundering, including, amongst others, such persons representing banks, financial institutions and cash dealers as the FlU considers desirable.

International Co-operation

4.64 The Attorney-General or the Enforcement Authority may enter into an agreement with any Ministry, Department, public authority or body outside Mauritius for the collection, use or disclosure of information, including personal information, for the purpose of exchanging or sharing information outside Mauritius or for any other purpose under the Act.

4.65 The Enforcement Authority may in the presence of a foreign request for the location of tainted property apply to a Judge for an order that, *inter alia*, a financial institution forthwith produces to the Enforcement Authority all information obtained by it about any business transaction relating to the property for such period before or after the date of the order as the Judge may direct.

4.66 If a person is failing to comply with, is delaying or is otherwise obstructing such an order, the Judge may, on good cause shown by the Enforcement Authority order a law enforcement agent to enter and search the premises specified in the order and remove any document, material or other thing therein for the purposes of executing such order.

Tipping Off

4.67 The Act provides for the offence of tipping off where any financial institution which has, pursuant to section 48 or 49 of the Act, been required to provide customer information or account information in relation to any person and provides information, or enables information to be provided, to that person by any means regarding the Customer Information Order or Account Monitoring Order.

Penalties

4.68 It is an offence under the Act to refuse to comply with an Ancillary Order or a written notice of the Enforcement Authority [paragraph 4.58 (b) and (c) refers] or to provide or make available any false or misleading information to the Enforcement Authority.

4.69 The Act provides for penalties ranging from fines not exceeding 100,000 rupees and 2 million rupees, imprisonment not exceeding 5 years and penal servitude not exceeding 10 years depending on the seriousness of the offences committed.

5. INTERNAL CONTROLS, POLICIES AND PROCEDURES

5. INTERNAL CONTROLS, POLICIES AND PROCEDURES

RESPONSIBILITIES AND ACCOUNTABILITIES

5.01 Financial institutions are required to have in place adequate policies, procedures and internal controls that promote high ethical and professional standards and prevent their institutions from being used, intentionally or unintentionally, by criminal elements.

5.02 Financial institutions must therefore establish clear responsibilities to ensure that policies, procedures and internal controls are introduced and maintained which deter criminals from using their facilities for money laundering and terrorist financing, thus ensuring that they comply with their obligations under the law.

5.03 Under section 3(2) of the FIAML, financial institutions are required to take such measures as are reasonably necessary to ensure that neither they nor any service offered by them, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence. Any financial institution which fails to take such measures shall commit an offence.

5.04 Under Regulation 9 of the Financial Intelligence and Anti-Money Laundering Regulations 2003, financial institutions are also required to implement internal controls and other procedures to combat money laundering and the financing of terrorism which among other things include establishing and maintaining a manual of compliance procedures in relation to money laundering and programmes for assessing risks relating to money laundering and the financing of terrorism.

5.05 It is therefore of utmost importance for financial institutions to have in place a sound 'Know Your Customer' (KYC) procedure and policy in place. KYC is most closely associated with the fight against money laundering and the financing of terrorism.

FINANCIAL INSTITUTION OPERATING IN A GROUP STRUCTURE

5.05A Financial institutions incorporated in Mauritius with overseas branches or subsidiary undertakings should put in place a group AML/CFT policy to ensure that all branches and subsidiary undertakings that carry on the same business as a financial institution in a place outside Mauritius have procedures in place to comply with the CDD and record keeping requirements similar to those imposed under these Guidance Notes to the extent permitted by the law of that place.

5.05B The financial institution should communicate the group policy to its overseas branches and subsidiary undertakings. The financial institution should have a thorough understanding of all the risks associated with its customers across the group, either individually or as a category, and should document and update these on a regular basis, commensurate with the level and nature of risk in the group.

5.05C When a branch or subsidiary undertaking of a financial institution outside Mauritius is unable to comply with requirements that are similar to those imposed

under these Guidance Notes because this is not permitted by local laws, the financial institution must:

(a) inform the Bank of such failure; and

(b) take additional measures to effectively mitigate ML/TF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the above requirements.

5.05D Financial institutions that use agents should include them in their AML/CFT programmes and monitor them for compliance with these programmes. The financial institution should maintain a current list of its agents and make this list available to the Bank upon request.

APPOINTMENT OF A MONEY LAUNDERING REPORTING OFFICER

5.06 It is imperative that every financial institution appoints an appropriate person who may be among the existing employees of the financial institution as Money Laundering Reporting Officer (MLRO) and to whom all internal suspicious transaction reports will be made. (See further paragraphs 8.08 to 8.12 on the role of a MLRO). The MLRO must be of sufficiently senior status and not below the rank of Manager. (See further Paragraph 5.14 regarding the discretion of financial institutions to allow Compliance Officers to cumulate the functions of the MLRO).

5.07 In branches of financial institutions, there should be a responsible officer on whom responsibility for AML/CFT matters would devolve.

5.08 It is incumbent on the MLRO, on behalf of the financial institution, to make Suspicious Transaction Reports to the FIU.

RECOMMENDED PROCEDURES

5.09 All financial institutions operating within Mauritius should:

(a) have procedures for the prompt validation of suspicions and subsequent reporting by the internal employees to the MLRO.

(b) provide the MLRO with necessary access to systems and records to enable him to investigate and validate internal suspicions reports which have been reported to him.

(c) inform all employees of the identity of the MLRO and in his absence, the person designated to replace him.

APPOINTMENT OF A COMPLIANCE OFFICER

5.10 Financial institutions are also required to appoint a Compliance Officer at Management level who will bear the responsibility to verify, on a regular basis, compliance with policies, procedures and controls relating to money laundering and the financing of terrorism activities.

5.11 This will help to establish that the responsibilities of financial institutions are being discharged as required under the FIAML.

5.12 It is important that the procedures and responsibilities for monitoring compliance with, and effectiveness of, anti-money laundering and financing of terrorism policies and procedures are clearly laid down by all financial institutions.

5.13 It is not necessary, however, to appoint a Compliance Officer in each and every branch of the financial institution. The appointment of a Compliance Officer at the Head Office with jurisdiction over its branches will suffice.

5.14 Although it is advisable for the Compliance Officer and the MLRO to be two distinct persons, it is left to individual financial institutions to decide whether the Compliance Officer may also cumulate the functions of the MLRO.

5.15 The responsibilities of the AML/CFT compliance officer should include -

(a) carrying out, or overseeing the carrying out of, ongoing monitoring of business relations and sample review of accounts for compliance with the AML/CFT laws, regulations and these Guidance Notes;

(b) promoting compliance with the AML/CFT laws, regulations and these Guidance Notes, and taking overall charge of all AML/CFT matters within the organisation;

(c) informing employees and officers promptly of regulatory changes;

(d) ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;

(f) advising and training employees and officers on developing and implementing internal policies, procedures and controls on AML/CFT;

(g) reporting to senior management on the outcome of reviews of the financial institution’s compliance with the AML/CFT laws, regulations and these Guidance Notes, and risk assessment procedures; and

(h) reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising from audit, inspection, and compliance reviews, to the financial institution’s senior management, and in the case of locally incorporated financial institutions, to the board of directors, at least annually and as and when needed.

5.16 The business interests of financial institutions should not interfere with the effective discharge of the above-mentioned responsibilities of the compliance officer, and potential conflicts of interest should be avoided. To enable unbiased judgments and facilitate impartial advice to management, the compliance officer should, for example, be distinct from the internal audit and business line functions. Where any conflicts between business lines and the responsibilities of the compliance officer arise, procedures should be in place to ensure that AML/CFT concerns are objectively considered and addressed at the appropriate level of the financial institution's management.

6. IDENTIFICATION PROCEDURES

6. IDENTIFICATION PROCEDURES

REGULATORY FRAMEWORK

6.01 Section 55 of the Banking Act 2004 in respect of identity of customers provides as follows:-

(1) Every financial institution shall only open accounts for deposits of money and securities, and rent out safe deposit boxes, where it is satisfied that it has established the true identity of the person in whose name the funds or securities are to be credited or deposited or the true identity of the lessee of the safe deposit box, as the case may be.

(2) Every financial institution shall require that each of its accounts be properly named, at all times, so that the true owner of the accounts can be identified by the public and no name shall be allowed that is likely to mislead the public.

6.02 It is therefore mandatory for financial institutions to verify the true identity of their customers before opening any account, accepting any deposit of money and securities and renting a safe deposit box. In that respect, it is in context to state that the Financial Intelligence and Anti-Money Laundering Regulations 2003 expressly prohibit financial institutions from opening anonymous or fictitious accounts.

6.03 By virtue of Section 55(2) of the Banking Act 2004 the keeping of reference accounts by financial institutions is prohibited.

6.04 Breach of section 55 of the Banking Act 2004 is an offence which carries a fine of not less than one million rupees and not more than 5 million rupees.

6.05 With regard to the period prior to 10 November 2004, the date on which the Banking Act 2004 became operative, the provisions of the Banking Act 1988 prevailed in Mauritius. Breach of section 40 of the Banking Act 1988 with respect to "Identity of Customers", during that period carries a fine of not less than 10,000 rupees and not more than 5,000,000 rupees.

6.06 In addition, the FIAML requires every financial institution to verify, in such manner as may be prescribed, the true identity of all customers and other persons with whom they conduct transactions.

6.07 The manner of verification of identity and address of customers is prescribed in the Financial Intelligence and Anti-Money Laundering Regulations 2003 as amended. For all business relationships entered into with applicants for business on or after 21 June 2003, financial institutions should ensure that the identification procedures stipulated in these Guidance Notes are complied with.

RELATIONSHIPS ENTERED INTO PRIOR TO 21 JUNE 2003

6.08 Where in relation to business relationships entered into prior to 21 June 2003 a financial institution believes that it has not satisfactorily established or has doubts or suspicion regarding the true identity of its customer, the financial institution should follow the identification procedures stipulated in these Guidance Notes.

CAVEAT

6.09 Financial institutions should never open, operate or carry out transactions pertaining to anonymous or fictitious accounts for customers.

'KNOW YOUR CUSTOMER'

6.10 The foundation of any effective system to combat money laundering and the financing of terrorism is the 'Know Your Customer' (KYC) Principle. It is the degree of proximity between the financial institution and the customer which the KYC principle entails that will allow financial institutions to gauge a situation, decide whether a transaction is suspicious and be able to avert risks inherent in money laundering and the financing of terrorism.

6.11 The safety and soundness of financial institutions are therefore largely dependent on their KYC procedures. Sound KYC procedures, inter alia,

(i) reduce the likelihood of financial institutions being used as a vehicle for the laundering of the proceeds of criminal activities or the moving of terrorist funds.

(ii) constitute an essential part of sound risk management by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities.

6.12 The inadequacy or absence of KYC standards can subject financial institutions to serious risks, especially

(i) **Reputational risk -** that is, the risk that adverse publicity regarding a financial institution's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution.

(ii) **Operational risk** – that is, the risk that the financial institution will suffer direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events which in the context of KYC relates to weaknesses in the implementation of programmes, ineffective control procedures and failure to practise due diligence.

(iii) **Legal risk** – that is, the possibility that lawsuits, adverse judgements or contracts turn out to be unenforceable and disrupt or adversely affect the operations or condition of a financial institution.

6.13 The need for financial institutions to know their customer is therefore vital for the prevention of money laundering and the financing of terrorism.

6.14 A financial institution which has permitted the opening of an account or performed a transaction under a false identity, address or date of birth will render it difficult for Law Enforcement Agencies to trace the customer if he is needed for interview in connection with an investigation.

6.15 When a business relationship is being established, the nature of the business that the customer expects to conduct with the financial institutions should be ascertained at the outset, to show what might be expected as normal activity. In order to be able to judge whether a transaction is or is not suspicious, financial institutions should have a clear understanding of the legitimate business of their customers and effect an ongoing monitoring of the activities of those customers in order to detect whether those transactions conform or otherwise with the normal or expected transactions of that customer.

6.16 KYC should be a core feature of financial institutions' risk management and control procedures, and should be complemented by regular compliance reviews and internal audit.

ESSENTIAL ELEMENTS OF KYC STANDARDS

6.17 The essential elements of KYC standards should start from the financial institutions' risk management and control procedures and should include the following :

(i) customer acceptance policy,
(ii) customer identification,
(iii) ongoing monitoring of accounts and transactions; and
(iv) risk management.

6.17A Sound risk management requires the identification and analysis of ML/TF risks present within the financial institution and the design and effective implementation of policies and procedures that are commensurate with the identified risks. Financial institutions should :

(i) develop a thorough understanding of the inherent ML/TF risks present in its customer base, products, delivery channels and services offered and the jurisdictions within which it or its customers do business; and

(ii) design and implement their policies and procedures for customer acceptance, due diligence and ongoing monitoring to adequately control those identified inherent risk.

6.17B In addition to assessing the ML/TF risks presented by an individual customer, financial institutions should identify and assess ML/TF risks on an enterprise-wide level. This should include a consolidated assessment of the institution's ML/TF risks that exist across all its business units, product lines and delivery channels. The enterprise-wide ML/TF risk assessment is intended to enable the financial institution better understand its overall vulnerability to ML/TF risks and forms the basis for the institution's overall risk-based approach.

6.17C The senior management of the financial institution should approve the enterprise-wide ML/TF risk assessment and relevant business units should give their full support and active co-operation to the enterprise-wide ML/TF risk assessment.

6.17D The scale and scope of the enterprise-wide ML/TF risk assessment should be commensurate with the nature and complexity of the financial institution's business. In conducting an enterprise-wide risk assessment, the broad ML/TF risk factors that the financial institution should consider include –

(a) in relation to its customers —

(i) target customer markets and segments;

(ii) profile and number of customers identified as higher risk;

(iii) volumes and sizes of its customers' transactions and funds transfers, considering the usual activities and the risk profiles of its customers;

(b) in relation to the countries or jurisdictions its customers are from or in, or where the financial institution has operations in —

(i) countries or jurisdictions the financial institution is exposed to, either through its own activities (including where its branches and subsidiaries operate in) or the activities of its customers (including the financial institution's network of correspondent banking relationships), especially countries or jurisdictions with relatively higher levels of corruption, organised crime or inadequate AML/CFT measures, as identified by the Financial Action Task Force ("FATF");

(ii) when assessing ML/TF risks of countries and jurisdictions, the following criteria may be considered:

- evidence of adverse news or relevant public criticism of a country or jurisdiction, including FATF public documents on High Risk and Non-cooperative jurisdictions;

- independent and public assessment of the country's or jurisdiction's overall AML/CFT regime such as FATF or FATF-Styled Regional Bodies' ("FSRBs") Mutual Evaluation reports and the IMF/World Bank Financial Sector Assessment Programme Reports or Reports on the Observance of Standards and Codes for guidance on the country's or jurisdiction's AML/CFT measures;

- the AML/CFT laws, regulations and standards of the country or jurisdiction;

- implementation standards (including quality and effectiveness of supervision) of the AML/CFT regime;

- whether the country or jurisdiction is a member of international groups that only admit countries or jurisdictions which meet certain AML/CFT benchmarks;

- contextual factors, such as political stability, maturity and sophistication of the regulatory and supervisory regime, level of corruption, financial inclusion etc.;

(c) in relation to the products, services, transactions and delivery channels of the financial institution —

(i) the nature, scale, diversity and complexity of the financial institution's business activities;

(ii) the nature of products and services offered by the financial institution; and

(iii) the delivery channels, including the extent to which the financial institution deals directly with the customer, relies on third parties to perform CDD measures or uses technology.

6.17E As far as possible, financial institutions' enterprise-wide ML/TF risk assessment should entail both qualitative and quantitative analyses to ensure that the financial institution accurately understands its exposure to ML/TF risks. A quantitative analysis of the financial institution's exposure to ML/TF risks should involve evaluating data on the financial institution's activities using the applicable broad risk factors set out in paragraph 6.17D.

6.17F In assessing its overall ML/TF risks, financial institutions should make its own determination as to the risk weights to be given to the individual factor or combination of factors.

6.17G The nature and extent of AML/CFT risk management systems and controls implemented should be commensurate with the ML/TF risks identified via the enterprise-wide ML/TF risk assessment, which should also serve to guide the allocation of AML/CFT resources within the institution.

6.17H Financial institutions should assess the effectiveness of its risk mitigation procedures and controls by monitoring the following:

(a) the ability to identify changes in a customer profile (e.g. Politically Exposed Persons status) and transactional behaviour observed in the course of its business;

(b) the potential for abuse of new business initiatives, products, practices and services for ML/TF purposes;

(c) the compliance arrangements (for e.g. through its internal audit or quality assurance processes or external review);

(d) the balance between the use of technology-based or automated solutions with that of manual or people-based processes, for AML/CFT risk management purposes;

(e) the coordination between AML/CFT compliance and other functions of the financial institution;

(f) the adequacy of training provided to employees and officers and awareness of the employees and officers on AML/CFT matters;

(g) the process of management reporting and escalation of pertinent AML/CFT issues to the financial institution's senior management;

(h) the coordination between the financial institution and regulatory or law enforcement agencies; and

(i) the performance of third parties relied upon by the financial institution to carry out CDD measures.

6.17I In order to keep its enterprise-wide risk assessments up-to-date, financial institutions should review its risk assessment at least once every two years or when material trigger events occur, whichever is earlier. Such material trigger events include, but are not limited to, the acquisition of new customer segments or delivery channels, or the launch of new products and services by the financial institution. The results of these reviews should be documented and approved by senior management even if there are no significant changes to the enterprise-wide risk assessment of the institution.

6.17J Financial institutions should ensure that the following documentation are kept on record and made available to the Bank upon request:

(a) enterprise-wide ML/TF risk assessment by the financial institution;

(b) details of the implementation of the AML/CFT risk management systems and controls as guided by the enterprise-wide ML/TF risk assessment;

(c) the reports to senior management on the results of the enterprise-wide ML/TF risk assessment and the implementation of the AML/CFT risk management systems and controls; and

(d) details of the frequency of review of the enterprise-wide ML/TF risk assessment.

CUSTOMER ACCEPTANCE POLICY

6.18 Regulation 9(d) of the Financial Intelligence and Anti-Money Laundering Regulations 2003 require financial institutions to implement due diligence procedures with respect to persons and business relations and transactions carrying high risk and with persons established in jurisdictions that do not have adequate systems in place against money laundering and the financing of terrorism.

6.19 Accordingly, financial institutions should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a financial institution.

6.20 In preparing such policies, factors such as the customer's background, nature of business or social engagement, country of origin with a view to determining whether those countries have adequate systems in place against money laundering and the financing of terrorism, public or high profile position and other risk indicators should be considered.

6.21 Customer acceptance policies and procedures should accordingly be graduated and require more extensive due diligence for higher risk customers, such as an individual planning to maintain a large account balance and conduct regular cross-border wire transfers or politically exposed persons. Decisions to enter into or pursue business relationships with higher-risk customers should require the application of enhanced due diligence measures, such as approval to enter into or continue such business relationships being taken by senior management. The customer acceptance policy should also define circumstances under which the financial institution would not accept a new business relationship or would terminate an existing one.

6.22 The exercise should however be calibrated to ensure that the customer acceptance policy does not result in a denial of access by the general public to legitimate banking, deposit taking and cash dealer services.

CUSTOMER IDENTIFICATION

6.23 For the purposes of section 6 of these Guidance Notes, the following definitions will be used :-

"Applicant for business" means a person, who seeks to form a business relationship, or carry out a one-off transaction with a financial institution.

"Business relationship" means an arrangement between a person and a financial institution where the purpose or effect of the arrangement is to facilitate the carrying out of transactions between the person and the financial institution on a frequent, habitual or regular basis.

"One-off transaction" means any transaction carried out other than in the course of a business relationship. For example, a single foreign currency transaction carried out for a customer who does not have an account at the financial institutions concerned.

"significant shareholders" means shareholders, other than shareholders which are companies listed on a recognised, designated and approved Stock/Investment Exchange as shown in Appendix A, who directly or indirectly hold 20% or more of the capital or of the voting rights of the company.

GENERAL IDENTIFICATION REQUIREMENTS AND RISK PROFILING

6.24 Regulation 4 of the Financial Intelligence and Anti-Money Laundering Regulations 2003 requires financial institutions to establish and verify the identity and current permanent address of an applicant for business, the nature of the applicant's business, his financial status and the capacity in which he is entering into the business relationship with the financial institution.

6.25 The overriding requirement is that (i) whenever a business relationship is or is resolved to be established, (ii) a one-off transaction exceeding Rs350,000.- or an equivalent amount in foreign currency is to be undertaken, (iii) a series of linked one-off transactions which together exceed Rs350,000.- or an equivalent amount in foreign currency is to be undertaken, or (iv) the one-off transaction is suspicious for any reason, the identity of the applicant for business must be obtained and verified prior to the opening of the account or the undertaking of the transaction.

6.26 Financial institutions should establish to its satisfaction that it is dealing with a real person or organisation, and verify the identity of the person or organisation accordingly. If funds that are to be deposited or transferred are being supplied on behalf of a third party, then the identity of the third party should be established and verified. In case a financial institution is not able to determine whether the applicant for business is acting for a third party, it should make a record of the grounds for suspecting that the applicant for business is so acting and make a Suspicious Transaction Report to the Financial Intelligence Unit. This paragraph, however, does not apply to "Client's Accounts opened by Professional Intermediaries" which are dealt with in paragraphs 6.81 to 6.82 of these Guidance Notes.

6.26a. Financial institutions should also require customers to complete a written declaration of the identity and details of natural person(s) who are the ultimate beneficial owner(s) of the business relationship or transaction as a first step in meeting their beneficial ownership customer due diligence requirements. Requiring a written declaration of beneficial ownership by the contracting customer is an important first step in the financial institution's effort to identify and verify the identity of the beneficial owner. The FATF defines 'beneficial owner' as the natural person(s) who ultimately owns or controls a customer and/or the natural 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.

6.27 Financial institutions need to obtain all information necessary to establish to their full satisfaction the identity of the applicant for business and the purpose and nature of the business relationship or transaction. They should cross check information by accessing available public databases such as telephone directories and electoral registers and private databases such as Credit Information Bureaux, both at the local and international levels and keep on their files full information on ultimate beneficial owners in case they are not the same persons as the applicant for business, as well as persons acting on their behalf, and accordingly take reasonable measures to verify the identity of the beneficial owner using relevant information or data obtained from a reliable source such that the financial institution is satisfied that it knows who the beneficial owner is.

6.28 When an existing customer closes one account and opens another there is no need to re-verify identity, although good practice requires that the details on the customer's file be reconfirmed. This is particularly important if there has been no recent contact with the customer e.g. for the past twelve months. Details of the previous accounts and steps originally taken to verify identity or any introduction records should be transferred to the new account records.

6.29 Subsequent changes to the name of the applicant for business, address or employment details of which the financial institution becomes aware, should be recorded and be duly substantiated by the appropriate documentary evidence as part of the KYC process. CDD information on the customer and the beneficial owner has to be kept up to date.

6.30 In the case of an applicant for business transferring an opening balance from an account which he maintains with one bank or non-bank deposit taking institution directly to another bank or non-bank deposit taking institution, banks and non-bank deposit taking institutions should consider the possibility that the previous account manager may have asked for the account to be closed because of suspicions about dubious activities. If a financial institution has any reason to believe that an applicant is being or has been rejected by another financial institution, it should apply enhanced diligence procedures before accepting the customer.

6.31 Financial institutions should pay special attention to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose and should examine as far as possible the background and purpose of such transactions and set their findings in writing. As part of the broader customer due diligence measures, financial institutions should ensure that information regarding source of funds and/or destination of funds are corroborated. Examples of such transactions or patterns of transactions include : significant transactions relative to a relationship; transactions that exceed certain limits, very high account turnover inconsistent with the size of the balance, or transactions which fall out of the regular pattern of the account’s activity. (See further paragraph 7.06 with respect to record keeping requirement.)

6.32 Financial institutions should, as far as is practicable, in the case of personal accounts ensure that evidence of identity is obtained during the course of an interview with the applicant for business so that the financial institution can verify that the customer is actually the person he claims to be, i.e. the applicant for business should be seen personally and photographic evidence of his identity obtained. Financial institutions should verify that any person whether an applicant for business, purporting to act on behalf of the customer or a potential customer is so authorised and any official judgment, signed mandate or equivalent document should be verified together with the identity of that person.

6.33 In respect of joint personal accounts, the names and addresses of all account holders should be verified.

6.34 The verification procedures necessary to establish the identity of the applicant for business should be the same whatever be the type of account or service that is required (e.g. current, deposit, or other accounts). The name of the member of staff undertaking or responsible for the account opening procedure should be

noted on the customer's file together with that of the higher ranking officer who has approved the business relationship.

6.35 Generally, the main objective of financial institutions in the case of entities should be to identify those who have control over the business and the assets.

6.36 The best identification documents are those that are the most difficult to obtain illicitly and to counterfeit. No single form of identification can be fully guaranteed as genuine or representing correct identity. To verify identity beyond reasonable doubt, the identification process will generally need to be cumulative.

6.37 Where a financial institution cannot obtain all the CDD information, it shall not open the account, commence the business relations or perform the transaction and consider making a suspicious transaction report to the FIU.

6.38 Financial institutions should apply CDD requirements to existing customers on the basis of materiality and conduct due diligence on such existing relationships at appropriate times. Examples of when it may be appropriate to do so are when–

(a) a transaction of significance takes place,

(b) customer documentation standards change substantially,

(c) there is a material change in the way that the account is operated,

(d) the institution becomes aware that it lacks sufficient information about an existing customer.

6.39 In the case where financial institutions have doubts about the veracity or adequacy of previously obtained customer identification data, it should terminate the business relationship and consider making a suspicious transaction report to the FIU.

Risk Profiling

6.39A. Financial institutions should have policies and procedures in place to conduct due diligence on its customers sufficient to develop customer risk profiles either for particular customers or categories of customers. Financial institutions should use the information obtained during the customer identification and verification process to build an understanding of the customer’s profile and behaviour. Examples of information typically collected are (i) the purpose of the relationship or the occasional banking transaction, (ii) the level of assets or the size of transactions of the customer and (iii) the regularity or duration of the relationship. The information collected should be determined by the level of risk associated with the customer’s business model and activities as well as the financial products or services requested by the customer. Financial institutions should also carry out additional searches, including carrying out verifiable adverse media searches, when performing the customer risk assessment. The customer risk profile will further determine the level and type of ongoing monitoring and support the bank’s decision whether to enter into, continue or terminate, the business relationship.

6.39B. When the account opening is the start of a customer relationship, financial institutions should collect the following information on the natural or legal person with a view to developing an initial customer risk profile :

(i) **Natural Persons**

The following key attributes are useful in establishing the first step of the customer's risk profile:

a) occupation, public position held;
b) income;
c) expected use of account : amount, number, type, purpose and frequency of the transactions expected;
d) financial products or services requested by customers.

Potential additional information, on the basis of risks, which may be requested are:

a) name of employer, where applicable;
b) sources of customer's wealth;
c) sources of funds passing through the account;
d) destination of funds passing through the account.

Financial institutions should also consider, on a risk-sensitive basis, whether the information regarding sources of wealth and funds or destination of funds should be corroborated.

(ii) **Legal Persons**

As a minimum, financial institutions may consider the following in establishing the risk profile of a legal person :

a) Nature and purpose of the activities of the legal entity and its legitimacy;
b) Expected use of the account : amount, number, type, purpose and frequency of the transactions expected.

The following potential additional information, on the basis of risk may be requested :

a) Financial situation of the entity;
b) Sources of funds paid into the account and destination of funds passing through the account.

(iii) **Legal Arrangements**

As a minimum, financial institutions should collect the following information :

a) Description of the purpose/activities of the legal arrangement (e.g. in a formal constitution, trust deed);
b) Expected use of the account : amount, number, type, purpose and frequency of the transactions expected.

Potential additional information, on the basis of risks, which may be collected are:

a) Source of funds;
b) Origin and destination of funds passing through the account.

ACCOUNT OPENING FOR PERSONAL CUSTOMERS

6.40 Paragraph 4 of Regulation 4 of the Financial Intelligence and Anti-Money Laundering Regulations 2003 provides that where an applicant for business is an individual customer, he shall submit to a financial institution, the original or a certified copy of an official valid document containing details of his current permanent address, a recent photograph of him and such other documents as may be required, to enable the financial institution to establish his identity.

6.41 Accordingly, financial institutions are required to maintain the following identification procedures in respect of individual customers.

FACE-TO-FACE APPLICATIONS

Residents of Mauritius (Personal)

6.42 An individual's true identity comprises his/her name, his/her date of birth, his/her current permanent residential address, the nature of his/her business, his/her normal financial transactions and any agency or beneficiary relationship.

Name

6.43 The name of individuals residing in Mauritius should, during the course of an interview with him, be verified from an original official valid document bearing his/her recent photograph and any of the following may be relied upon:-

- National identity cards
- Current valid passports
- Current valid driving licences.

On the basis of risks involved, any other names used such as marital name, former legal name or alias and the gender of the applicant for business may be collected.

6.44 What constitutes recent, for the purposes of the photograph, will in the circumstances, be decided during the course of the interview with the individual. A material difference in the photograph will lead the inference that the photograph may not be recent.

6.45 Financial institutions should keep a copy of that page which contains the photograph of the applicant for business and ensure that the relevant reference numbers of those documents are recorded.

6.46 Because documents providing photographic evidence of identity need to be compared with the applicant's appearance, and to guard against the dangers of fraud, it would be appropriate to ensure that applicants for business do not send those identity documents by post to financial institutions.

Address

6.47 In addition to the name, it is important that the current permanent address of the applicant for business be verified as an integral part of identity. Satisfactory evidence of address can be obtained by any of the following, a copy of which should be retained, after the originals have been sighted. The retained copy shall be duly annotated "original sighted". Alternatively, the original document may be scanned and retained in electronic form in such manner that it may be retrieved as and when information is sought on the applicant for business.

- a recent[19] utility bill
- a recent bank or credit card statement
- a recent bank reference
- any other document or documents which either singly or cumulatively establishes, beyond reasonable doubt, the address of the applicant for business.

On the basis of risks involved, the business address, email address and landline or mobile telephone number as well as the residency status of the applicant for business may be collected.

6.48 Financial institutions may effect additional verification of identity by -

- checking a local telephone directory
- checking a current register of electors
- visiting the applicant for business at his/her permanent residential address.
- contacting the customer by telephone, letter or email to confirm the information supplied, after an account has been opened.
- checking references provided by other financial institutions.
- For higher-risk customers, additional sources of information such as requesting for prior bank reference, verification of income sources, funds and wealth, may be considered.

Non Residents (Personal)

6.49 Regarding applicants for business who are not resident in Mauritius but who make face-to-face contact with a financial institution, they should be required to complete a standard application form which should incorporate the following details :-

- True name
- Current permanent address
- Mailing address
- Telephone and fax number
- Date and place of birth
- Nationality
- Occupation and name of employer (if self-employed, the nature of the self-employment)
- signature/signatures

[19] For the purposes of this paragraph 'recent' refers to not more than 3 months.

- authority to obtain an independent bank reference

6.50 The form, duly filled in must be supported by a clear legible copy of any of the following documents:-

- National Identity Card
- Current valid passports
- Current valid driving licences
- Armed forces identity card

6.51 Financial institutions should keep a copy of that page which contains the recent photograph of the applicant for business, ensure that the relevant reference numbers of the passports or National Identity Card, driving licences or armed forces identity card of those documents are duly recorded.

6.52 In the case of non-residents making face-to-face contact, however, financial institutions should in addition verify identity and current permanent address of the applicant for business with a reputable credit or financial institution in the applicant's normal home country or country of residence.

NON FACE-TO-FACE VERIFICATION

6.53 It is most important that the procedures adopted to confirm identity for non-face-to-face verification be at least as robust as those for face-to-face verification. Examples of non-face to face operations include: business relationships concluded over the Internet or by other means such as through the post; services and transactions over the Internet including trading in securities by retail investors over the Internet or other interactive computer services; use of ATM machines; telephone banking; transmission of instructions or applications via facsimile or similar means and making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid or reloadable or account-linked value cards.

6.54 As with face-to-face verification, the procedures to check identity must serve two purposes:

- they must ensure that a person bearing the name of the applicant exists and lives at the address provided; and

- that the applicant is that person.

6.55 Accordingly, in accepting business from non-face-to-face customers:

- financial institutions should apply equally effective customer identification procedures as for those available for interview; and

- other specific and adequate measures to mitigate the higher risk posed by non-face-to-face verification of customers.

Non-Resident (Personal) Applying from Abroad

6.56 Non-Residents applying from abroad should be required to complete a standard application form, which should incorporate the following details:

- true name
- current permanent address
- mailing address
- telephone and fax number
- date and place of birth
- nationality
- occupation and name of employer (if self-employed, the nature of the self-employment)
- passport details, or National Identity Card, driving licence or armed forces identity card details (i.e. number and country of issuance), together with issue date and expiry date
- signature/signatures
- authority to obtain independent verification of any data provided

6.57 The application form, duly filled in, should be accompanied by the following supporting documents :-

- Identity - a clearly legible photocopy of any of the following documents :-

  - National Identity Card
  - Current valid passports
  - Current valid driving licences
  - Armed forces identity card

  duly certified as a true copy by a lawyer, accountant or other professional persons who clearly adds to the copy (by means of a stamp or otherwise) his name, address and profession to aid tracing of the certifier if necessary and which the financial institution believes in good faith to be acceptable to it for the purposes of certifying.

- Address –

  (i) an original or certified copy of utility bill addressed to the applicant at the address from which he, she or they are applying;

  (ii) an original or certified copy of a bank statement addressed to the applicant at the address from which he, she or they are applying.

6.58 The following additional steps may be taken :- developing independent contact with the customer, confirmation by the financial institutions from directory enquiries or from a recognised telephone directory for the locality from which the applicant is applying, containing an entry for the applicant and showing the address from which he, she or they are applying.

6.59 Financial institutions may also rely on other regulated institutions to verify identity of non-resident customers, in accordance with paragraphs 6.83 to 6.91 on "Reliance On Other Regulated Institutions To Verify Identity".

ACCOUNT OPENING FOR LEGAL PERSONS AND ARRANGEMENTS

6.59A Financial institutions should verify the identity of the customer as set out below, using reliable, independent source documents[20], data or information. The measures to verify the information produced should be proportionate to the risk posed by the customer relationship and should allow the financial institution to satisfy itself that it knows the customer's identity. Financial institution may consider the following non-exhaustive list:

- reviewing a copy of the latest financial statements (audited, if available). for established corporate entities;
- undertaking a company search and/or other commercial enquiries to ascertain that the legal person has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;
- utilising an independent information verification process, such as by accessing public corporate registers, private databases or other reliable independent sources (e.g. lawyers, accountants);
- validating the Legal Entity Identifier (LEI), if available, and associated data in the public access service;
- obtaining prior bank references;
- visiting the corporate entity, where practical;
- contacting the corporate entity by telephone, mail or e-mail.

Locally Incorporated Companies

6.60 With regard to locally incorporated companies, financial institutions should verify:-

(i) the identity of those who ultimately own or have control over the company's business and assets, more particularly

- their directors,
- beneficial owner(s)[21],
- their significant shareholders, and
- their authorised signatories. In the absence of an authorised signatory, the identity of the relevant person who is the senior managing official[22].

20 Reliable documents include, but are not limited to, any valid form of Government Issued Identification such as driver's license, passport or ID card. Identification documents which do not bear photographs or signatures are not considered appropriate evidence of identity.

[21] The FATF defines 'beneficial owner' as the natural person(s) who ultimately owns or controls a customer and/or the natural 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.

22 Senior managing official means an individual who makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of a customer or who has the capacity to affect significantly the financial standing of a customer.

(ii) the legal existence of the company, namely, the name, legal form, status and proof of incorporation of the legal person as well as its permanent address of the principal place of the legal person's activities, its mailing and registered address.

6.61 The following documents should be obtained and retained in the case of locally incorporated companies :

(i) In respect of employees authorised to open and operate accounts on their behalf, the beneficial owners, their directors and significant shareholders, proof of identity, proof of current permanent address and such other documents as may be required to enable the financial institution to establish their identity;

(ii) A certified copy of the resolution of the Board of Directors or managing body and the power of attorney granted to its employees to open and to operate accounts on their behalf; and

(iii) Official documents which collectively establish the legal existence of that entity, e.g. the original, including an electronic certificate of incorporation issued by the Registrar of Companies of Mauritius, or certified copy of the certificate of incorporation of the company, business registration number, details of its registered office and permanent address of the principal place of business etc.

6.62 Enquiries should be made to confirm :

(i) by verifying with the Registrar of Companies, that the company continues to exist and has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;

(ii) by conducting in cases of doubt a visit to the place of business of the company, to verify that the company exists for a legitimate trading or economic purpose.

6.63 As with personal accounts, 'know your customer' is an ongoing process. If changes to the company structure or ownership occur subsequently, or if suspicions are aroused by a change in the nature of the business transacted or the profile of payments through a company account, further checks should be made to ascertain the reason for the changes.

Foreign Companies

6.64 Where the applicant for business is a foreign company, the same documents as are required for locally incorporated companies should be requested and retained.

6.65 In addition financial institutions should check the veracity of the information provided with a credit or financial institution of good standing in the permanent place of business of the company.

6.66 Financial institutions may also rely on other regulated institutions to verify identity of foreign companies, in accordance with paragraphs 6.83 to 6.91 on "Reliance On Other Regulated Institutions To Verify Identity".

Partnerships /Unincorporated Businesses

6.67 Where the applicant for business is a partnership or an unincorporated business,

(i) the identity of any partner owning or controlling more than 20% of the partnership, controllers of the unincorporated business and their authorised signatories should be verified in accordance with procedures required for the identification of personal applicants for business, and

(ii) the same documents as are required for personal applicants for business should be requested and retained.

6.68 In the case of unincorporated businesses, in addition, the necessary licence given by the competent Authorities for the conduct of such business should be requested and retained and in the case of partnerships, an original or certified copy of the partnership deed obtained.

6.69 Financial institutions should also in cases of doubt make enquiries to confirm the true nature of the business activities to ascertain whether those business activities have a legitimate purpose.

Clubs and Charities

6.70 It is increasingly being recognised that terrorists and terrorist groups are having recourse to clubs and charities for the financing of terrorism.

6.71 Accordingly, in the case of accounts to be opened for clubs or charities, financial institutions should at the very beginning satisfy themselves as to the legitimate purpose of the organisation by requesting a certified copy of the constitution of the club or charity and also in case of doubt by paying a visit to its premises, where practicable, to satisfy themselves as to the true nature of its activities. They may also satisfy themselves by independent confirmation of the purpose of the club or charity.

6.72 The identity of the persons in control of the club or charity should be ascertained, in accordance with the procedures required for personal customers.

6.73 Control of clubs and charities are most likely to change from time to time and the identity of those new controllers of the clubs or charities should be verified as and when financial institutions are advised of any change.

Sociétés

6.74 In the case of sociétés, the original or certified copy of the Acte de Société should be requested and retained.

6.75 For Mauritian sociétés, the financial institution should ensure, by verifying with the Registrar of Companies, that the société continues to exist.

6.76 As regards foreign sociétés the financial institution should obtain a certificate of good standing from them.

6.77 Financial institutions should also, in accordance with the procedures set out for personal customers, verify the identity of those in control of the société, e.g. its administrators and gérants etc. and retain the same relevant documents as are required for personal customers accordingly.

Cooperatives

6.77A Where cooperatives are applicants for accounts, those persons, quite often the board members as well as executives and account signatories, exercising control or significant influence over the organisation's assets should be considered the beneficial owners and therefore identified and verified, in addition to the normal identification documents establishing the legal existence of the Cooperative.

Trusts

6.78 Financial institutions should exercise particular caution with respect to trusts, given the common perception that trusts are often misused for laundering the proceeds of crime and hiding terrorist funds.

6.79 In the case of trusts, the following information should as a minimum be required for identification purposes: name of trust, proof of existence, address, country of establishment, nature, purpose, objects, names of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership). Financial institutions should collect further information such as certified extracts of the original trust deed or probate copy of a will creating the trust, documentary evidence pertaining to the appointment of the current trustees and the nature and purpose of the trust, as well as documentary evidence as are required for personal customers on the identity of the current trustees, the settlor and/or beneficial owner of the funds and of any controller or similar person having power to appoint or remove the trustees should be requested and retained.

6.80 Financial institutions should also obtain written confirmation from the trustees that they are themselves aware of the true identity of the underlying principals i.e. the settlors/named beneficiaries, and that there are no anonymous principals.

6.80A Financial institutions should also gather the maximum information on the trust's operations prior to opening of the account and should also monitor on a regular basis the inflows and outflows in line with the given business plan.

'Client Accounts' Opened By Professional Intermediaries

6.81 Professional intermediaries, such as stockbrokers, fund managers, law practitioners, accountants, estate agents and other professional intermediaries, frequently hold funds on behalf of their clients in 'client accounts' opened with financial institutions. Such accounts may be opened on behalf of either a single client or for many clients.

6.81A When a professional intermediary opens a customer account on behalf of a single customer, the financial institution must identify the customer.

6.81B Where funds held by the professional intermediary are not co-mingled but "sub-accounts" are established which can be attributed to each beneficial owner, the financial institution must identify all beneficial owners of the account held by the professional intermediary.

6.81C Where the funds are co-mingled, the financial institution should look through to the beneficial owners. However, where the professional intermediary is subject to due diligence standards in respect of its customer base that are equivalent to those applying to the financial institution itself, the latter may not need to look beyond the intermediary and may obtain an undertaking from it that it has verified the identity of its clients and secured particulars of the identity of those clients.

6.81D Where the professional intermediary is subject to due diligence as stated in paragraph 6.81C above and an account is opened for an open or closed-end investment company, unit trust or limited partnership that is subject to customer due diligence requirements which are equivalent to those applying to the financial institution itself, the latter should treat this investment vehicle as its customer and take steps to identify:

i. the fund itself;
ii. its directors or any controlling board where it is a company;
iii. its trustee where it is a unit trust;
iv. its managing (general) partner where it is a limited partnership;
v. account signatories; and
vi. any other person who has control over the relationship e.g. fund administrator or manager.

6.81E Where other investment vehicles are involved, the same steps should be taken as in paragraph 6.81D where it is appropriate to do so. In addition, in cases when no equivalent due diligence standards apply to the investment vehicle, all reasonable steps should be taken to verify the identity of the beneficial owners of the funds and of those who have control of the funds.

Retirement benefit programmes

6.82 Where an occupational pension programme, employee benefit trust or share option plan is an applicant for business, the trustee and any other person who has control over the relationship (e.g. administrator, programme manager or account signatories) can be considered as beneficial owners. The financial institution should conduct, in accordance with the procedures laid down in Paragraphs 6.01 to 6.80 as applicable, due diligence on the applicant.

Foundations

6.82A A foundation may be established in Mauritius or elsewhere and registered in Mauritius in accordance with the Foundations Act 2012. A foundation will not have legal personality unless it is registered and has been issued with a certificate

of registration by the Registrar of Companies who also cumulates the function of Registrar of Foundations.

6.82B A foundation may be charitable or non-charitable, or both.

6.82C When verifying the identity of a foundation, the financial institution must, in line with guidance provided for individuals and legal bodies, verify:

With respect to the foundation:

(a) its name;
(b) its date of registration with the Registrar of Foundations;
(c) its date and country of incorporation;
(d) its official identification number;
(e) its business address;
(f) its principal place of business and operations (if different),

by using the following verification methods, namely, the Charter (or equivalent) of the foundation, search at the Registrar of Foundations, the latest audited financial statements and independent data sources.

With respect to the persons who are concerned with the foundation :

(g) the identity of, *inter alia*, (i) the council members, specially those who have authority to operate a business relationship or to give instructions concerning the use or transfer of funds or assets, (ii) the founder, (iii) the executor, (iv) the protector, (v) the beneficiary, and (vi) the administrator.

6.82D Where a foundation is a charitable foundation, the financial institution must ensure that it adheres to the guidance issued for 'Clubs and Charities' at paragraphs 6.70 to 6.73 above.

RELIANCE ON OTHER REGULATED INSTITUTIONS TO VERIFY IDENTITY

6.83 Although the ultimate responsibility for verifying the identity and address of customers always lies with the financial institution, it is recognised that to avoid duplication, financial institutions may rely on other eligible or group introducers to verify the identity of applicants for business. Financial institutions should however have clear policies and procedures on whether and when it is acceptable and prudent to rely on other eligible or group introducers.

6.84 An eligible introducer is any person who introduces an applicant for business to a financial institution in Mauritius and –

(a) is regulated under the Financial Intelligence and Anti-Money Laundering Act 2002 or any similar legislation in an equivalent jurisdiction, or is subject to rules of professional conduct relating to the prevention of money laundering and terrorist financing; and

(b) is based either in Mauritius or in an equivalent jurisdiction.

6.85 A group introducer is an introducer which is part of the same group as the financial institution to whom the applicant for business is introduced and is, for anti-money laundering purposes, subject to either the consolidated supervision of a regulator in Mauritius or in an equivalent jurisdiction or is subject to the anti-money laundering regulations of a regulator in Mauritius or in an equivalent jurisdiction.

6.86 An equivalent jurisdiction is a jurisdiction which has a legislation equivalent to Mauritius as specified in Appendix B.

6.87 Financial institutions may rely on an eligible or a group introducer to verify the identity of an applicant for business where –

(i) the financial institution obtains and maintains documentary evidence that the eligible introducer or group introducer is regulated for the purposes of preventing money laundering and terrorist financing; and

(ii) the financial institution is satisfied that the procedures laid down by the eligible introducer or group introducer is effectively regulated and supervised and has measures in place to meet the requirements specified in the FIAML, regulations made thereunder and these Guidance Notes. In the case of a group introducer, the implementation of these measures is supervised at a group level by a competent authority and any higher country risk is adequately mitigated by the group's AML/CFT policies.

6.88 In this case, financial institutions should immediately obtain from the eligible or group introducer the necessary information concerning, inter alia, the following elements of the CDD process.

(a) identity of customer and beneficial owner and verify that customer's identity using reliable, independent source documents, data or information;

(b) verify whether the customer is acting on behalf of a third party;

(c) obtain information on the purpose and intended nature of the business relationship.

6.89 Where a financial institution relies on customer identification documentation in the possession of an eligible or group introducer, it is not required to retain copies of the customer identification documentation in its own records where the financial institution is satisfied that he may obtain that customer identification documentation from the eligible introducer or group introducer upon request without delay. The financial institution should, in its procedures and policies, document the reliance and should establish adequate controls and review procedures for such a relationship and should identify and mitigate any additional risk posed by reliance on multiple parties and its risk assessment should identify reliance on third parties as a potential risk factor.

6.90 In addition, financial institutions should conduct periodic reviews to ensure that an introducer which it relies on continues to conform to the criteria set out above. For that purpose, the financial institution should obtain all the CDD information

and documents from the eligible or group introducer and assess due diligence conducted, including screening against local databases to ensure compliance with local regulatory requirements.

6.91 Financial institutions must request group or eligible introducers to provide them with a duly completed Group Introducers Certificate or Eligible Introducers Certificate as the case may be. It is left to financial institutions to design their own Group or Eligible Introducers Certificates, provided that the information called for in the certificate do not materially differ with the specimens at Appendices C and D. The financial institution must reach an agreement with the introducer that it will be permitted at any stage to verify the due diligence undertaken by the introducer. Financial institutions should consider terminating reliance on entities that do not apply adequate CDD on their customers and give due consideration to adverse public information about the entity.

TRADE BASED MONEY LAUNDERING/FINANCING OF TERRORISM

6.91a. Trade-based money laundering and terrorist financing refers to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origins or finance their activities. Examples of how trade-based money laundering and terrorist financing may be carried out include, but are not limited to: misrepresentation of the price, quantity or quality of imports or exports; and money laundering through fictitious trade activities and/or through front companies. The most basic schemes involve fraudulent trade practices such as: over- and under-invoicing of goods and services, multiple invoicing of goods and services, over- and under-shipments of goods and services, and falsely describing goods and services. Particular attention should be paid by financial institutions when undertaking transactions on behalf of customers involved in free trade activities.

6.91b. Financial institutions shall accordingly, have adequate systems to properly manage risks associated with trade finance activities. Such systems shall depend on the financial institution's size, complexity, location and types of customer relationship and shall effectively enable a financial institution to identify and monitor its trade finance portfolio for suspicious or unusual activities, in particular those that pose a higher risk for money laundering.

6.91c. Financial institutions shall also have their trade finance accounts regularly sample-tested with the view to verifying whether they are meeting their customer due diligence, record keeping, monitoring and reporting obligations.

6.91d. Financial institutions may, for guidance, refer to the FATF Report on "Money Laundering vulnerabilities of Free Trade Zones" issued by the FATF in March 2010 and to the "Best Practices Paper on Trade Based Money Laundering" and to the report on "Trade Based Money Laundering" issued by the FATF in June 2008 and June 2006 respectively and available on the website of the FATF at http://fatf-gafi.org.

CORRESPONDENT SERVICES

6.92 Correspondent services are the provision of services by one financial institution to another financial institution. Used by financial institutions throughout the world, correspondent services enable financial institutions to conduct business that the financial institutions do not offer directly. Particular care should be taken where correspondent services involve jurisdictions where the correspondent financial institutions have no physical presence. If financial institutions fail to apply an appropriate level of due diligence to such services, they expose themselves to a range of risks and may find themselves holding and/or transmitting money linked to terrorism, corruption, fraud or other illegal activity.

6.93 Financial institutions should -

(i) gather sufficient information about their correspondents to understand fully the nature of the correspondent's business. Factors to consider include: information about the correspondent's management, major business activities, where they are located and its money-laundering prevention and detection efforts; the identity of any third party entities that use the correspondent services;

(ii) determine from public available information the reputation of the institution and quality of the institution's regulation and supervision, including whether it has been subject to money laundering or terrorist financing investigation or regulatory action;

(iii) assess the institution's AML/CFT controls and ascertain that they are adequate and effective and establish correspondent relationships with foreign financial institutions only if financial institutions are satisfied that the foreign financial institutions are effectively supervised by the relevant authorities and have effective customer acceptance and KYC policies;

(iv) obtain approval from senior management before establishing new correspondent relationships.

(v) document the respective AML/CFT responsibilities of each institution. It is not necessary that the two financial institutions always have to reduce the respective responsibilities into a written form provided there is a clear understanding as to which institution will perform the required measures.

(vi) where a correspondent relationship involves the maintenance of "payable-through accounts", be satisfied that –

(a) the respondent financial institution has performed all the normal CDD obligations set out in these Guidance Notes on those of its customers that have direct access to the accounts of the correspondent financial institution; and

(b) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.

6.94 In particular, financial institutions should refuse to enter into or continue a correspondent relationship with a financial institution incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. it may involve shell financial institution). They should also satisfy themselves that the respondent financial institutions do not permit their accounts to be used by shell banks. Financial institutions should pay particular attention when continuing relationships with correspondents or establishing relationships and transactions with persons located in jurisdictions that have poor KYC standards or have been identified as being "non-cooperative" in the fight against anti-money laundering or as having deficiencies in their AML/CFT regime. Financial institutions should establish that their correspondents have due diligence standards as set out in these Guidance Notes, and employ enhanced due diligence procedures with respect to transactions carried out. A list of jurisdictions that have been classified as non co-operative by the FATF or as having deficiencies in their AML/CFT regime is shown at Appendix E. Where a financial institution finds that those transactions have no apparent economic or visible lawful purpose, it must as far as possible examine the background and purpose of such transactions and keep its findings in writing to be made available to the auditors and to the Bank upon request. Senior management should be regularly informed of high-risk correspondent banking relationship and how they are monitored.

6.95 Financial institutions should be particularly alert to the risk that correspondent services might be used directly by third parties to transact business on their own behalf. Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria set out for introduced business.

EXEMPTIONS

6.96 Where an applicant for business is itself a financial institution based in Mauritius or in a jurisdiction which has a legislation equivalent to Mauritius as specified in Appendix B verification of identity shall not be required.

6.97 The financial institution should, however, obtain and retain a written declaration from the other financial institution that it holds documentary evidence of the existence of the legal entity, its regulated or listed status.

6.98 In the case of

(a) Public companies listed on a recognised, designated and approved Stock/Investment Exchange as shown in Appendix A or subsidiaries thereof, financial institutions are not required to verify the identity of their directors or significant shareholders. Verification of the identity of their authorised signatories will be enough. Financial institutions are, however, required to obtain a copy of the annual report and accounts of such entities and to keep them on record,

(b) Parastatal bodies in Mauritius, documentary evidence of the residential address of their authorised signatories may not be sought.

6.99 Identification procedures shall also not be required in relation to a one-off transaction, in which the proceeds of the transaction are not paid, but are directly reinvested on behalf of the person to whom the proceeds are payable in another transaction –

(i) of which a record is kept; and

(ii) which results only in another reinvestment made on that person's behalf or, in payment made directly to that person.

POLITICALLY EXPOSED PERSONS

6.100 Business relationships with individuals holding important public positions and with persons or entities clearly related to them may expose a financial institution to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") be it local or foreign, are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations, important political party officials, their family members and their close associates. In the case of entities relating to local PEPs, these would comprise entities that are 20 per cent or more owned or controlled by those local PEPs. The possibility exists that such persons may abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc. The measures applicable to a PEP are also applicable to family members or persons known to be close associates of PEPs as well as persons who have been entrusted with a prominent function by an international organisation.

6.100A A list of PEPs is given at Appendix H. Family members of PEPs are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership and shall comprise their spouses, any partner considered by national law as being equivalent to a spouse and their children, the children and their spouses, or persons considered to be equivalent to a spouse, the parents of a PEP. Close associates are individuals who are closely connected to a PEP, either socially or professionally and include (i) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations with a PEP; and (ii) natural persons who have sole beneficial ownership of a legal entity or legal arrangement, which is known to have been set up for the de facto benefit of a PEP. International organisation PEPs are persons who are or have been entrusted with a prominent function by an international organisation and refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions.

6.101 Accepting and managing funds from local or foreign corrupt PEPs will severely damage the financial institution's own reputation and can undermine public confidence in the ethical standards of an entire financial centre, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove. Under certain circumstances, the financial institution and/or their officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds were destined for the financing of terrorism or stemmed from corruption or other crimes.

6.102 In Mauritius corruption is a predicate offence for money laundering and all the relevant anti-money laundering laws and regulations apply (e.g. reporting of suspicious transactions, prohibition on informing the customer). There is a compelling need for a financial institution considering a relationship with a person, be it local or foreign, whom it considers to be a PEP to identify that person fully, as well as people and companies that are clearly related to him/her.

6.103 Financial institutions should gather sufficient information from a new customer, including information on the beneficial owner, check publicly available information or access commercial electronic databases, in order to establish whether or not the customer or the beneficial owner is a PEP. Financial institutions should also take reasonable measures to establish the source of wealth and the source of funds of the customer and beneficial owners identified as PEPs. Financial institutions are encouraged to consider the ongoing PEP status of their customers on a case-by-case basis using a risk-based approach. If the risk is low, financial institutions may consider declassifying the relationship, but only after careful consideration of continuing anti-money laundering risks and approval by senior management.

6.104 Financial institutions should put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a PEP. It can reduce risk by conducting detailed due diligence at the out-set of the relationship including requiring a declaration of beneficial ownership and enhanced ongoing monitoring where a business relationship has been established with a PEP.

6.105 All financial institutions should assess which countries, with which they have financial relationships, are most vulnerable to corruption. One source of information is the Transparency International Corruption Perceptions Index at www.transparency.org. Financial institutions which are part of an international group might also use the group network as another source of information.

6.106 Where financial institutions do have business in countries vulnerable to corruption, they should establish who are the senior political figures in that country and, should seek to determine whether or not their customer has any connections with such individuals (for example they are immediate family or close associates). Financial institutions should note the risk that individuals may acquire such connections after the business relationship has been established.

6.107 In particular detailed due diligence should include:

- Close scrutiny of any complex structures (for example, involving companies, trusts and multiple jurisdictions) so as to establish that there is a clear and legitimate reason for using such structures bearing in mind that most legitimate political figures would expect their personal affairs to be undertaken in a more than usually open manner rather than the reverse.

- Every effort to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship – again establishing that these are legitimate, both at the outset of the relationship and on an ongoing basis.

- The development of a profile of expected activity on the business relationship so as to provide a basis for future monitoring. The profile should be regularly reviewed and updated.

- An approval at senior management or board level of the decision to commence the business relationship and to continue the business relationship where the customer has been accepted and the customer or beneficial owner is subsequently found to be or subsequently becomes a PEP.

- Regular review by senior management using a risk-based approach, at least yearly, with the results of the review duly documented. Over the course of a business relationship with a PEP, ongoing monitoring procedures may reveal changes to the profile and activity. The PEP may have been promoted or elected to a more senior position, engaged in litigation, or made transactions deviated from the norm. Considered separately, the activities, transactions or profile changes may not be sufficient to raise "red flags." Implementing a periodic review of PEP customers on a risk-based approach, and at least yearly, would help to overcome the approach in which decisions are made transaction-by-transaction, activity-by-activity which would enhance the oversight of the PEPs customer relationships by senior management.

- Close scrutiny of any unusual features, such as very large transactions, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of small and unknown financial institutions in secrecy jurisdictions and regular transactions involving sums just below a typical reporting amount.

6.107A. Where a politically exposed person is no longer entrusted with a prominent public function either domestically or abroad, or with a prominent public function by an international organisation, financial institutions should, for at least 12 months, take into account the continuing risk posed by that person and apply appropriate and risk sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed persons. The financial institution should document the reasons justifying the decision to declassify the customer as a PEP and make these reasons available to the Bank upon request.

WIRE TRANSFER TRANSACTIONS

6.108 Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the originator is not clearly shown in an electronic payment message instruction.

6.109 To ensure that wire transfer systems are not used by criminals as a means to break the audit trail, where a financial institution makes a payment on behalf of its customer, accurate and meaningful originator[23] information (name, residential

[23] Where the originator is acting on behalf of others (e.g. as nominee, agent, or trustee), then it is the name, address, and account number of the nominee, agent, trustee, etc. that should be included. The financial institution making the payment should have on file the name and address of underlying principals.

address[24] and any account number or reference of the originator) should be included on all funds transfers and related messages and should remain with the transfer through the payment chain until it reaches its final destination. This information is particularly important for international transfers on behalf of individual customers to ensure that the source of funds can be identified in the event of an investigation in the receiving jurisdiction.

6.110 When the financial institutions act as the ordering institution, -

(1) All cross-border wire transfers of USD/EUR 1,000 or more should always be accompanied by the following:

(a) required and accurate originator information:

(i) the name of the originator;

(ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and

(iii) the originator's address, or national identity number, or customer identification number, or date and place of birth.

(b) required beneficiary information:

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(2) Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file should contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country. The financial institution should also include the originator's account number or unique transaction reference number.

(3) Cross-border wire transfers of less than USD/EUR 1,000 should be accompanied by the following :

(a) required originator information:

(i) the name of the originator; and

(ii) the originator account number where such an account is used to process the transaction or, in the absence of an

[24] Registered office address where an originator is a company.

account, a unique transaction reference number which permits traceability of the transaction.

(b) required beneficiary information:

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(4) The above information need not be verified for accuracy. However, the financial institution should verify the information where there is a suspicion of money laundering or terrorist financing.

(5) For domestic wire transfers, the financial should ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire transfers.

(6) The financial institution should not execute the wire transfer if it does not comply with the requirements specified above.

6.111 Financial institutions should not omit, delete or alter information in payment messages, for the purpose of avoiding detection of that information by another financial institution in the payment process.

6.112 Financial institutions should monitor payment messages to and from higher risk countries or jurisdictions, as well as transactions with higher risk countries or jurisdictions and suspend or reject payment messages or transactions with sanctioned parties or countries or jurisdictions.

6.113 Where name screening checks confirm that the wire transfer originator or wire transfer beneficiary is a terrorist or terrorist entity, the requirement for the financial institution to block or reject assets of these terrorists or terrorist entities cannot be risk-based.

6.114 Where there are positive hits arising from name screening checks, they should be escalated to the AML/CFT compliance function. The decision to approve or reject the receipt or release of the wire transfer should be made at an appropriate level and documented.

6.115 Where funds transfers are processed as an intermediary, e.g. where financial institution “B” is instructed by financial institution “A” to pay funds to an account held by a beneficiary at financial institution “C”, the originator and beneficiary data provided by financial institution “A” should be preserved and, wherever possible, included in the message generated by financial institution “B”.

6.116 Where a cross-border wire transfer, regardless of amount, is a cover payment (e.g. MT202COV payments), ordering institutions should ensure that the payment message of the cover payment sent to the intermediary institution contain information of the wire transfer originator and wire transfer beneficiary. The

information included in the payment message of the cover payment should be identical to that contained in the cross-border wire transfer message sent directly to the beneficiary institution.

6.117 An intermediary institution that receives and transmits a cover payment should ensure that the relevant fields for storing originator and beneficiary information in the payment message of the cover payment are duly completed. In addition, such intermediary institutions should ensure that the wire transfer originator and wire transfer beneficiary information in the payment message of the cover payment is complete. The intermediary institution should also screen the names of the wire transfer originator and wire transfer beneficiary.

6.118 Financial institutions should conduct enhanced scrutiny of, and monitor for suspicious activity, incoming funds transfers which do not contain complete originator information. This will involve examining the transaction in more detail in order to determine whether certain aspects related to the transaction could make it suspicious (origin in a country known to harbour terrorists or terrorist organisations, for example). Where an incoming wire transfer is not accompanied by complete wire transfer originator information and wire transfer beneficiary, a beneficiary institution should request the information from the ordering institution. Financial institutions should consider rejecting incoming wire transfers or terminating business relations with overseas ordering institutions that fail to provide originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transaction is suspicious and to consider, as appropriate, whether they are thus required to be reported to the FIU. In some cases, the beneficiary financial institution should consider restricting or even terminating its business relationship with financial institutions that fail to meet the above requirements.

ONGOING MONITORING OF ACCOUNTS AND TRANSACTIONS

6.119 Ongoing monitoring is an essential aspect of effective KYC procedures. Ongoing due diligence should include scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the financial institution's knowledge of the customer, their business and risk profile, and where necessary, the source of funds. Financial institutions should have in place a monitoring system that is adequate with respect to its size, its activities and complexity as well as the risks present in the financial institution. When an IT system is used, it should cover all accounts of the financial institution's customers and transactions for the benefit of, or by order of, those customers.

6.120 Financial institutions should ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships. Financial institutions should be able to risk-rate customers and manage alerts with all the relevant information at their disposal. Using CDD information, financial institutions should be able to identify transactions that do not appear to make economic sense, that involve large cash deposits or that are not consistent with the customer's normal and expected transactions.

6.121 The extent of the monitoring needs to be risk-sensitive. For all accounts, financial institutions should have systems in place to detect complex, unusual or suspicious transactions or patterns of activity. In establishing scenarios for identifying such activity, financial institutions should consider the customer's risk profile developed as a result of the financial institution's risk assessment, information collected during its CDD efforts and other information obtained from law enforcement and other authorities in its jurisdiction. Certain types of transactions should alert financial institutions to the possibility that the customer is conducting complex, unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account. Financial institutions should have access to updated, comprehensive and accurate customer profiles and records to be able to effectively monitor and identify suspicious activities.

6.122 Examples of suspicious activities are given at annexes F and G. Financial institutions are enjoined to study money laundering or terrorist financing typologies coming their way or published by the Financial Action Task Force (FATF) at http://www.fatf-gafi.org to keep their relevant staff duly informed of the patterns of abuse.

6.123 There should be intensified monitoring for higher risk accounts. Every financial institution should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors. For higher risk accounts:

- Financial institutions should ensure that they have adequate management information systems to provide managers and MLROs with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. The types of reports that may be needed in the AML/CFT area include transactions made through an account that are unusual.

- Financial institutions should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them. As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

6.124 Financial institutions should ensure that they have appropriate integrated management information systems commensurate with its size, organizational structure or complexity, based on materiality and risks, to provide both business units and risk and compliance officers with timely information needed to identify, analyse and effectively monitor customer accounts. Financial institutions should screen its customer database(s) whenever there are changes to sanction lists and also, periodically, to detect PEPs and other higher risk accounts and subject them to enhanced due diligence.

TECHNOLOGICAL DEVELOPMENTS

6.125 Financial institutions should also have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes. Financial institutions may, for guidance, refer to the "Risk Management Principles for Electronic Banking" issued by the Basel Committee in July 2003 and available on the website of the BIS at http://www.bis.org and to the reports on (i) "Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites & Internet Payment Systems" issued by the FATF on 10 July 2008 and (ii) "Money Laundering Using New Payment Methods" issued by the FATF in October 2010. The report on "Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites & Internet Payment Systems" focuses on the type of electronic commerce identified as the most vulnerable to money laundering and terrorist financing: mediated customer-to-customer. The report also provides a number of case studies illustrating how mediated customer-to-customer systems can be exploited for ML/TF purposes. The FATF Report on "Money Laundering Using New Payment Methods" describes a number of indicators of suspicious activity which may help detect ML/TF activities. The FATF issued typologies reports which focused on the potential for new payment products and services to be misused by criminals, the identification of risk factors which can significantly differ from one new payment product or service to another, depending on functionality; and risk mitigates which can be tailored to particular new payment product or service to address its specific risk profile. In 2013, the FATF issued guidance on taking a risk-based approach to prepaid cards, mobile payments and internet payment systems, which financial institutions are recommended to consider prior to offering new payment products and services. These reports are available on the website of the FATF at http://www.fatf-gafi.org.

RISK MANAGEMENT

6.126 The ultimate responsibility and accountability for ensuring compliance with AML/CFT laws, regulations, guidelines and instructions vest with the board of directors and senior management of the financial institution. The board of directors of the financial institution should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the financial institutions for ensuring that their policies and procedures are managed effectively. While certain responsibilities can be delegated to senior AML/CFT employees, final accountability rests with the board of director and senior management of the financial institution. Financial institutions should ensure that there is a strong compliance culture throughout the organization, where the board of directors and senior management set the right tone. The board of directors and senior management should set a clear risk appetite and ensure a compliance culture where financial crime is not acceptable.

6.127 As a general rule and for the purposes of AML/CFT, the business units, namely the front office, customer-facing activity, are the first line of defence in charge of identifying, assessing and controlling the risks of their business. They should know and carry out the policies and procedures and be allotted sufficient resources to do this effectively. The financial institution's policies, procedures and controls on AML/CFT should be clearly specified in writing, and communicated to all

relevant employees and officers in the business units. The financial institution should adequately train employees and officers to be aware of their obligations, and provide instructions as well as guidance on how to ensure compliance with prevailing AML/CFT laws, regulations and guidelines.

6.128 The second line of defence includes the Compliance officer or the Chief Officer in charge of AML/CFT, the compliance function, as well as other support functions such as operations, human resources or technology, which work together with the AML/CFT compliance function to identify ML/TF risks when they process transactions or applications or deploy systems or technology. The third line of defence is ensured by the internal audit function. Accordingly, financial institutions' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. As a general rule, the compliance function should through the Compliance Officer provide an independent evaluation of the financial institution's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors if it believes management is failing to address KYC procedures in a responsible manner. Other support functions such as operations, human resource or technology also play a role to help mitigate the ML/TF risks that the financial institution faces.

6.129 As the third line of defence, internal audit plays an important role in independently evaluating the risk management and controls, discharging its responsibility to the Audit Committee of the Board of Directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training. Management should ensure that internal audit functions are staffed adequately with individuals who are well-versed in such policies and procedures. In addition, internal auditors should be proactive in following-up their findings and criticisms. Internal audit should also evaluate the IT system to ensure that it is appropriate and used effectively by the first and second lines of defence. Financial institutions should accordingly establish policies for periodic AML/CFT internal audits covering areas such as –

(a) the adequacy of the financial institution's AML/CFT policies, procedures and controls in identifying MF/TF risks, addressing the identified risks and complying with laws, regulations and guidelines;

(b) the effectiveness of the financial institution's employees and officers in implementing the financial institution's policies, procedures and controls;

(c) the effectiveness of the compliance oversight and quality control including parameters and criteria for transaction alerts; and

(d) the effectiveness of the financial institution's training of relevant employees and officers.

6.130 The AML/CFT framework of the financial institution should, therefore, be subject to periodic audits (including sample testing). Such audits should be performed not just on individual business functions but also on an institution-wide basis.

Auditors should assess the effectiveness of measures taken to prevent ML/TF. This would include, among others –

(a) determining the adequacy of the institution's AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;

(b) reviewing the content and frequency of AML/CFT training programmes, and the extent of employees' and officers' compliance with established AML/CFT policies and procedures; and

(c) assessing whether instances of non-compliance are reported to senior management on a timely basis.

6.131 The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the institution's business.

6.132 External auditors also have an important role to play in monitoring financial institutions' internal controls and procedures, and in confirming that they are in compliance with laws, rules, regulations and these Guidance Notes.

GOVERNANCE

6.133 Strong board and senior management leadership is indispensable in the oversight of the development and implementation of a sound AML/CFT risk management framework across the financial institution. The board of directors and senior management should ensure that the financial institution's processes are robust and there are adequate risk mitigating measures in place. The successful implementation and effective operation of a risk-based approach to AML/CFT depends on the financial institution's employees and officers having a good understanding of the ML/TF risks inherent in the financial institution's business.

6.134 Financial institutions' board of directors and senior management should understand the ML/TF risks the financial institution is exposed to and how the financial institution's AML/CFT control framework operates to mitigate those risks. This should involve the board and senior management —

(a) receiving sufficient, frequent and objective information to form an accurate picture of the ML/TF risks including emerging or new ML/TF risks, which the financial institution is exposed to through its activities and individual business relations;

(b) receiving sufficient and objective information to assess whether the financial institution's AML/CFT controls are adequate and effective;

(c) receiving information on legal and regulatory developments and the impact these have on the financial institution's AML/CFT framework; and

(d) ensuring that processes are in place to escalate important decisions that directly impact the ability of the financial institution to address and control ML/TF risks, especially where AML/CFT controls are assessed to be inadequate or ineffective.

7. RECORD-KEEPING

7. RECORD-KEEPING

STATUTORY REQUIREMENTS

7.01 Section 33 of the Banking Act 2004 provides as follows:

> ***33. Records***
>
> *(1) Every financial institution shall, for the purposes of the banking laws, keep in relation to its activities, a full and true written record of every transaction it conducts.*
>
> *(2) The records under subsection (1) shall include -*
>
> *(a) accounting records exhibiting clearly and correctly the state of its business affairs, explaining its transactions and financial position so as to enable the central bank to determine whether the financial institution has complied with all the provisions of the banking laws;*
>
> *(b) the financial statements;*
>
> *(c) account files of every customer, business correspondences exchanged with every customer and records showing, for every customer, at least on a daily basis, particulars of its transactions with or for the account of that customer, and the balance owing to or by that customer;*
>
> *(d) proper credit documentation; and*
>
> *(e) such other records as the central bank may determine.*
>
> *(3) Every record under this section shall be kept -*
>
> *(a) in written form or kept on microfilm, magnetic tape, optical disk, or any other form of mechanical or electronic data storage and retrieval mechanism as the central bank may agree to;*
>
> *(b) for a period of at least 7 years after the completion of the transaction to which it relates;*
>
> *(c) at the principal office of the financial institution, or at such other place, in Mauritius, as may be approved by the central bank; and*
>
> *(d) for identification purposes, in chronological order or sequential order, as appropriate, in batches of convenient size.*

AUDIT TRAIL

7.02 Record keeping is an essential component of the combat against money laundering and the financing of terrorism in the sense that an audit trail is established. Otherwise, an authority investigating a case relating to money laundering or the financing of terrorism would not be able to follow the movement of the funds through the financial system thus rendering enquiry and confiscation of those funds difficult. Often the only valid role a financial institution can play in a money laundering or financing of terrorism investigation is through the provision of relevant records, particularly where a complex web of transactions specifically for the purpose of confusing the audit trail has been used.

IDENTITY RECORDS

7.03 All documentation required by financial institutions to verify the identity of customers and of beneficial owners in accordance with these Guidance Notes must be retained for a period of not less than 7 years after the completion of the transaction to which it relates, closure of the account or cessation of the business relationship with the customer concerned.

7.04 In cases where a third party has been relied upon to undertake verification of identity procedures or to confirm identity, arrangements should be made for the records to be retained for the same period as stated in paragraph 7.03 above.

TRANSACTION RECORDS

7.05 Transaction records, in whatever form they are used, e.g. credit/debit slips, cheques etc. need to be maintained for a period of not less than 7 years after the completion of the transactions concerned, in such a manner to enable investigating authorities to compile a satisfactory audit trail for suspected laundered and terrorist money and establish a financial profile of any suspect account and should include the following :-

(i) the volume of funds flowing through the account

(ii) the source of the funds, including full remitter details

(iii) the form in which the funds were offered or withdrawn i.e. cash, cheques, etc.

(iv) the identity of the person undertaking the transaction and of the beneficiary

(v) counterparty details

(vi) the destination of the funds

(vii) the form of instruction and authority

(viii) the date of the transaction.

(ix) the type and identifying number of any account involved in the transaction.

Reports made to and by the MLRO

7.06 Records of all internal reports made to the Money Laundering Reporting Officer and also all reports made by the MLRO to the Financial Intelligence Unit should be retained for a period of not less than 7 years after the date on which the report was made.

Any findings relating to the background and purpose of complex, unusual or suspicious transactions should also be retained for a period of not less than 7 years after the date on which the finding was made.

Records Relating to Ongoing Investigations

7.07 Where the records relate to ongoing investigations, they should be retained until it is confirmed by the authorities that the case has been closed.

Electronic Records

7.08 Records of electronic payments and messages must be treated in the same way as any other records and kept for the period mentioned in 7.03 above.

7.09 A comprehensive set of identification documents in respect of each customer should be kept in an orderly manner and produced to the Bank of Mauritius on request.

7.10 It is lawful to electronically record any matter and a personal identification mark on the electronically recorded document is as good as a signature.

Powers of the Director of FIU

7.11 Notwithstanding the above provisions, where a report of a suspicious transaction is made under section 14 of the FIAMLA, the Director of the FIU can, by written notice, not later than 15 days before the end of the 7th year following the completion of the transaction to which the suspicious transaction report relates, require the financial institution to keep the records in respect of that suspicious transaction for such period as may be specified in the notice.

8. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

8. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

WHAT IS A SUSPICIOUS TRANSACTION?

8.01 Suspicious transaction has been defined in the interpretation section of the FIAML. This statutory definition is reproduced at paragraph 4.17 of these Guidance Notes under the section "The Legislative Framework of Mauritius". It is noteworthy that, in accordance with that definition, a suspicious transaction is a transaction which gives rise to suspicion for any reason.

RECOGNITION OF SUSPICIOUS TRANSACTIONS

8.02 Where there is a business relationship, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognition is knowing enough about the customer and the customer's business to recognise that a transaction, or series of transactions, is unusual.

8.03 Questions that a financial institution might consider when determining whether an established customer's transaction might be suspicious are:

- is the size of the transaction consistent with the normal activities of the customer?
- is the transaction rational in the context of the customer's business or personal activities?
- has the pattern of transactions conducted by the customer changed?
- where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

Examples of Suspicious Transactions

8.04 Examples of what may constitute suspicious transactions in relation to money laundering are given in guidance to that effect issued by the FIU and also at Appendix F. Other examples provided by the FATF of what may constitute suspicious transactions in relation to the financing of terrorism are given in Appendix G. These are not intended to be exhaustive and provide examples only of the most basic ways by which money may be laundered or terrorism can be financed. However, identification of any of the types of transactions listed in Appendices F and G along with other available information including in the case of terrorism, lists of suspected terrorists, terrorist groups and associated individuals and entities issued by the United Nations, should prompt further investigation and be a catalyst towards making further enquiries.

8.05 Sufficient guidance must be given to staff to enable them to recognise suspicious transactions (see section on "Education and Training"). The type of situations giving rise to suspicions will depend on a financial institution's customer base and range of services and products. Financial institutions might also consider monitoring the types of transactions and circumstances that have given rise to suspicious transaction reports by staff, with a view to updating internal instructions from time to time.

REPORTING OF SUSPICIOUS TRANSACTIONS

8.06 There is an obligation on all staff to report in writing to the MLRO suspicions of money laundering and terrorist financing.

8.07 All financial institutions have a clear obligation to ensure:

- that each relevant employee knows to which person he should report suspicions

- that there is a clear reporting chain under which those suspicions will be passed directly and without delay to the MLRO.

Once an employee has reported his suspicion to the MLRO, he has fully satisfied and discharged his statutory obligation.

The Money Laundering Reporting Officer (MLRO)

8.08 Financial institutions should ensure that appropriate replacement be provided in case the MLRO is absent. In no case, however, should a member of the Internal Audit Department of the financial institution perform the duties of the MLRO as this will create a conflict of interest.

8.09 The MLRO must be endowed with a significant degree of responsibility and independence. He is required to determine whether the information or other matters contained in the transaction report he has received give rise to knowledge or reasonable suspicion that a customer is engaged in money laundering or the financing of terrorism.

8.10 In making this judgment, he should consider all other relevant information available within the financial institution concerning the person or business to whom the initial report relates. This may include making a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship, and referral to identification records held. If, after completing this review, it is decided that there are no facts that would negate the suspicion, then he must report that suspicious transaction to the FIU.

8.11 Nevertheless, care should be taken to guard against a report being submitted as a matter of routine without undertaking reasonable internal enquiries to determine that all available information has been taken into account.

8.12 The MLRO will be expected to act honestly and reasonably and to make his determinations in good faith. Provided the MLRO or in his absence, the person authorised to replace him, does act in good faith in deciding not to pass on any suspicions, there will be no liability for non-reporting if his judgment is later found to be wrong.

INTERNAL REPORTING PROCEDURES AND RECORDS

8.13 Reporting lines should be as short as possible, with the minimum number of people between the person with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO.

8.14 All suspicions reported to the MLRO should be documented. The person with the suspicion may first discuss it with the MLRO and then prepare the initial report and send it to the MLRO. The report should include full details of the customer and as full a statement as possible of the information giving rise to the suspicion.

8.15 The MLRO should acknowledge receipt of the report. All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the authorities, should be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, there is an investigation in a case on which the MLRO has opted not to report and suspicions are later found to be confirmed.

8.16 Ongoing communication between the MLRO and the internal reporting person/department is important. The person who has made the report to the MLRO should be made aware of the MLRO's decision whether a report has been made by him to the FIU or otherwise. Likewise, at the end of an investigation, all members of staff concerned should be informed of the outcome. It is particularly important that the MLRO is informed of all communication between the investigating authorities and the financial institution at all stages of the investigation.

REPORTING

8.17 All reports of suspicious transactions whether in relation to money laundering or terrorist financing should be made to:

The Director
Financial Intelligence Unit
7th Floor, Ebène Heights
34, Ebène Cybercity
Ebène
Republic of Mauritius

Telephone: (230) 454 1423
Fax: (230) 466 2431
Email: fiu@fiumauritius.org

Crimes other than money laundering and the financing of terrorism

8.18 MLROs should distinguish between the making of Suspicious Transaction Reports in respect of money laundering or the financing of terrorism and the lodging of a complaint or allegation of crime with the Police for investigation.

Contents of Suspicious Transactions Reports

8.19 It is mandatory for every report which a financial institution lodges with the FIU to contain the information stated at paragraph 4.25 of these Guidance Notes.

Method of Reporting

8.20 The use of a standard format in the reporting of suspicious transactions is important. A format has been devised by the FIU and is available on the website of the FIU, www.fiumauritius.org.

9. EMPLOYEE SCREENING, EDUCATION AND TRAINING

9. EMPLOYEE SCREENING, EDUCATION AND TRAINING

SCREENING OF EMPLOYEES

9.01 Every financial institution must put in place screening procedures to ensure high standards when hiring employees. In this respect, consideration may be given to–

(a) obtaining and confirming appropriate references at the time of recruitment;

(b) requesting information from the employee with regard to any regulatory action taken against him or action taken by a professional body; and

(c) requesting information from the employee with regard to any criminal convictions and the provision of a check of his criminal record.

ONGOING TRAINING PROGRAMME

9.02 Every financial institution must, in order to combat money laundering and the financing of terrorism, implement an ongoing training programme for its employees in order to discharge part of its statutory duty to take reasonable measures in that regard.

STAFF AWARENESS

9.03 Financial institutions must take appropriate measures to make employees aware of:

i. policies and procedures put in place to prevent money laundering and the financing of terrorism including those for identification, record-keeping, the recognition and handling of suspicious transactions and internal reporting.

ii. the legal requirements contained in the Financial Intelligence and Anti-Money Laundering Act 2002, the Prevention of Corruption Act 2002 in so far as it is applicable to money laundering, the Prevention of Terrorism Act 2002 with regard to the financing of terrorism and the Convention for the Suppression of the Financing of Terrorism Act 2003 and Regulations applicable to them.

iii. their own personal statutory obligations, and the fact that they can personally be liable for failure to report information in accordance with internal procedures.

iv. new developments, including information on current money laundering and financing of terrorism techniques, methods and trends.

DIFFERENT REQUIREMENTS FOR DIFFERENT CATEGORIES OF STAFF

9.04 Account Opening Personnel

Those members of staff responsible for account opening and acceptance of new customers must receive training in respect of the need to verify a customer's identity and on the internal opening and customer verification procedures available in the institution. They should also be familiarised with the recognition and handling of suspicious transactions and internal suspicious transaction reporting procedures.

9.05 Front Line Staff

All front line staff who are dealing directly with the public are the first point of contact with potential money launderers and terrorists or their agents. They have to be trained to know the true identity of the customer and the need to, at the outset, know enough of the type of business activities expected of the customer to know what might constitute suspicious activities at a future date. They should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal conduct. They should be provided with training on the recognition and handling of suspicious transactions and on the procedures to be adopted when a transaction is regarded as suspicious.

9.05a Global Trade Services Staff

Financial institutions shall provide AML/CFT training, with special emphasis on trade-based money laundering and terrorist financing, to their global trade services departments and personnel.

9.06 New Employees

New employees must, as soon as may be reasonably practicable be given a broad appreciation of the general background to the combating of money laundering and the financing of terrorism, and the internal suspicious transactions reporting procedures. They should be made aware of the importance placed on the reporting of suspicions by the organisation, that there is a legal requirement to report and that there is a personal statutory obligation in this respect. They should also be provided with a copy of the written policies and procedures in place for the reporting of suspicious transactions.

9.07 Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the penalties arising under the Act for non-reporting, assisting money launderers and 'tipping off'; internal reporting procedures; and the requirements for the verification of identity and retention of records.

9.08 MLROs and Compliance Officers

In-depth training concerning all aspects of the Financial Intelligence and Anti-Money Laundering Act 2002, the Prevention of Corruption Act 2002 in so far as it is applicable to money laundering, the Prevention of Terrorism Act 2002 with regard to the financing of terrorism and the Convention for the Suppression of the Financing of Terrorism Act 2003 and Regulations applicable to those legislations, the internal policies applicable in their institutions and the recognition of suspicious transactions, will be required for the MLRO and Compliance Officer. In addition, the MLRO and Compliance Officer will require extensive initial and ongoing instruction on the validation and reporting of suspicious transactions, on feedback arrangements, and on new trends and patterns of criminal activity.

9.09 Refresher Training

It will be necessary to make arrangements for refresher training at regular intervals to ensure that staff do not forget their responsibilities.

9.10 Records

Financial institutions should keep a record of all anti-money laundering and combating the financing of terrorism training delivered to their employees.

APPENDIX A

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)
Tradepoint Financial Networks Plc

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
Australian Securities Exchange
Bermuda Stock Exchange
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 Terminbörse
European Opinions Exchange
Finaciele Termijnmarkt, Amsterdam
Finnish Options Market
Hong Kong Futures Exchange
Hong Kong Stock Exchange
International Securities Market Association
Irish Futures and Options Exchange (IFOX)
Johannesburg Stock Exchange
Kansas City Board of Trade
Korea Stock Exchange
Marché des Options Négociables de Paris (MONEP)
Marché à Terme International de France
MEFF Renta Fija

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

3. Approved Exchanges

Amsterdam Stock Exchange (Amsterdamse Effectenbeurs)
Antwerp Stock Exchange (Effectenbeurs vennootschap van Antwerpen)
Association 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
Belgium Futures & Options Exchange (BELFOX)
Berlin Stock Exchange (Berliner Börse)
Bergen Stock Exchange (Bergen Bors)
Bhubaneswar S.E. Assoc. Ltd.
Bilbao Stock Exchange (Borsa de Valores de Bilbao)
Bologna Stock Exchange (Borsa Valori de Bologna)
Bolsa de Mercadorios & Futures (BM & F)
Bolsa de Comercio de Buenos Aires (The Buenos Aires Stock Exchange)
Borsa Istanbul
Bordeaux Stock Exchange (Bourse de Bordeaux)

Boston Stock Exchange
Bovespa (São Paulo Stock Exchange)
Bremem Stock Exchange (Bremener Werkpapierbörse)
Brussels Stock Exchange (Société de la Bourse des Valeurs Mobilieres/Effecten Beursvennootschap van Brussels)
Bursa Malaysia Berhad
BVRJ (Rio de Janeiro Stock Exchange)
Calcutta Stock Exchange Assoc. Ltd.
Cincinnati Stock Exchange
Cochin Stock Exchange Ltd.
Coimbatore Stock Exchange
Copenhagen Stock Exchange (Kobenhavns Fondsbors)
Delhi Stock Exchange Assoc. Ltd.
Dusseldorf Stock Exchange (Rheinisch - Westfälische Börse zu Dusseldorf)
Florence Stock Exchange (Borsa Valori di Firenze)
Frankfurt Stock Exchange (Frankfurter Wertpapierbörse)
Fukuoka Stock Exchange
Gauhati Stock Exchange Ltd.
Geneva Stock Exchange
Genoa Stock Exchange (Borsa Valori di Genoa)
Hamburg Stock Exchange (Hanseatische Vertpapier Börse Hamburg)
Hannover SE (Niedersachsische Börse zu Hannover)
Helsinki Stock Exchange (Helsingen Arvopaperipörssi Osuuskunta)
Hyderabad Stock Exchange Ltd.
Inter-connected Stock Exchange of India
Jaipur Stock Exchange Ltd.
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
Malta Stock Exchange
Madras Stock Exchange Ltd.
Madrid Stock Exchange (Borsa de Valores de Madrid)
Madhya Pradesh Stock Exc Ltd.
Magadh Stock Exchange Association
Mangalore Stock Exchange Ltd.
Marseilles Stock Exchange
Mercato Italiano Futures (MIF)
Mid West Stock Exchange
Milan Stock Exchange (Borsa Valores de Milano)
Munich Stock Exchange (Bayerische Börse 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 Palermo)
Prague Stock Exchange
Pune Stock Exchange Ltd.
Rome Stock Exchange (Borsa Valori di Roma)
Santiago Stock Exchange
Saurashtra Kutch Stock Exchange Ltd.
SIX Stock Exchange
Stock Exchange of Mauritius
Stockholm Stock Exchange (Stockholm Fondbörs)
Stuttgart Stock Exchange (Baden – Würtembergische Wertpapierbörse 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)
Trondhiem Stock Exchange (Trondheims Bors)
Turin Stock Exchange (Borsa Valori de Torino)
Uttar Pradesh Stock Exchange Assoc Ltd.
Vadodara Stock Exchange Ltd.
Valencia Stock Exchange (Borsa de Valores de Valencia)
Venice Stock Exchange (Borsa Valori de Venezia)
Vienna Stock Exchange
Warsaw Stock Exchange

4. EEA 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 Wertpapierborse)
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 le second marché et le nouveau marché de la bourse de valeurs mobilières de Bruxelles [Bourse de Bruxelles]
De Belgium future-en optiebeurs, afgekort Belfox/La bourse belge des futures et options, en abrégé Belfox.

De secondaire buiten-beursmarkt van de lineaire obligaties, der gesplitste effecten en de scharkistcertificaten/Le marché 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 le second marché de la bourse de Paris
Le nouveau marché
Le Monep

Germany

Berliner Wertpapierbörse (Amtlicher Handel, Geregelter Markt) (Berlin Stock Exchange)
Wertpapierbörse in Brenme (Amtlicher Handel, Geregelter Markt) (Bremen Stock Exchange Dusseldorf)
Rheinisch - Westfälische Börse zu Düsseldorf (Amtlicher Handel, Geregelter Markt) (Rhine - Westphalian Stock Exchange Dusseldorf)
Frankfurter Wertpapiernbörse (Amtlicher Handel, Geregelter Markt) (Frankfurt Stock Exchange)
Deutsche Terminbörse (DTB)
Hanseatische Wertpapierbörse Hamberg (Amtlicher Handel, Geregelter Markt) (Hanseatic Stock Exchange Hamburg)
Niedersächsische Börse (Amtlicher Handel, Geregelter Markt) (Amstock Exchange of Lower Saxony (Hanover))
Bayerishce Börse (Amtlicher Handel, Geregelter Markt) (Bavarian Stock Exchange (Munich))
Baden - Württembergische Wertpapierbörse (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'artocolo 1, cooma 1, lettere (f) e (i), del d. lgs. n.415/1996 (IDEM)
Mercato all'ingresso dei titoli di Stato di cul al decreto del Ministro del Tesoro 24 febbraio 1994 (MTS)
Mercato dei contratti uniformi a termine sui titoli di Stato di cui al decreto del Ministro del Tesoro 24 febbraio 1994 (MIF)

Luxembourg

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

Malta

Malta Stock Exchange

The Netherlands

Amsterdam Exchanges (Amsterdamse effectenbeurs)
EOE-optiebeurs

Norway

The Oslo Stock Exchange

Portugal

Mercado de Cotações Oficiais da Bolsa de Valores de Lisboa (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 Cotações 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
AIAF, 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 B

COUNTRIES AND TERRITORIES WITH LEGISLATION/STATUS/ PROCEDURES EQUIVALENT TO OURS

COUNTRIES AND TERRITORIES WITH LEGISLATION/STATUS/PROCEDURES EQUIVALENT TO OURS

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

APPENDIX C

GROUP INTRODUCERS CERTIFICATE

GROUP INTRODUCERS CERTIFICATE

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 either the consolidated supervision of [……] located in [……] or is subject to the anti-money laundering regulations 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 due diligence as required by Group standards and by local law in the area of establishment of identity for the purposes of combating money laundering has been satisfactorily undertaken.

2. There is sufficient information on file at the above group company to establish the ownership of the *Applicant*, if a corporate entity, or the customer's true name and address of a natural person.

3. A certificate/summary sheet containing all relevant identification data and other information pertaining to the *Applicant* is enclosed herewith.

4. The underlying records of identity and copies of the documentary evidence held by us will, upon request, be made available to the financial institution without delay.

5. *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 or any other form of criminal conduct. Should *I/we* subsequently become so suspicious, *I/we* shall inform you immediately.

6. *I/we* undertake to advise the ……..Department 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: ……..

Department: …… Date: …….

APPENDIX D

ELIGIBLE INTRODUCERS CERTIFICATE

ELIGIBLE INTRODUCERS 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 Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism issued by the Bank of Mauritius, as amended from time to time, or *equivalent legislation:*

1 We have verified the identity of the Applicant and confirm that documentary evidence has been obtained and identity checks have been undertaken to confirm that the Applicant(s) name(s) and address(es) as shown on the Applicant form(s) is/are correct.

2 A certificate/summary sheet containing all relevant identification data and other information pertaining to the *Applicant* is enclosed herewith.

3 The underlying records of identity and copies of the documentary evidence held by us will, upon request, be made available to the financial institution without delay.

AND

4. 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.

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

Full Name of Regulated Introducer: ……..…….

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

Licence or Registration No: …….……

Signed: …… Full Names: ……

Job Titles: ……..….. Date: ……

APPENDIX E

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.

In order to protect the international financial system from money laundering and financing of terrorism (ML/FT) risks and to encourage greater compliance with the AML/CFT standards, the FATF identified jurisdictions that have strategic deficiencies and works with them to address those deficiencies that pose a risk to the international financial system.

The FATF has identified the following jurisdictions as posing a risk to the international financial system.[25]

Jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the on-going and substantial money laundering and terrorist financing (ML/FT) risks emanating from the jurisdictions.
Democratic People's Republic of Korea (DPRK)
Jurisdictions subject to a FATF call on its members and other jurisdictions to apply enhanced due diligence measures proportionate to the risks arising from the jurisdiction
Iran
Jurisdictions with strategic deficiencies
Bosnia and Herzegovina Ethiopia Iraq Syria Uganda Vanuatu Yemen

[25] FATF Public Statement issued on 23 June 2017.

APPENDIX F

EXAMPLES OF SUSPICIOUS TRANSACTIONS (MONEY LAUNDERING)

EXAMPLES OF SUSPICIOUS TRANSACTIONS (MONEY LAUNDERING)

1. Money laundering using cash transactions

(a) Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

(b) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

(c) Customers who deposit cash by means of numerous credit slips so that the amount of each deposit is unremarkable, but the total of all the credits is significant, or similar deposits at a number of branches within a short space of time, all being credited to a central account.

(d) Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.).

(e) Customers who constantly pay in or deposit cash to cover requests for money transfers, bankers' drafts or other negotiable and readily marketable money instruments.

(f) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

(g) Frequent exchange of cash into other currencies.

(h) Branches that have a great deal more cash transactions than usual.

2. Money laundering using bank accounts

(a) Customers who wish to maintain a number of trustee accounts which do not appear consistent with the type of business, including transactions which involve nominees.

(b) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

(c) Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

(d) Paying in large third party cheques endorsed in favour of the customer.

(e) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

(f) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

(g) Greater use of safe deposit facilities. The use of sealed packets deposited and withdrawn.

(h) Companies' representatives avoiding contact with the branch.

(i) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client, company and trust accounts.

(j) Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

(k) Insufficient use of normal banking facilities (e.g. avoidance of high interest rate facilities for large balances).

(l) Large number of individuals making payments into the same account without an adequate explanation.

3. Money laundering by offshore international activity

(a) Customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.

(b) Use of letters of credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

(c) Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs and/or proscribed terrorist organisations.

(d) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer of account(s) held overseas.

(e) Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.

(f) Frequent requests for traveller's cheques, foreign currency drafts or other negotiable instruments to be issued.

(g) Frequent paying in of traveller's cheques or foreign currency drafts, particularly if originating from overseas.

4. Money laundering involving financial institution employees and agents

(a) Changes in employee characteristics (e.g. lavish lifestyles).

(b) Changes in employee or agent performance (e.g.. the salesman selling products for cash has remarkable or unexpected increase in performance).

(c) Any dealing with an agent where the identity of the ultimate beneficiary or counterparty is undisclosed, contrary to normal procedure for the type of business concerned.

(d) Overbilling Schemes, whereby materials ordered for a purchase are of a poorer quality and lower price that what was specified, but this is not reflected in the negotiated contract.

(e) Corporate crime against the interests of shareholders and of the public at large.

(f) Admissions or statements by directors, officers or employees to law practitioners of their or their company's involvement in criminal activities.

5. Money laundering by secured and unsecured lending

(a) Customers who repay problem loans unexpectedly.

(b) Request to borrow against assets held by the institution or a third party, where the origin of the assets is not reasonably known or the assets are inconsistent with the customer's standing.

(c) Request by a customer for an institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

6. Sales and dealing staff

(a) New business

(i) A client with no discernible reason for using the firm's services, e.g. clients with distant addresses who could find the same service nearer their home base; clients whose requirements are not in the normal pattern of the firm's business which could be more easily serviced elsewhere.

(ii) An investor introduced by an overseas bank, affiliate or other investor both of which are based in countries where production of drugs or drug trafficking may be prevalent.

(iii) Any transaction in which the counterparty to the transaction is unknown.

(b) Intermediaries

There are many clearly legitimate reasons for a client's use of an intermediary. However, the use of intermediaries does introduce further parties into the transaction thus increasing opacity.

Any apparently unnecessary use of an intermediary in the transaction should give rise to further enquiry.

7. Potentially Suspicious Circumstances - Trust Companies

The following are examples of potentially suspicious circumstances which may give rise to a suspicion of money laundering in the context of Trust Companies:

Suspicious Circumstances Relating to the Customer/Client's behaviour

(a) The establishment of Companies or Trusts which have no obvious commercial purpose

(b) Clients/customers who appear uninterested in legitimate tax avoidance schemes

(c) Sales invoice totals exceeding the known value of goods

(d) The client/customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, bankers drafts etc.

(e) The customer/client pays either over the odds or sells at undervaluation

(f) Customers/clients have a myriad of bank accounts and pay amounts of cash into all those accounts which, in total, amount to a large overall sum

(g) Customers/clients transferring large sums of money to or from overseas locations with instructions for payment in cash (h) The payment into bank accounts of large third party cheques endorsed in favour of the client/customer.

Potentially Suspicious Secrecy may involve the following:

(a) The excessive or unnecessary use of nominees

(b) The unnecessary granting of wide ranging Powers of Attorney

(c) The utilisation of a client account rather than the payment of things directly

(d) An unwillingness to disclose the sources of funds

(e) The use of a mailing address

(f) The tardiness and/or unwillingness to disclose the identity of the ultimate beneficial owners or beneficiaries.

Suspicious Circumstances in Groups of Companies and/or Trusts:

(a) Companies which continually make substantial losses

(b) Complex group structures without a cause

(c) Subsidiaries which have no apparent purpose

(d) A frequent turnover in shareholders, directors or trustees

(e) Uneconomic group structures for tax purposes

(f) The use of bank accounts in several currencies for no apparent reason

(g) The existence of unexplained transfers of large sums of money through several bank accounts.

(h) A medium sized corporate customer, shortly before going into voluntary liquidation, sells its prime asset at apparently less than market value. At around the same time less desirable assets are purchased by the company from interests which it is suspected are associated with the directors and at prices which according to your information are well in excess of their true value.

(i) The payment of secret commissions.

(j) Skimming of profits to executive directors.

(k) Directors or management fraudulently acting against the interests of their company.

(l) Payment of large management fees to entities associated with directors or management.

It should be noted that none of these factors on their own necessarily mean that a customer/client or any third party is involved in any money laundering. However, in most circumstances a combination of some of the above factors should arouse suspicions. In any event, what does or does not give rise to a suspicion will depend on the particular circumstances.

APPENDIX G

EXAMPLES OF SUSPICIOUS TRANSACTIONS (FINANCING OF TERRORISM)

EXAMPLES OF SUSPICIOUS TRANSACTIONS (FINANCING OF TERRORISM)

A. Accounts

(1) Accounts that receive relevant periodical deposits and are dormant at other periods. These accounts are then used to create a legitimate appearing financial background through which additional fraudulent activities may be carried out.

(2) A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

(3) When opening an account, the customer refuses to provide information required by the financial institution, attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify.

(4) An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).

(5) An account opened by a legal entity or an organisation that has the same address as other legal entities or organisations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.).

(6) An account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits is made in comparison with the income of the founders of the entity.

(7) The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.

(8) An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organisation.

(9) An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organisation and that shows movements of funds above the expected level of income.

B. Deposits and withdrawals

(1) Deposits for a business entity in combinations of monetary instruments that are atypical of the activity normally associated with such a business (for example, deposits that include a mix of business, payroll and social security cheques).

(2) Large cash withdrawals made from a business account not normally associated with cash transactions.

(3) Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in cheques or other payment instruments.

(4) Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.

(5) Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.

(6) The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.

(7) The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

(8) The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.

(9) The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

C. Wire Transfers

(1) Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

(2) Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.

(3) Use of multiple personal and business accounts or the accounts of non-profit organisations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

(4) Foreign exchange transactions that are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern.

D. Characteristics of the customer or his/her business activity

(1) Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types.

(2) Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.).

(3) Stated occupation of the transactor is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

(4) Regarding non-profit or charitable organisations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

(5) A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

(6) Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

E. Transactions linked to locations of concern

(1) Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).

(2) Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).

(3) A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern.

(4) The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern.

(5) A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations.

(6) The opening of accounts of financial institutions from locations of specific concern.

(7) Sending or receiving funds by international transfers from and/or to locations of specific concern.

APPENDIX H

POLITICALLY EXPOSED PERSONS (PEPs)

POLITICALLY EXPOSED PERSONS

'natural persons who are or have been entrusted with prominent public functions' shall include the following:

Domestic PEPs

1. President/Vice President of Republic of Mauritius
2. All members of the National Assembly and the Speaker
3. Chief Judge and Senior Puisne Judge
4. Director of Public Prosecutions
5. Attorney General
6. Commissioner of Police/Prison
7. Leaders and Senior Office Bearers of major Political Parties
8. Members of Rodrigues Regional Assembly
9. Governor/Deputy Governors of the Central Bank
10. Chairman and Chief Executive Officers of Parastatal Organisations, Independent Bodies and State- Owned Enterprises
11. Commissioners of Various Government Bodies
12. Advisor/ Counsellor to Heads of States and Ministers
13. Head of Mauritian Embassies abroad, Consulates and Diplomats
14. Mayors and President of District Councils
15. Head of National Secret Services

Foreign PEPs

1. Heads of state, heads of government, ministers and deputy or assistant minister
2. Members of parliament or of similar legislative bodies
3. Members of the governing bodies of political parties
4. Members of supreme courts, constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances
5. Members of courts of auditors or of the boards of central banks
6. Ambassadors, chargés d'affaires and high-ranking officers in the armed forces
7. Members of the administrative, management or supervisory bodies of state-owned enterprises
8. Directors, deputy directors and members of the board or equivalent function of an international organisation.

SOURCES OF INFORMATION

1. Anti-Money Laundering Guidance Notes for the Finance Sector issued by the Jersey Financial Services Commission

2. Guidance for Financial Institutions in detecting Terrorist Financing issued by the Financial Action Task Force (FATF)

3. Sound management of risks related to money laundering and financing of terrorism Guidelines issued by the Basel Committee on Banking Supervision in February 2016

4. FATF Member States

5. FATF Public Documents identifying jurisdictions that may pose a risk to the international financial system, namely:

   (i) Jurisdictions with strategic anti-money laundering and combating the financing of terrorism (AML/CFT) deficiencies for which a call for action applies ;

   (ii) Jurisdictions with strategic AML/CFT deficiencies for which they have developed an action plan with the FATF .

6. FATF Recommendations, Guidance, Reports, Papers and methodology issued from time to time

7. EU directives on AML/CFT

8. Guidance Notes issued by the Mauritius FIU