GUIDELINES ON THE MEASURES FOR THE PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM FOR THE REAL ESTATE SECTOR

Issued pursuant to Section 10(2)(ba) of the Financial Intelligence and Anti Money Laundering Act 2002

MAY 2020

DISCLAIMER

These Guidelines are intended to provide assistance to real estate agents(hereinafter referred to as Agents) in meeting their obligations under the Financial Intelligence and Anti Money Laundering Act (FIAMLA), United Nations(Financial Prohibitions, Travel Ban and Arms Embargo) Sanctions Act 2019 (UN Sanctions Act) and the Financial Intelligence and Anti Money LaunderingRegulations 2018 (FIAML Regulations). If you are unsure about your obligations in a given case, you should consider taking independent legal advice.

The Guidelines must be read in conjunction with the Financial Intelligence and Anti-Money Laundering Act 2002, Prevention of Corruption Act 2002, Prevention of Terrorism Act 2002, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, the Convention of the Suppression of the Financing of Terrorism Act and the Financial Intelligence and Anti-Money Laundering Regulations 2018.

Note: For the purposes of these Guidelines, the term "Real Estate Agent" is used throughout the document to collectively refer to Land and/or Building or Estate Agencies, LandPromoters and PropertyDevelopers.

ACRONYMS

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
CDD	Customer Due Diligence
CO	Compliance Officer
DNFBPs	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FIAMLA	Financial Intelligence Anti-Money Laundering Act
FIU	Financial Intelligence Unit
ML	Money Laundering
NRA	National Risk Assessment
PCPs	Policies, Controls and Procedures
PEP	Politically Exposed Person
PF	Proliferation Financing
STR	Suspicious Transaction Report
TF	Terrorism Financing

TABLE OF CONTENTS

1 Introduction

Money laundering, terrorism and proliferation financing have far reaching consequences for a country's financial system and economy. With these crimes becoming increasingly cross border in nature, jurisdictions must equip themselves to protect the integrity of their financial systems and must also be prepared to deal with any abuses which are encountered. In order to achieve this, there are several building blocks which are required. The first is a sound and robust legal framework, which empowers institutions and lays down the obligations of all parties concerned. The second is an open and collaborative approach between AML/CFT supervisors and the reporting persons that they regulate. Additionally, there must be a willingness from the sectors which are regulated to understand their obligations and to accept that they also have to contribute to the fight against ML and TF. Against this background, the FIU, as the AML/CFT regulator for the real estate sector, firmly believes that one crucial way through which ML and TF can be curbed, is through the implementation of strong controls, policies and procedures by real estate agents. These act as a line of defence in ensuring that our real estate industry does not become a haven for criminals. The purpose of these guidelines is to assist the sector in establishing strong systems and in becoming partners in the fight against ML and TF. Its objective is also to help the sector in understanding its AML/CFT obligations.

1.1The Mauritian AML/CFT LegislativeFramework

Mauritius has taken significant steps to ensure that it has a robust AML/CFT legal framework which is aligned with international standards. The FIAMLA was enacted in 2002 and provided for several of the key requirements of a strong AML/CFT system. It has been amended to ensure that Mauritius meets its international obligations. Among other things, the FIAMLA makes provision for an independent FIU, the obligation of filing suspicious transaction reports, CDD obligations as well as a framework for the AML/CFT supervision of DNFBPs.

In 2018, the FIAML Regulations 2018 were made and revoked the then 2003 FIAML Regulations. The 2018 Regulations make extensive provision in relation to the measures which must be put in place by reporting persons (which includes real estate agents) to ensure that they are complying with the requirements of the law and that they are taking the required steps to safeguard their businesses from ML/TF abuses.

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019

(henceforth referred to as the 'UN Sanctions Act') was also passed in May 2019. This act enables Mauritius to implement the measures under all the United Nations Security Council Resolutions and deal with other matters of international concern, and to give effect to Article 41 of the Charter of the United Nations.

Copies of the above legislation are available on the FIU's website: www.fiumauritius.org.

1.2Purpose and Scope of theGuidelines

Real estate agents may become a preferred choice for criminals for hiding illicit gains. This arises because of a number of factors such as the relatively high monetary value of the transactions conducted, the appreciation of the assets' value over time and the opportunity to conceal ownership. Real Estate Agents are involved in the vast majority of real estate transactions in Mauritius and, therefore, can play a key role in detecting money laundering and financing of terrorism and proliferation schemes involving the real estate industry. Given that they are in direct contact with clients (either buyer and/or sellers), they generally know their clients better than the other parties in the transactions. Therefore, they are well placed to detect any suspicioustransaction/activity.

This document has been issued pursuant to section 10(2)(ba) of the Financial Intelligence and Anti Money Laundering Act (FIAMLA) 2002. They are intended to assist real estate agents in complying with their obligations in relation to the prevention, detection and reporting of money laundering, financing of terrorism and proliferation. Through compliance with their obligations, the real estate profession can safeguard that it is not misused by money launderers or those financing terrorism or proliferation.

1.3Businesses and Individuals covered by theGuidelines

This guideline is addressed to the following:

- Agents in Land/or Building or Estate Agency under the Local GovernmentAct and
- Land Promoters and Property Developers under the Local GovernmentAct who are involved in transactions for a client, with respect to both the purchaser and the vendor, concerning the buying and selling of real estate.

1.4The Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) was established in 1989 by the G7countries. It is an inter-governmental body whose purpose is to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, financing of terrorism and other related threats to the integrity of the international financial system.

As a member of the Eastern and Southern Africa Anti-Money Laundering Group, Mauritius has made the commitment to implement these standards into its domestic AML/CFT framework.

1.5The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)

The ESAAMLG was founded in 1999 and its main objective is to ensure that its Members comply with the FATF standards. Assessment for compliance with the FATF Recommendations is done through the Mutual Evaluation Process following which a Mutual Evaluation Report (MER) is prepared and posted on the ESAAMLG's website. The most recent MER of Mauritius can be accessed on the FIU Website.

1.6Compliance with Guidelines andEnforcement

As the AML/CFT regulator for real estate, the FIU is mandated to ensure compliance by real estate agents with the FIAMLA, the UN Sanctions Act, and any regulations and guidelines issued under these Acts. Following legal amendments made in May 2019, FIU has been further empowered, and provided with significant powers to enforce compliance by the sector. The FIU is now able to:

- give directions to members falling under their respective purview;
- require members to submit a report on corrective measures it is taking to ensure compliance with the relevant legislation;
- take administrative sanctions as provided for by FIAMLA;
- revoke or cancel licences, approvals or authorization as the case may be; and
- request information or records from its members in the discharge of its functions.

1.7The Financial Intelligence Unit (FIU)

The FIU Mauritius was set up in August 2002 under the provisions of section 9 of the FIAMLA. It is the central agency in Mauritius responsible for receiving, requesting, analyzing and disseminating to the investigatory, supervisory authorities[1], Registrars and overseas FIU disclosures of information regarding suspected proceeds of crime and alleged money laundering offences as well as the financing of any activities or transactions related to terrorism to relevant authorities.

[1]Investigatory authorities" include the Commissioner of Police, the Director, The Mauritius Revenue Authority, the Enforcement Authority and the ICAC and "supervisory authorities" include the Bank of Mauritius, the Financial Services Commission, the GRA, the FIU, the Mauritius Institute of Professional Accountants, the Attorney General's Office and the Registrar of Companies.

2. Money Laundering and Financing ofTerrorism and Proliferation

2.1 Money Laundering

Money laundering is the process intended to disguise the illegal origin of proceeds of crime in order to make them appear legitimate. If undertaken successfully, it allows criminals to maintain control over proceeds of criminal activities and, ultimately, provide a legitimate cover for these activities. The process is often carried out in three stages:

(1) Placement

This initial stage involves the introduction of criminally tainted money into the financial system. The launderer seeks to introduce illegal proceeds into the financial system by, for example breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (e.g. cheques etc.) that are then collected and deposited into accounts at another location.

(2) Layering

The layering stage is the dissociation of the dirty money from their source through a series of transactions to obscure the origins of the proceeds. These transactions may involve different entities such as companies and trusts as well as different financial assets such as shares, securities, properties or insurance products. It is the separation of benefits of drug trafficking or criminal conduct from their source by creating layers of financial transactions designed to disguise the audit trail. Illustratively, the launderer may engage in a series of conversions or movements of the funds to distance them from their source. (e.g. buying and selling of stocks, commodities or properties, buying precious metals or stones with cash, taking out and repaying a loan, use of gatekeepers and their services to buy and sell assets etc). The funds might even be channelled through the purchase and sale of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services or use gatekeepers to carry out such transactions, thus giving them a legitimate appearance.

(3) Integration

The integration stage is the use of the funds in the legitimate economy through for instance, investment in real estate or luxury assets. Essentially, it is the provision of apparent legitimacy to benefits of drug trafficking or other illegal activities. If the layering process has been successful, the integration schemes thus place the laundered funds back into the economy so that they re-enter the financial system appearing as legitimate business funds. They can then be used for legitimate purchase of luxury goods, real estate and soon.

2.2 Financing of Terrorism

Financing of terrorism is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike money laundering, funds can come from both legitimate sources as well as from criminal activity for the financing of terrorism. Funds may also originate from personal donations, profits from businesses and charitable organizations but all the funds are actually used to finance terrorism. Funds may come, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Unlike money laundering, which precedes criminal activity, with financing of terrorism, it is possible to have fundraising or a criminal activity generating funds prior to the terrorist activity actually taking place. However, similar to money launderers, those financing terrorism also move funds to conceal their source of those funds. The motive is to prevent leaving a trail of incriminating evidence.

2.3 Proliferation Financing

Proliferation of weapons of mass destruction (“WMDs”) can be in many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long-range missiles). Proliferation of WMD financing is an important element and, as with international criminal networks, proliferation support networks may use the international financial system to carry out transactions and business deals. Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organizations or acting as representatives or middlemen.

3. Risk-Based Approach

3.1 Adopting a risk-based approach

Recommendation 1 of the FATF focuses on assessing risks and applying a risk-based approach. Based on the findings of the first national ML and TF risk assessmentof Mauritius, which was completed in August 2019, the ML risk[2] associated with theReal Estate sector was found to be Medium-High. The level of ML threat was rated Medium. Themost recurrent predicate offences associated with the sector are drug trafficking and embezzlement.Alternatively, the following factors make the sector inherently vulnerable to money laundering:

(a) the client-base profile of the sector, which includes domestic politically exposed persons, high-net worth individuals, non-resident clients, clients with criminal records or past administrative and/or supervisory actions against them and legal entities;
(b) the use of cash;
(c) the anonymous use of the product – purchase of immoveable properties through *prêtes-noms*; and
(d) the relative difficulty of tracing transaction recordsdue to an absence of CDD measures[3].

It is an obligation for real estate agents to identify, assess and understand their ML/TF risk pursuant to Section 17 of FIAMLA.It is highlighted that real estate agents should take into account the

[2]For the purpose of assessing money laundering and terrorism financing risks, risk is defined as a function of threat, vulnerability and consequence.

- A threat is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities.

- Vulnerabilities comprise those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at vulnerabilities means focusing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes.

- Consequence refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally.

[3] At the time of the NRA, there was no legal requirement to conduct CDD measures for agents. However, this is no longer the case now as extensive CDD obligations have now been provided for in the FIAMLA and the FIAMLA Regulations which apply to agents.

outcome of the National Risk Assessment[4] when applying CDD measures in relation to each customer.

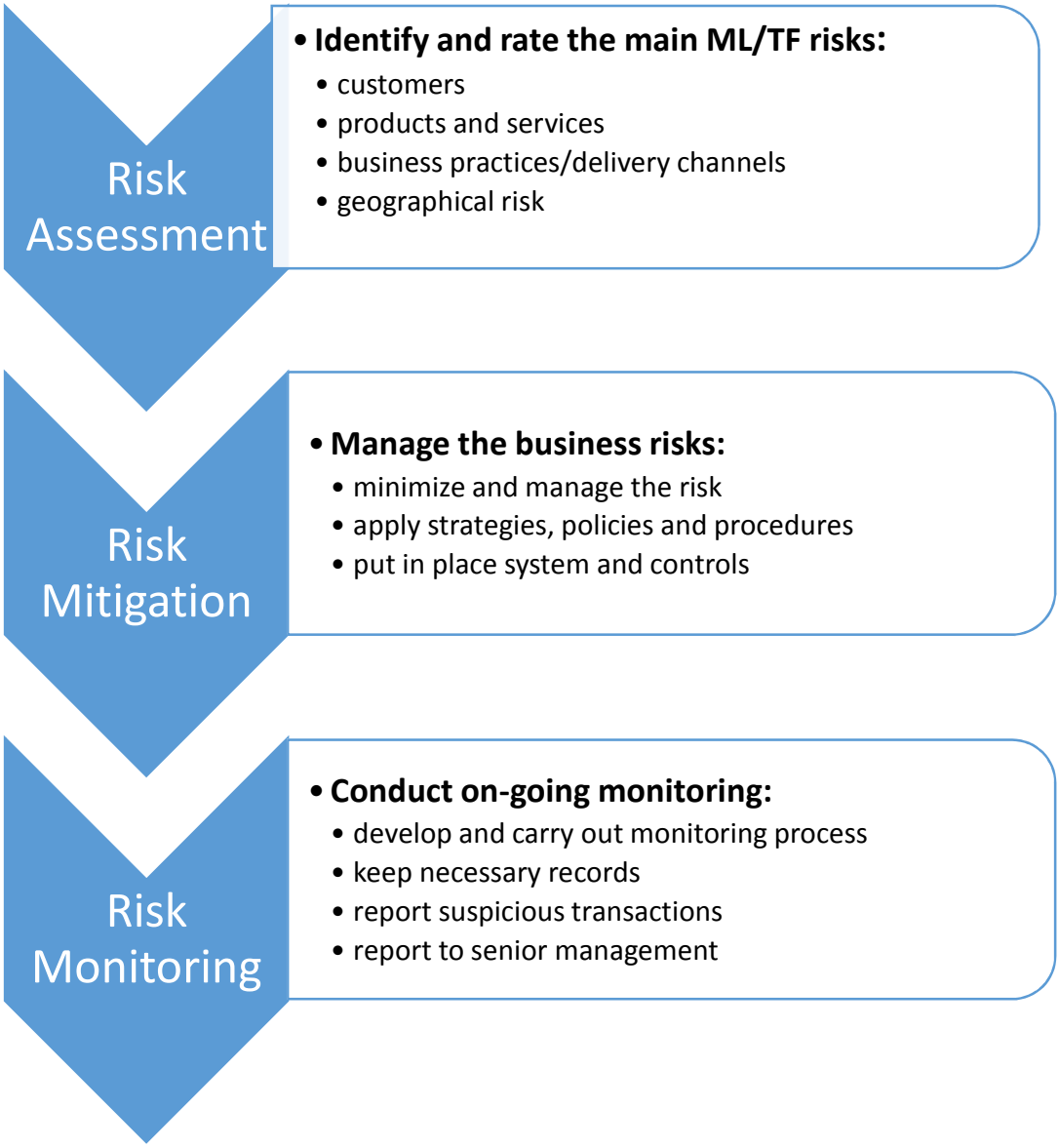
A risk-based approach also requires real estate agents to have systems and controls that are commensurate with the specific risks of money laundering and financing of terrorism facing them. Assessing this risk is, therefore, one of the most important steps in creating a good anti-money laundering compliance program.

As money laundering risks increase, stronger controls are necessary. However, all categories of risk — whether low, medium or high — must be identified and mitigated by the application of controls, such as verification of customer identity, CDD policies, suspicious activity monitoring and checking list of people on whom sanctions have been applied or being applied. A risk-based approach should be flexible, effective andproportionate.

It is important to note that pursuant to section 3(2) of FIAMLA, real estate agents are required to take such measures that are necessary to ensure that their services are not being misused to commit a money laundering or the financing of terrorism offence. The penalty for such an offence is a fine not exceeding 10million rupees and penal servitude for a term not exceeding 20years. No real estate agent can reasonably be expected to detect all wrongdoing by clients, including money laundering. However, if any real estate agent develops systems and procedures to detect, monitor and report the riskier clients and transactions, he will reduce its chances of being misused by criminals.

There are three steps to establishing a risk-based approach: risk assessment, risk mitigation and risk monitoring. The following diagram depicts visually the three different steps in implementing a risk-based approach.

[4] The public version of the NRA report may be accessed here: http://www.fiumauritius.org/English//DOCUMENTS/NRA%20FINAL%20REPORT.PDF


Risk Assessment
• Identify and rate the main ML/TF risks:
• customers
• products and services
• business practices/delivery channels
• geographical risk
Risk Mitigation
• Manage the business risks:
• minimize and manage the risk
• apply strategies, policies and procedures
• put in place system and controls
Risk Monitoring
• Conduct on-going monitoring:
• develop and carry out monitoring process
• keep necessary records
• report suspicious transactions
• report to senior management

3.1.1 Risk Assessment

Agents can assess money laundering and terrorist financing risks by using various categories. The application of risk categories provides a strategy for managing potential risks by enabling agents to subject each customer to reasonable and proportionate risk assessment

3.1.1.1 Criteria to determine Risk

The risks the sector faces depend on variety of factors, namely:

- The client base;
- The services and products provided;
- Geographic location; and
- Delivery channels and business practices

The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may vary from one agentto another, depending upon their respective circumstances. The categories however should be considered holistically and not in isolation. The risk categories may be broken down into different levels of risks and they also help to determine the rigidity of your policies and procedures.

(a) Risk of Client Base

The levels of risks associated with the client base could include for example, (i) **prohibited** clients (i.e., clients that are prime candidates for prohibited transactions, a list of designated persons/ entities on any sanctions Lists such as the Un Sanctions List[5], persons whose assets may have been frozen under section 45 of the Dangerous Drugs Act, (ii) clients considered as **high risk** (for example, Politically Exposed Persons), (iii) **medium risk** client, (iv) **low/standard** risk client.

The type of client may also pose ML/FT risks, e.g., individuals, listed companies, private companies, joint ventures, partnerships, etc. The following is a list of type of clients and the level of risks associated with them. Note that this is not a prescriptive list nor does it imply that the risk is the same across the real estate sector, i.e., it may be low risk for one real estate agent and considered as high risk for another.
Identification of high-risk clients may be based on thefollowing:

[5] These lists may be accessed on the FIU website here:
http://www.fiumauritius.org/English/United%20Nations%20Security%20Council/Pages/default.aspx

- Unusual involvements of third parties;
- Titling a residential property in the name of third party; for example, a friend, relative, business associate, orlawyer;
- Use of legal entities (corporations, LLCs or partnerships) that obscure the identity of the person who owns or controls them without a legitimate businessexplanation;
- Non face to faceclient;
- Politically exposed persons (PEPs);
- Persons whose assets have been frozen under section 45 of the Dangerous Drugs Act or whose assets have been temporarily or permanently confiscated under the Asset Recovery Act;
- Persons who appear on the UN Sanctions list or any domestic terrorist list pursuant to the UN Sanctions Act; and
- Clients with an affiliation to countries with high levels of corruption or having known associations with terroristorganizations.

(b) Risk of Products/Services

An essential element of risk assessment is to review new and existing services that the real estate agents offer to determine how they may be used to launder money or finance terrorism**.** For instance, some services can be used to conceal the ownership or the source of property, such as:

- Services in relation to complex transactions/ enabling significant volumes of transactions to occur rapidly;
- Services allowing customer to engage in transactions with minimal oversight by the institution; and
- Services allowing levels of anonymity to theusers.

Given the nature of services offered by real estate agents, they may be exposed to transactions risks such as:

- Under or over-valued properties (E.g., is the property owner selling the property for significantly less than the purchaseprice);
- Disinterest in obtaining a betterprice;
- Use of large amounts ofcash;

- Buyer brings actual cash to theclosing;
- The purchase of a property without a mortgage, where it does not match the characteristics of thebuyer;
- Property purchases inconsistent with the individual's occupation orincome;
- Immediate resale of theproperty;
- Difficulties in obtaining identification documents; and
- Purchases being made without viewing the property, no interest in the characteristics of theproperty.

(c) *Geographical Locations of the Business/Clients/Products being used*

There is no unique definition of what consists a high-risk country or geographic location. However, there are several factors which can be considered when assessing whether a particular country or location presents higher risk. It is important to conduct such an assessment to ensure that agents do not engage in transactions emanating from such countries or, if they do, that they have well established controls and procedures to mitigate the associated risk. Geographic location is generally accepted as a contributing factor to the level of risk. However, there is no definite, independent system for assessing the money laundering risks of various territories.

Accordingto guidance provided by the FATF[6], factors that are generally agreed to place a country in a higher risk category include:

a) Countries/areas identified by credible sources[7] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

b) Countries identified by credible sources as having significant levels of organised crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.

c) Countries subject to sanctions, embargoes or similar measures issued by international

[6] https://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Guidance%20for%20Real%20Estate%20Agents.pdf at paragraphs 108 and 109.

[7] "Credible sources" refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units.

organisations such as the United Nations.

d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, and in relation to which financial institutions (as well as DNFBPs) should give special attention to business relationships and transactions.[8]

e) Countries identified by credible sources to be uncooperative in providing beneficial ownership information to competent authorities, a determination of which may be established from reviewing FATF mutual evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards

(d) Business Practices/Delivery Channels

Real estate agents should also consider the channels used to deliver their products or services. In today's economy and global market, many delivery channels do not bring the client into direct face-to-face contact with the reporting entity (for example, Internet, telephone or mail), and are accessible 24 hours a day, 7 days a week, from almost anywhere. The remoteness of some of these distribution channels can also be used to obscure the true identity of a client or beneficial owners and can therefore pose higher risks. The examination of business practices and delivery channels should also include conducting a risk assessment of any new technologies (e.g. Internet based services) that you are planning to implement. The risk assessment should be conducted prior to the new technology being implemented.

3.1.1.2 Risk Assessment Tool

A risk assessment tool at Annex 1 provides an example, for use by real estate agents, to facilitate the assessment of the above factors. However, a real estate agent's risk assessment has to be appropriate for their specific business needs which means that it may have to be more detailed than the checklist provided. Real estate agents can customize the checklist or can use a different method or another tool.

3.1.2Risk Mitigation

[8]The link to FATF statements may be consultedhere:https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

The second component of a risk-based approach is risk mitigation. Risk mitigation is about implementing measures to limit the potential money laundering and terrorist financing risks the reporting entity has identified while staying within its risk tolerance level. Pursuant to section 17A of FIAMLA, agents must establish policies, controls and procedures to mitigate and manage the ML/TF risks that they have identified as part of their assessment.

As part of its internal controls, when the risk assessment determines that risks are higher for ML or TF, the reporting entity has to develop written risk mitigation strategies (policies and procedures designed to mitigate high risk) and apply them for high risk situations.

It is important that the risk mitigation strategies are developed by the agent for higher risk situations and that these mitigation strategies are documented. This allows the risk mitigation strategies to be shared with management and employees. Furthermore, the application of the mitigation strategies should be recorded to demonstrate that mitigation measures have been applied. Strong senior management leadership and engagement in AML/CFT is an important aspect of the application of the risk-based approach. Senior management should approve the risk mitigations strategies and ensure that they are reviewed every time the risk assessment is updated.

The development of a robust AML/CFT program is thus a crucial component of risk mitigation.

Risk mitigation strategies that can be applied have been identified at Annex 1.a.

3.1.3 Risk Monitoring

In addition to risk assessment and risk mitigation activities, a risk-based approach also requires agents to take measures to conduct on-going monitoring of financial transactions when there is a business relationship. The level of monitoring should be adapted according the ML/TF risks as outlined in the entity's risk assessment. The purpose of on-going monitoring activities is to help detect suspicious transactions. The agent's policies, controls and procedures have to determine what kind of monitoring is done for particular high-risk situations, including how to detect suspicious transactions. The policies, controls and procedures should also describe when monitoring is done (its frequency), how it is reviewed, and how it will be consistently applied.

4. Internal Controls

4.1 AML/CFT Program

An AML/CFT program is required to identify, mitigate and manage the risk of the products or services being offered by the agent that could facilitate money laundering or terrorism financing. Through an AML/CFT program, the agent is able to set out how it is going to implement its AML/CFT obligations.

As previously mentioned, AML/CFT programs should be risk-based. This means that agents must develop their own program, tailored to their situation to mitigate money laundering and terrorism financing risks. This approach recognizes that not all aspects of an institution' business present the same level of risks. The reporting person is in the best position to assess the risk of its clients, products and services and to allocate resources to counter the identified high-risk areas.

Although not exhaustive, the list below provides the basics of an AML/CFT program:

- Appointment of key officers
- Policies and Procedures
- Training
- Audit and Review

As mentioned at the start of this chapter, having an AML/CFT program enables the dealer to have a clear approach on how it is going to fulfill its AML/CFT obligations. These obligations are the following and are discussed in detail at Chapter 5 and6 of these guidelines:

- Customer Due Diligence (CDD)
- Record Keeping
- Enhanced Due Diligence (EDD)
- Politically Exposed Persons (PEPs)
- Ongoing Monitoring
- Suspicious Transaction Reporting
- Training
- Terrorism Financing Obligations

4.1.1 Appointment of Key Officers

Subject to the size and nature of their business, Agents are required to appoint both a compliance officer and a Money Laundering Reporting Officer (MLRO) as part of their internal procedures and controls.

4.1.1.1 The Compliance Officer

The compliance officer (CO), who must be part of senior management is responsible for ensuring that the agent is complying with its AML/CFT obligations.

The agent must ensure that the CO:

(a) has timely and unrestricted access to the records of the agent;
(b) has sufficient resources to perform his or her duties;
(c) has the full co-operation of the agent's staff;
(d) is fully aware of his or her obligations and those of the agent; and
(e) reports directly to, and has regular contact with, the Board (where applicable) so as to enable the Board to satisfy itself that all statutory obligations and provisions in FIAMLA and the Regulations issued thereunder, are being met and that the agent is taking sufficiently robust measures to protect itself against the potential risk of being used for ML and TF. Where there is no Board, the CO must report directly to the business owner or to any other senior officer appointed by the owner.

In accordance with Regulation22(3) of the FIAML Regulations 2018, the functions of the CO include:

(a) ensuring continued compliance with the requirements of the FIAMLA and FIAML Regulations 2018 subject to the ongoing oversight of the Board of the agentwhere applicable and senior management;

(b) undertaking day-to-day oversight of the program for combatting money laundering and terrorism financing;

(c) regular reporting, including reporting of non-compliance, to the Board where applicable and senior management; and

(d) contributing to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combatting money laundering and terrorism financing.

For the avoidance of doubt, the same individual can be appointed to the positions of Money Laundering Reporting Officer ("MLRO") and CO, provided the agent considers this appropriate with regard to the respective demands of the two roles and whether the individual has sufficient time and resources to fulfil both roles effectively.

4.1.1.2 The Money Laundering Reporting Officer

In accordance with Regulation 26(1) of FIAML Regulations 2018, the agent shall appoint a MLRO to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person gives rise to knowledge or reasonable suspicion that another person is engaged in money laundering or the financing of terrorism. The MLRO must be sufficiently senior within the organization and must have the technical skills required to make an assessment of internal reports prior to determining whether an STR should be filed with the FIU.

There should be clear reporting lines internally, to ensure that all employees including directors or partners, know what the process is to report any suspicion that they may have internally to the MLRO. Records must be kept by the agent of both internal and external disclosures.

Where due to its size or the nature of its business anagent cannot appoint an MLRO,it must nevertheless have documented policies and procedures in place to ensure that it is complying with the FIAMLA and the 2018 Regulations. In these instances, the STR is filed by the agent with the FIU directly.

4.1.2 Policies and Procedures

Agents should have in place adequate policies, controls and procedures(PCPs) that promote high ethical and professional standards and prevent their business from being misused by criminals.

PCPs should clearly document the steps which the agent intends to follow in the implementation of each element of its AML/CFT Program. The agent must for example have policies on employee screening and procedures detailing how it will meet the expectation set out in its policy.
These policies, procedures and internal controls should be efficiently introduced and maintained and each agent should be aware of his responsibilities. All these PCPs must be widely publicized across the agent's business and all its employees must be made aware of their role and existence. They should also be easily accessible across the business.

Annex 2 provides a template to assist agents in the development of internal policies, procedures and controls.

4.1.3Employment Screening and Training

4.1.3.1 Employment Screening

Agents are required, under Regulation 22(1)(b) of FIAML Regulations 2018, to implement programmes for screening procedures so that high standards are maintained when hiring employees.

In light of the above, significance may be givento:

- Obtaining and confirming proper references at the time ofrecruitment;
- Requesting information from the member of staff with regard to any regulatory action taken against him; and
- Requesting information from the member of staff pertaining to any criminal convictions and the provision of a check of his criminal record (for instance, requiring a Certificate of Character).

4.1.3.2 Employee Training

Regulation 22(1)(c) of FIAML Regulations 2018 states that programmes against money laundering and terrorism financing should be in place to include ongoing training programme for the directors, officers and employees of the agent, to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to:

(i) assist them in recognizing transactions and actions that may be linked to money laundering

or terrorism financing; and

(ii) instruct them in the procedures to be followed where any links have been identified under subparagraph (i).

A training program should be designed to train the appropriate personnel on a regular basis. A successful training program not only should meet the standards set out in laws (i.e. FIAMLA Act 2002) but should also satisfy internal policies and procedures in place. For the purpose of this "Guidelines", training includes not only formal training courses, but also communications that serves to educate and inform employees such as e-mails, newsletters, periodic team meetings and anything else that facilitates sharing ofinformation.

Topics to be taught in the training program vary according to target audience and services being offered but several basic matters should be factored into the program:

- Policies and Procedures in place to prevent money laundering and financing of terrorism for instance identification, record-keeping, the recognition and reporting of suspicious transactions;

- Legal Requirements under relevant AML/CFT legislations and the statutory obligations under these laws;

- Understanding ML/TF risk of the sector and of their business;

- Penalties for anti-money laundering violations;

- How to react when facing a suspicious client or transaction;

- Duties and accountabilities of employees; and

- New developments together with information on current money laundering and financing of terrorism techniques, methods and trends.

Lastly, it would be advisable for agents to keep a record of all anti-money laundering and combating

the financing of terrorism training delivered to theiremployees.

4.1.4Auditing the AML/CFT Program

Putting in place an AML/CFT Program is not sufficient; the program must be monitored and evaluated. The agent should assess their anti-money laundering and combating the financing of terrorism programs at a minimum every two years to ensure their effectiveness and to look for new risk factors. The audit program should address issues such as (i) the adequacy of its ML/TF risk assessment, (ii) the adequacy of CDD policies, procedures and processes, and whether they comply with internal requirements, (iii) the adequacy of its risk-based approach in relation to the services offered clients and geographic locations, (iv) the training adequacy, including its comprehensiveness, accuracy of materials, training schedule, (v) compliance with applicable laws, (vi) the system's ability to identify unusual activity, (vii) the adequacy of recordkeeping and (viii) the review of its Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transaction among others.

The audit can be conducted by an internal or external auditor. If the reporting entity does not have an auditor, it can conduct a self-review. The self-review should be conducted by an individual who is independent of the compliance-monitoring functions and should not be conducted by the compliance officer. This could be an employee or an outside consultant. For sole proprietorships, the review can be conducted by the sole proprietor directly.

The objective of a self-review is similar to the objectives of a review conducted by internal or external auditors. It should address whether policies and procedures are in place and are being adhered to, and whether procedures and practices comply with legislative and regulatory requirements.

The results of the audit should be documentedand presented either to the Board of Directors (if applicable) or to senior management. The recommended changes should beimplemented no later than a month following the completion of the audit.

5. Preventive Measures

5.1Customer Due Diligence: Identification and Verification Procedures

Both the FIAMLA and the FIAML Regulations make provision for CDD and KYC obligations and these apply to agents as well.

In line with section 17C of FIAMLA, agents need to **identify** and **verify** the true identity of the customer that they are conducting a transaction with. The identity of a customer must be established and verified using independent source documents, data or information. All CDD information collected must be kept up to date by the agent. Additionally, CDD information must be verified against independent and reliable sources.

In case of corporate bodies, the company's ultimate beneficial owner must be ascertained (see further below for more information on beneficial ownership) by obtaining information on their identity on the basis of documents, data or information obtained from a reliable and independent source and verifying the accuracy of the information obtained. The beneficial owner is the natural person who owns or controls the legal person or legal arrangement.

Timing of CDD

Identification and verification measures need to be carried out:

- When establishing a business relationship with a customer;
- When dealing with a one-off customer or counterparty and the transaction concerned is equal to or above 500,000 rupees whether conducted as a single transaction or several transactions that appear to be linked;
- Where there is a suspicion of money laundering or financing of terrorism; and

- Where there are doubts concerning the veracity of previous customer/counterparty identification information

5.1.1 Natural Persons (i.e. Individuals)

(a) Face to Face transactions

Regulation 4 of the FIAML Regulations requires that the agent shall obtain from and verify a customer who is a natural person the following information:

a. the full legal and any other names, including, marital name, former legal name or alias;
b. the date and place of birth;
c. the nationality;
d. the current and permanent address; and
e. such other information as may be specified by a relevant supervisory authority or regulatory body.

Identification and Verification Methods for Natural Persons

Data to be collected	Verification Methods
1. Full legal and any other names, including, marital name, former legal name or alias 2. Date of birth 3. Gender 4. Place of birth 5. Nationality 6. Occupation and Name of Employer (if self-employed, the nature of the self-employment) 7. Telephone number	▪ Current Valid National Identity Card ▪ Current Valid Passport ▪ Current valid driving licence- where the Real Estate Agent is satisfied that the driving licensing authority carries out a check on the holder's identity before issuing the licence. In each case, the document must incorporate a photographic evidence of identity. Where the legal person with which the natural person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. However, where the legal person is high risk, or where a high-risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary For self-employed, any of the sources below should be used: ■ Trade Licence ■ Business Registration Card
8. Current and Permanent residential address	Any of the identity sources listed below: ▪ a recent utility bill issued to the individual by name; ▪ a recent bank or credit card statement; or

(PO Box addresses are not acceptable)	▪ a recent reference or letter of introduction from (i) a legal professional that is regulated in Mauritius; (ii) a regulated financial services business which is operating in an equivalent jurisdiction or a jurisdiction that complies with the FATF standards; or (iii) a branch or subsidiary of a group headquartered in a well-regulated overseas country or territory which applies group standards to subsidiaries and branches worldwide, and tests the application of, and compliance with, such standards. 'Recent' means within the last three months.
9. Government issued personal identification number or other government issued unique identifier	The relevant government document such as, but not limited to, any trade licence issued or the Tax Account Number (TAN) of the Individual.

(b) Non-Face-to-Face Transactions

It is most vital that the procedures adopted to verify identity of clients for non-face-to-face transaction is at least as robust as those for face-to-face verification. Accordingly, in accepting transactions from non-face-to-face clients, agents should apply uniformly effective customer identification procedures as for those mentioned above and other specific and appropriate measures to mitigate the higher risk posed by non-face-to-face verification of clients.

In addition, for non-residents requiring services from abroad, details such as 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, authority to obtain any data provided.

Documents provided should be duly certified as a true copy by a lawyer, accountant or other professional person 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 agent believes in good faith to be acceptable to it for the purposes of certifying.

5.1.2 Legal Persons and Legal Arrangements

Legal persons refers to any entities other than natural persons that can establish a permanent customer relationship with a reporting entity including anagent or otherwise own property. In Mauritius, a legal person includes a company, a foundation, an association and a limited liability partnership.Legal arrangements, on the other hand, refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie.

Regulations 5, 6 and 7 of the FIAML Regulations 2018 lay down specific requirements where an applicant is a legal person or a legal arrangement.

(a) Legal persons(For example: Companies)

Agents must, in relation to companies, understand and document the nature of the company's business as well as the ownership and control structure. The following documents must be obtained to identify and verify the customer's identify:

i. The name, legal form and proof of existence of the company;
ii. Powers that regulate and bind the customer;
iii. The names of persons having senior management positions; and
iv. The address of the registered office or principal place of business.

Identification and Verification Methods for Legal Persons

Person to be identified	**Data to be identified**	**Method of data verification**
Underlying persons who are individuals.	As per the requirements for natural person Agents should collect identification data in relation to the following: 1.Directors 2.Beneficial Owner(s) 3.Significant Shareholders and 4.Authorised signatories. In the absence of an authorised signatory, the identity of the relevant person who is the senior managing officials. 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 client.	▪ As per the requirements for natural person ▪ Where the legal person with which the underlying person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. ▪ However, where the legal person is high risk, or where a high-risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary
1. Private companies 2. Partnerships	1. Legal status of body 2. Legal name of body 3. Any trading names	▪ Certificate of incorporation (or other appropriate certificate of registration or licensing); ▪ Memorandum and Articles of Association (or

3. Sociétés 4. Foundations 5. Other legal persons	4. Nature of business 5. Date and country of incorporation/registration 6. Official identification number (for example, company number) 7. Registered office address 8. Mailing address (if different) 9.Principal place of business / operations (if different) 10. Any other data which the real estate agent considers to be reasonably necessary for the purposes of establishing the true identity of the legal person.	equivalent); ▪ Company registry search, including confirmation that the person is not in the process of being dissolved, struck off, wound up or terminated; ▪ Latest audited financial statements or equivalent; ▪ Annual report or equivalent; ▪ Personal visit to principal place of business; ▪ Partnership deed or equivalent; ▪ Charter of Foundation; ▪ Actede société; ▪ Certificate of good standing from a relevant national body; ▪ Reputable and satisfactory third-party data, such as a business information service ▪ Any other source of information that to verify that the document submitted is genuine.

Where identification information relating to a legal person is not available from a public source, a real estate agent will be dependent on the information that is provided by the legal person. Agents should accordingly treat such information with care and in any event in accordance with the legal person's risk assessment.

(b) Legal Arrangements(For example: Trusts)

In the case of trusts, 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. Additionally, the identity of the settlor, beneficiaries or class of beneficiaries and where applicable the protector or enforcer and any other natural person exercising ultimate effective control over the trust must be established and verified.

In the case of other legal arrangements, the agent must identify and verify through reasonable means the identity of the persons in equivalent or similar positions to those described for trusts

above.

Identification and Verification Methods for Legal Arrangements

Person/ arrangement to be identified	Data to be identified	Method of data verification
Underlying persons who are individuals.	As per the requirements for natural person	▪ As per the requirements for natural person
Underlying principals who are legal persons	As per the requirements for legal persons above In circumstances where an applicant for business which is a legal arrangement acts or purports to act on behalf of a legal person, then identification and verification must take place not just in respect of that legal person, but also in respect of that legal person's underlying principals.	▪ As per the requirements for legal persons above
Legal arrangement	1. Legal status of arrangement (including date of establishment) 2. Legal name of arrangement (if applicable) 3. Trading or other given name(s) of arrangement (if applicable) 4. Nature of business 5. Any official registration or identifying number (if applicable) 6. Registered office address (if applicable) 7. Mailing address (if different) 8. Principal place of business/ operations (if different) 9. Any other data which the real estate agent considers to be reasonably necessary for the purposes of establishing the true identity of the legal arrangement.	▪ Trust deed or equivalent instrument ▪ Official certificate of registration (if applicable) ▪ Where the above proves insufficient, any other document or other source of information on which it is reasonable to place reliance in all the circumstances.

Agents must seek and obtain assurances from the trustee/s (or controlling individual/s) that all of the data requested by the Agent under the above process has been provided, and that the individual(s) will notify the Agent in the event of any subsequent changes.

Where identification information relating to a legal arrangement is not available from a public source, an Agent will be dependent on the information that is provided by the legal arrangement (usually

through its controlling individuals, such as trustees). Agents should accordingly treat such information with care and in any event in accordance with the legal arrangement risk assessment.

5.1.3 Establishing and Verifying Beneficial Ownership

Section 17E(3)of the FIAMLA defines a 'beneficial owner' as a natural person:

i. Who ultimately owns or controls a customer;
ii. On whose behalf a transaction is being conducted;
iii. Includes those natural persons who exercise ultimate control over a legal person or arrangement; and
iv. Such other persons as may be prescribed.

In line with Regulation 6 of the FIAML Regulations, Agents must identify and take reasonable measures to verify the identity of the beneficial owners. This should be done by obtaining the following information:

a) The identity of the natural persons having an ultimate controlling ownership interest in the company;

b) In the event the requirements of paragraph (a) cannot be fully satisfied, or where no natural person has control through ownership interests, the identity of the natural person who exercises control through other means; and

c) Where no natural person has been identified in (a) or (b), the identity of the natural person holding a senior management position.

When gathering the above data, agents must document the process as well as any difficulties encountered during. Further enquiries may be made for verification such as 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, 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.

5.1.4 Individuals acting on Behalf of Applicants for Business and Customers

There might be cases where customers (particularly those which are legal persons) will have one or more individuals authorised to act on their behalf in dealing with agents.

Agents must have in place appropriate policies, procedures and controls to ensure that they are able to identify and verify the identity of all persons purporting to act on behalf of customers, and to confirm the authority of such persons to act. Agents must, in the case of individuals acting on behalf of customers, obtain identification data and verify that data, in line with guidelines provided above.

Where the agent is unable to determine whether the customer is acting for a third party or not, it shall make a suspicious activity report pursuant to section 14 of the FIAMLA to the Financial Intelligence Unit.

5.1.5 Third Party Reliance

In order to rely on another regulated/supervised/monitored person to perform CDD measures in accordance with section 17D of the FIAMLA, agents must also ensure that the requirements of Regulation 21 of the FIAML Regulations are fulfilled and that –

i. the necessary information required is obtained immediately;
ii. he is satisfied that copies of identification data and other relevant documentation related to CDD requirements shall be made available from the third party upon request without delay;
iii. he is satisfied that the party is regulated and supervised or monitored for the purposes of combating money laundering and terrorism financing and has measures in place for compliance with CDD and record keeping requirements in line with the FIAMLA and FIAML Regulations; and
iv. he shall not rely on a third party based in a high-risk country.

5.1.6 Inability to Establish Customer Identity

Where the agent cannot obtain all the information required to establish the identity of the customer to its full satisfaction, he shall not commence the business relation or perform the transaction and shall file a suspicious transaction report with the FIU.

Moreover, if during the course of its business activities, the agent has doubts about the veracity or adequacy of previously obtained client identification data, he must identify and verify the identity of the customer and beneficial owner before conducting any further

5.2 Record Keeping

All agents are required to keep records of all the transactions in which they are involved and of all customers. The following records must be kept:

a) Records relating to the identification of customers and beneficial owners (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as business correspondence for at least 7years after the business relationship has ended.

b) Records concerning transactions, both domestic and international shall be kept for a period of 7 years after the completion of the transaction; and

c) Copies of all STRs filed with the FIU shall also be kept for a period of at least 7 years from the date the report was made.

5.3 Enhanced Due Diligence (EDD)

Regulation 12 of the FIAML Regulations 2018 provides that agents shall implement internal controls and other procedures to combat money laundering and financing of terrorism, including EDD procedures with respect to high-risk persons, business relations and transactions and persons established in jurisdictions that do not have adequate systems in place to combat money laundering and financing of terrorism.

Where the ML/TF risks are identified to be higher, agents shall take EDD measures to mitigate and manage those risks.

The EDD measures that may apply for higher risk relationships should include:

(a) requesting additional information on the customer and updating on a frequent basis the customer or the beneficial owner;

(b) obtaining additional information on the intended nature of the business relationship and the source of fund/wealth;

(c) obtaining information on the intended or performed transactions;

(d) obtaining the approval of senior management to commence or continue the business relationship;

(e) conducting close monitoring of the business relationship; and

(f) any other measures the agent may undertake with relation to a high-risk relationship.

Where anagent is unable to perform the required Enhanced CDD requirements, the latter shall terminate the business relationship and file a suspicious transaction report under section 14 of the FIAMLA. See below for EDD measures to applicable to Politically exposed Persons (PEPs).

5.4 Simplified Due Diligence

In general, the full range of CDD measures should be applied by agents. However, simplified CDD measures can be implemented in cases where lower risks have been identified. The simplified CDD measures have to be commensurate with the lower risk factors and in accordance with any guidelines issued by a regulatory body or supervisory authority.

Where anagent determines that there is a low level of risk, he shall ensure that the low risk identified is consistent with the findings of the national risk assessment or any risk assessment of his supervisory authority or regulatory body, whichever is most recently issued. Importantly, simplified CDD shall not apply where, anagent knows, suspects, or has reasonable grounds for knowing or suspecting that a customer is engaged in money laundering or terrorism financing or that the transaction being conducted by the customer is being carried out on behalf of another person engaged in money laundering or terrorist financing. The possibility of applying simplified CDD is not an exemption. It only allows for the application of reduced measures. The ultimate decision rests with the agent and there may be instances, depending on the level of risk and all the known circumstances (a high-risk relationship e.g. PEP will be dealt with more caution rather than the routine CDD measures), where it is inappropriate to adopt these simplified measures. Under all circumstances, agents must keep the client risk assessment up to date and review the appropriateness of CDD obtained even if simplified CDD measures are adopted. Agents are required

to keep the risk assessment and level of CDD requirements under review and the level of risk of the CDD measures should be consistent with the risk of the relationship.Where simplified CDD measures are adopted, agents should apply a risk-based approach to determine whether to adopt the simplified CDD measures in a given situation and/or continue with the simplified measures, although these customers' accounts are still subject to transaction monitoring obligations.

5.5 Politically Exposed Persons (PEPs)

PEPs are individuals who are or who have been entrusted with prominent public functions foreign, domestic and international organisation PEP, as well as the close relatives and associates of such persons.Pursuant to the FIAML Regulations 2018, PEPs have been classified as "domestic PEPs," "foreign peps" and "international organization PEPs" in the FIAML Regulations.

5.5.1 Types of PEPs

(a) Domestic PEPs

A domestic PEP means a natural person who is or has been entrusted domestically with prominent public functions in Mauritius and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

Examples on who may be a PEP

- Heads of state
- Heads of government
- Ministers and deputy or assistant ministers
- Members of parliament or similar legislative bodies
- Members of governing bodies of political parties
- Members of supreme courts, or any judicial body whose decisions are not subject to furtherappeal, except in exceptional circumstances
- Members of courts of auditors or of the boards of central banks
- Ambassadors, charges d' affaires and high-ranking officers in the armed forces
- Members of the administrative, management or supervisory bodies of state-ownedenterprises

- Directors, deputy directors and members of the board of equivalent function of an international organization

(b) Foreign PEPs

Foreign PEPs have the same definition as above insofar as they are entrusted with prominent public function by a foreign country.

(c) International Organization PEPs

An “international organization PEP” means a person who is or has been entrusted with a prominent function by an international organization and included members of senior management or individuals who have been entrusted with equivalent functions including directors, deputy directors and members of the board or equivalent functions and such other person or category of person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

(d) Close Associates and Family members

As provided by regulation 15(5) FIAML Regulations, in addition to the primary PEPs listed above, a PEP also includesclose associates and family members.

i. Close associates mean-
   - an individual who is closely connected to a PEP, either socially or professionally; and
   - any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

ii. Family members mean-
   - an individual who is related to a PEP either directly through consanguinity, or through marriage or similar forms of partnership; and
   - any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

5.5.2 PEPs and Due Diligence Measures

Business relationships with PEPs pose a greater than normal money laundering risk to agents, by virtue of the possibility for them to have benefitted from proceeds of corruption, as well as the potential for them (due to their offices and connections) to conceal the proceeds of corruption or other crimes.

As such, agents are required to have a clear policy in relation to transactions involving such persons. Agents must therefore establish appropriate risk management systems to determine whether the customer or beneficial owner is a PEP. Regulation 12 of the FIAML Regulations prescribe that when dealing with domestic or international organization PEPs, the following EDD measures must be applied in addition to the normal CDD measures applicable under the Regulations:

(a) reasonable measures must be taken to determine whether a customer or the beneficial owner is a PEP; and

(b) in cases when there is higher risk business relationship with a domestic PEP or an international organization PEP, adopt the measures listed below:

- obtain senior management approval before establishing or continuing, for existing customers, such business relationships;
- take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
- conduct enhanced ongoing monitoring on that relationship

Additionally, agents shall apply all the above measures to family members or close associates of all types of PEP.

5.6 Reporting Suspicious Transactions

Section 14 of FIAMLA imposes an obligation on agents to make a report, **as soon as possible but not later than 15 working days**to the FIU of any transaction which they have reason to believe may be suspicious. The form, as approved by the FIU and in accordance with section 15 of the FIAMLA, to be used for reporting suspicious transaction is the Suspicious Transaction Report (STR) Form. A copy of the form is available on the website of the FIU on the link below:
http://www.fiumauritius.org/images/stories/STR_FORM_FINAL_VERSION.pdf

Information on the manner in which a STR shall be reported is contained in the FIU's **Guidance Note No. 3** which is also available on the FIU's website.

5.6.1 Suspicious Transaction

'*Suspicious transaction'* is defined under FIAMLA as *a transaction which (a) gives rise to a reasonable suspicion that it may involve (i) the laundering of money or the proceeds of any crime; or (ii) funds linked or related to, or to be used for, terrorist financing, proliferation financing or by proscribed organizations, whether or not the funds represent the proceeds of a crime; (b) is made in circumstances of unusual or unjustified complexity; (c) appears to have no economic justification or lawful objective; (d) is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; (e) gives rise to suspicion for any otherreason.*

A 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 or an attempted transaction.

For further details on how to identify and report a suspicious transaction, please refer to the FIU current Guidance Note No 3, mentioned above. The offence for failing to report an STR is set out under section 19 of the FIAMLA. The penalty is a fine not exceeding one million rupees and imprisonment for a term not exceeding 5 years.

Ongoing Monitoring

The ability to file an STR of good quality is heavily reliant on the robustness of the systems put in place by the agent. In fact, agents are required to scrutinize transactions undertaken throughout the course of a business relationship, including where necessary the source of funds to ensure that the transactions are consistent with his knowledge of the customer. As part of the monitoring of transactions, agents must examine the background and purpose of each transaction especially where these are complex, unusually large or conducted in unusual patterns. Equally, they must pay attention to transactions that do not seem to have an apparent economic or lawful purpose.

5.6.2 Request for Information by the FIU

Under section 13(2) (a) and 13(2)(b) of FIAMLA, the Director of the FIU may request additional information from agents who submitted the suspicious transaction report or from any other reporting person which is, or appears to be, involved in the transaction. Also, pursuant to section 13(3) of the FIAMLA, the Director of the FIU can request information from agents, whenever the FIU becomes aware of information that may give rise to reasonable suspicion of ML/TF offences, or it has received a request from investigatory /supervisory /overseas FIU/government agencies. The information sought for under the above sections shall, as soon as practicable but not later than 15 days, be furnished to the FIU.

Also, in line with section 13(6) of the FIAMLA, the FIU may order agents to inform it if a person has been their client, or has acted on behalf of their client; or whether a client of the agent has acted for a person.

If agents fail to supply any information requested by the FIU under section 13(2), 13(3) or 13(6) of FIAMLA, they commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years as provided for in section 19 and 32A of the FIAMLA.

5.6.3 Protection of Information

Confidentiality is a key success factor for the operations of an FIU. In this context, the FIU has put in place a proper Program Level Security and a System Level Security policies and procedures. Under the Program Level Security (based on protection afforded under the law), and in line with section 30(1) of the FIAMLA, the Director, every officer of the FIU, the Chairperson and members of the Board shall take an oath of confidentiality before they begin to perform their duties. They should maintain during and after their relationship with the FIU, the confidentiality of any matter relating to the relevant enactments. Section 30(2) of the FIAMLA further provides that no information from which an individual or body can be identified and which is acquired by the FIU in the course of carrying out its functions shall be disclosed except where disclosure appears to the FIU to be necessary to enable it to carry out its functions, or in the interests of the prevention or detection of crime, or in connection with the discharge of any international obligation to which Mauritius is subject. More so, in view of preserving the confidentiality of information disseminated, at the time of disclosure of intelligence to recipients, the FIU imposes terms and conditions on the usage of such

intelligence in line with section 30(2A) of FIAMLA. Any breach of this section shall be punishable by a fine not exceeding Rs1 million and to imprisonment for a term not exceeding 3 years.Additionally, under the Program Level Security, the FIU has adopted clear policies on recruitment and termination of employment of staff.

5.6.4 Tipping Off

After making a suspicious transaction report to the FIU, section 16 (1) of FIAMLA prevents agents from informing anyone, including the customer, about the contents of a suspicious transaction report or even discloses to him that he/she has made such a report or information has been supplied to the FIU pursuant to the request made under section 13(2), 13(3) or 13 (6) of FIAMLA. It shall amount to an offence under the Act punishable by a fine not exceeding five million rupees and to imprisonment for a term not exceeding 10 year.

Reasonable enquiries of a customer, conducted in a discreet manner, regarding the background to a transaction or activity which has given rise to the suspicion is prudent practice, forms an integral part of CDD and on-going monitoring, and should not give rise to tipping off. If the employee suspects that CDD will tip off the client, the employee should stop conducting CDD and instead the agent should immediately file an STR with the FIU.

5.6.5Registration with the FIU

Also, in line with section 14C of the FIAMLA, the agent must register with the FIU, within such time, form and manner as may be prescribed. The Financial Intelligence and Anti Money Laundering (Registration of Reporting Persons) Regulations 2019 were made on 5th November 2019 to this effect. All agents who fall within the purview of the FIAMLA must register with the FIU in accordance with the time frames which shall be specified by the FIU.

5.7 Cash Prohibition

Moreover, agents shall not make or accept any payment in cash in excess of 500,000 rupees or an equivalent amount in foreign currency pursuant to section 5 of FIAMLA. Under FIAMLA, "cash" means money in notes or coins of Mauritius or in any other currency; and it includes any cheque which is neither crossed nor made payable to order whether in Mauritian currency or in any other currency.

6. Terrorist Financing Offences

6.1 Introduction

Terrorist organizations require funds to plan and carry out attacks, train militants, pay their operatives and promote their ideologies. The Convention for the Suppression of the Financing of Terrorism Act and the Prevention of Terrorism Act criminalize the financing of the terrorism in Mauritius. Additionally, the UN Sanctions Act provides the legal framework for implementing targeted financial sanctions imposed by the United Nations Security Council.

6.2 Extension of Obligations

According to section 19H & K of the FIAMLA, anagentfalling under the purview of a regulatory body must ensure compliance with the UN Sanctions Act. Agents should be aware that once a person has been designated domestically or listed by the UN, it is an offence to deal with the funds or other assets of such a person. It is also an offence to make funds or other assets available to a designated party or listed party. As soon as there is a designation or a listing, two prohibitions prevail under the UN Sanctions Act:

- A prohibition to deal with the funds or other assets of the designated or listed party under section 23; and
- A prohibition to make available funds or other assets to the designated or listed party under

section 24.

The prohibitions to apply to all persons (including all agents).

Under the UN Sanctions Act, there are also several reporting obligations which apply to agents. These are set out below.

6.3 Reporting obligations

Where any person holds, controls or has in his custody or possession any funds or other assets of a designated party or listed party, he/she shall immediately notify (section 23(4) UN Sanctions Act) the National Sanctions Secretariat of-

i. details of the funds or other assets against which action was taken against;
ii. the name and address of the designated party or listed party; and
iii. details of any attempted transaction involving the funds or other assets, including-
    - the name and address of the sender
    - the name and address of the intended recipient
    - the purpose of the attempted transaction
    - the origin of the funds or other assets
    - where the funds or other assets were intended to be sent.

The reporting obligations continue under section 25 of the UN Sanctions Act which says that a reporting person shall immediately verify whether the details of the designated or listed party match with the particulars of any customer and if so, identify whether the customer owns any funds or other assets in Mauritius. A report has to be submitted to the National Sanctions Secretariat regardless of whether any funds or other assets were identified by the reporting person.

Contact details for the National Sanctions Secretariat:

National Sanctions Secretariat

Prime Minister's Office (Home Affairs)
Fourth floor
New Government Centre
Port Louis

Phone Number: (+230) 201 1264 / 201 1366
Fax: (+230) 211 9272

Email: nssec@govmu.org

6.4 Reporting of Suspicious Information

Pursuant to section 39 of the UN Sanctions Act, any information related to a designated party or listed party which is known to the agent should be submitted to the FIU in accordance with section 14 of the FIAMLA. For more information on how to file an STR please refer to Section 5.6 of this guideline.

6.5 Internal controls

Section 41 of the UN Sanctions Act states that a reporting person shall implement internal controls and other procedures to enable it to effectively comply with their obligations under this Act. As such, when anagent designs his AML/CFT program, detailed in the previous section, he must also ensure that he incorporates policies and procedures to ensure that he is not engaging in any transactions with designated or listed parties. Each of the building blocks of his AML/CFT program must also take into account the obligations under the UN Sanctions Act and the agent must have systems which will allow him to screen customers against the lists of designated or listed parties maintained by the NSS on its website. Additionally, any agent already registered with the FIU will also receive any changes to these lists as soon as these are made.

7. ML/TFIndicators for Real Estate Agents

There are a number of situations which may give rise to a suspicion that a transaction may involve money laundering. The list of situations given below is meant to assist real estate agents to detect/identify suspicious or unusual transactions in the conduct of their operations and business activities. It is not a prescriptive list of all possible transactions linked to money laundering or terrorism financing. Nor does it imply that the transactions listed below are necessarily linked to such activities. The role of the real estateagent is to be familiar with these indicators, and exercise sound judgment based on their knowledge of the real estate industry, and where they identify any “suspicious or unusual transactions”, know the proper action to take.

7.1 General Indicators

- Client brings a significant amount of cashtothereal estate agent for transactions.
- Client purchases property in the name of a nominee such as an associate or a relative (other than a spouse), or on behalf of minors or incapacitated persons or other persons who lack the economic capacity to carry out suchpurchases.
- Client does not want to put his or her name on any document that would connect him or her with the property or uses different names on relevantdocuments.
- Client attempts to hide the identity of the true customer or requests that the transaction be structured to hide the identity of the truecustomer.
- Buyer is an agent or owner of a shell company who refuses to disclose the identity of the company.
- Address given by client is unknown or is believed to befalse.
- Client inadequately explains the last minute substitution of the purchasing party’s name.
- Client pays substantial down payment in cash and balance is financed by an unusual source or ‘offshore’ bank.

- Client purchases property without inspecting it.

- Client purchases multiple properties in a short period of time, and seems to have few concerns about the location, condition and anticipated repair costs, etc., of each property.

- Client is a recently created legal entity and the amount of the transaction is large compared to their assets.

- Transaction does not match the business activity known to be carried out by the client company.

- Transaction is made in circumstances of unusual or unjustified complexity and without any economic justification or lawful objective

- Transaction is entered into at a value significantly different (much higher or much lower) from the real or market value of the property.

- Property is sold in a series of successive transactions each time at a higher price between the same parties.

- Buyer takes on a debt significantly higher than the value of the property.

Annex 1. Risk Assessment Form for Real Estate Agents

Name of Real Estate Agent: _____

The *Financial Intelligence Anti-Money Laundering Act* requires agents to conduct a risk assessment of their exposure to money laundering and terrorism financing and apply corresponding mitigation and controls. This checklist is meant to assist agents in meeting these obligations. This form is presented as an example only. Agents may choose to conduct their risk assessment using a different approach.

Instructions: When you answer yes to one of the questions, this situation or client is considered higher risk and a control measures to reduce the risk should be applied. For each higher risk client or situation a suggested control measure is proposed. You can adapt the control measures to correspond to your business (see Annex 1.A for a list of control measures).

The results of this risk assessment should be communicated to all real estate agents and employees in your business that deal with clients. The training should include a review of what is considered higher risk and the corresponding control measures. The date of the training should be documented. You should review your risk assessment every two years.

Risk Assessment

Higher risk clients and situations	Yes Higher risk	No Moderate risk	Suggested Control Measures
■ **Clients**			
Are your clients foreigners?			■ Determine if individuals are politically exposed persons.[9] ■ Obtain additional information on source of funds or source of wealth.
Do you have clients who are politically exposed persons?			■ Obtain senior management approval to conduct the transaction. ■ Obtain additional information on source of funds or source of wealth. ■ Conduct enhanced on-going monitoring any future real estate transactions.
Is your client a company, trust, foundation, partnership or other structure that makes it difficult to determine who is the beneficial owner (the natural person who owns or controls the funds or property)?			■ Obtain name of natural person(s) behind company, trust or other legal arrangements.[10] ■ Obtain additional information on organizational structure. ■ Obtain additional information on source of funds or source of wealth.
Are your clients intermediaries (i.e. lawyers and accountants acting on behalf of clients)?			■ Obtain name of person(s) on whose behalf the transaction is being conducted. ■ Verify that the intermediary has the necessary documentation to act on behalf of the client. ■ Obtain additional information on source of funds or source of wealth.
Has one of your clients been named in the media as being involved with criminal organizations or having committed a crime?			■ File Suspicious Transaction Report (STR). ■ Obtain additional information on source of funds or source of wealth.
Do you have a client that is purchasing a property that is not within his or her means based on his stated occupation or income?			■ Obtain additional information on source of funds or source of wealth.
Do your clients that engage in activities that are consistent with the indicators identified for Suspicious Transactions? (See Guidance Note on AML/CFT Guidance on Suspicious Transaction Reports for			■ Consider filing a Suspicious Transaction Report (STR). ■ Obtain additional information on source of funds or source of wealth.

[9]Pursuant to FIAMLA, you are required to ascertain whether all clients and beneficial owners are politically exposed persons. The mitigation measure is suggested here for emphasis.

[10]For further information on how to comply with your beneficial ownership obligations please consult the Guideline on the Prevention of Money Laundering and Countering the Financing of Terrorism in the Real Estate Sector.

suspicious transactions indicators). Link to the Guidance note: http://www.fiumauritius.org/English/Reporting/Documents/Guidance%20Note_310817.pdf			
■ **Geographic Risk**			
Are any of your clients or the source funds originate from countries subject to sanctions, embargoes or similar measures issued by Mauritius or International Organizations such as the United Nations ("UN"). Mauritius http://www.fiumauritius.org/English/United%20Nations%20Security%20Council/Pages/default.aspx United Nations: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list			■ Obtain senior management approval to proceed with the transaction. ■ Ask for additional information, piece of identification to confirm the identity. ■ Obtain additional information on source of funds or source of wealth.
Do any of your clients or the source funds originate from foreign jurisdictions known for high levels of financial secrecy or jurisdictions with low tax rates? http://www.imolin.org/imolin/finhaeng.html#Map.%20%20Major%20Financial%20Havens https://www.financialsecrecyindex.com/en/			■ Obtain senior management approval to proceed with the transaction. ■ Ask for an additional piece of identification to confirm the identity. ■ Obtain additional information on source of funds or source of wealth.
Do any of your clients or the source funds originate from foreign jurisdictions identified by the Financial Action Task Force (FATF) as having strategic deficiencies in the fight against money laundering or subject to an FATF statement? FATF: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)			■ Obtain senior management approval to proceed with the transaction. ■ Ask for an additional piece of identification to confirm the identity. ■ Obtain additional information on source of funds or source of wealth.

Do any of your clients or the source funds originate from jurisdictions identified by credible sources (for example international organizations such as the UN, credible news reports) as providing funding or support for terrorist activities?			■ Obtain senior management approval to proceed with the transaction. ■ Ask for an additional piece of identification to confirm the identity. ■ Obtain additional information on source of funds or source of wealth.
Do any of your clients or the source funds originate from countries identified by credible sources as having significant levels of corruption, or other criminal activity? http://www.transparency.org/news/feature/corruption_perceptions_index_2016			■ Obtain senior management approval to proceed with the transaction. ■ Ask for an additional piece of identification to confirm the identity. ■ Obtain additional information on source of funds or source of wealth.
■ **Delivery Channel and Business Practices**			
Do you accept cash?			■ Confirm source of funds ■ Set limits to cash transaction amounts recognizing the 500,000 rupee cash prohibition outlined in the FIAMLA. ■ Request bank drafts instead of accepting large amounts of cash.
Do you conduct transactions where you do not meet the client?			■ Deliver comprehensive AML/CFT training to your employees specifically focused on client due diligence requirements ■ Ask for an additional piece of identification to confirm the identity. ■ Confirm the beneficial owner (the natural person who owns or controls the funds or property) ■ Confirm that any intermediary has the necessary documentation to act on behalf of the client. ■ Conduct periodic review of records to ensure that client due diligence requirements are adequately implemented
Do you have clients that are referred to you by a third party (such as a lawyer, accountant or other real estate agent)?			■ Conduct client due diligence measures directly. ■ Conduct periodic review of records to ensure that client due diligence requirements are respected by third party if you rely on them for due diligence measures.
Do you have short-term or part-time agents?			■ Include AML/CFT obligations in job descriptions and performance reviews. ■ Deliver comprehensive AML/CFT training for all employees

Do you undertake high value transactions (over5 million rupees[11])?			■ Pay special attention for unusual transaction and ML/TF indicators. ■ Obtain additional information on source of funds or source of wealth.
Other risk factors: (list any additional factors)			

_____ _____

Signature of the real estate agent ***Date***

Date of employee training:_____

[11]Transaction for the purpose of this section means the total value (inclusive of all taxes) of the project/sale/purchase of any property that may concern the buying and selling of a real estate in Mauritius.

Annex 1.A - Examples of Risk Control Measures

1. Obtain senior management or compliance officer approval to proceed with the transaction.
2. Ask for an additional piece of identification to confirm the identity.
3. Obtain name of natural person(s) behind company, trust or other legal arrangement.
4. Monitor if client conducts additional real estate transactions.
5. Obtain information on source of funds or source of wealth of the client.
6. Deliver more frequent employee training.
7. Monitor AML/CFT legislative and regulatory changes.
8. Include AML/CFT obligations in job descriptions and performance reviews.
9. Set limits to cash transaction amounts (less than the 500,000 rupees prohibition).
10. Request bank drafts instead of accepting large amounts of cash.
11. Conduct transaction only in person.
12. Obtain appropriate additional information to understand the client's business or circumstances.
13. Conduct transaction only in person.
14. Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the client risk profile (provided that the internal policies of accountants should enable them to disregard source documents, data or information, which is perceived to be unreliable).
15. Obtaining additional information and, as appropriate, substantiating documentation, on the intended nature of the business relationship.
16. Obtaining information on the source of funds and/or source of wealth of the client and clearly evidencing this through appropriate documentation obtained.
17. Obtaining information on the reasons for intended or performed transactions.
18. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

19. Requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards.

Annex 2: Template for AML/CFT Policies and Procedures

Address | City Postal Code| Telephone

Email

NAME OF ENTITY

Risk Assessment and Risk mitigation (Section 17 of the Financial intelligence Anti-Money Laundering Act (FIAMLA))

Describe how you will comply with your risk assessment and risk mitigation obligations including:

- Identifying what clients and situations you have identified as higher risk (copy of the risk assessment should be attached)
- What mitigation and control measures you will be implementing to reduce the risk
- How you will document the risk of any new product or services
- How often you will update the risk assessment

See How to conduct a risk assessment in real estate sector for additional guidance (Please refer to Annex 1).

Customer due diligence (CDD): (section 17C of the FIAMLA)

Describe how you will comply with CDD requirements including:

- When will you identify the buyer and seller of a real estate transaction?
- What information will you collect when you identify a natural person?
- What information will you collect when you identify a legal persons and legal arrangements?
- What identification documents are acceptable?
- Only original documents will be acceptable
- How will you identify clients that are not physically present?
- What will you do if you cannot complete customer due diligence measures?

Record Keeping (Section 17F of FIAMLA)

Describe how you will comply with record keeping requirements including:

- How long will you retain records related to real estate transactions?
- What records will you retain?
- Where will records be retained?
- How will you ensure that information can be provided in a timely manner to the Financial Intelligence Unit, the police and other competent authorities?
- If you are using a third party to conduct customer due diligence measures:
    - How you will ensure that they are properly identifying clients?
    - How you will gain access to information in a timely fashion?

Enhanced due diligence (Regulation 12 of the Financial Intelligence Anti-Money Laundering Regulations (FIAMLR))

Describe how you will comply with enhanced due diligence requirements including:

- How you will apply enhanced due diligence measures to:
    - Persons or transactions involving a country identified as higher risk by FATF
    - Persons or transactions involving higher risk countries for ML, TF, corruption or subject to international ML/TF
    - Any other situation representing a higher risk of ML/TF based on your risk assessment
- What enhanced due diligence measures will be applied in those circumstances?

Politically Exposed Persons (Regulation 15 of the FIAMLR)

Describe how you will comply with enhanced due diligence requirements related to politically exposed persons including:

- What is a politically exposed person?
- How you will identify politically exposed persons?
- How you will seek approval from senior management?
- How you will take adequate measures to establish source of wealth and source of funds?
- How you will conduct enhanced ongoing monitoring?

Ongoing monitoring (Section 3(e) of the FIAMLR)

Describe how you will comply with ongoing monitoring requirements including:

- How you will conduct ongoing monitoring for:
  - Business relationships (typically after 2 transactions)
  - Complex and unusual transactions
  - Unusual patterns of transactions which have no economic or lawful purpose?
- How you will record the findings?

Suspicious transaction reporting (Section 15 of the FIAMLA)

Describe how you will comply with suspicious transaction reporting requirements including:

- What is a suspicious transaction?
- How you and your employees/agents will identify suspicious transactions (should refer to ML/TF indicators)
- Who is your Money Laundering Reporting Officer?
- How employees/agents should raise suspicions to the reporting officer?
- Specify that you cannot communicate that an STR has been filed with the FIU

Training (Regulation 22 (1) (c) of the FIAMLR)

Describe how you will comply with training requirements including:

- How you will screen employees to ensure high standards before hiring
- How you will train employees/agents on:
  - How to identify a suspicious transaction?
  - What are the AML/CTF obligations?
  - How to implement your policies and procedures?

Terrorist Financing Obligations (Regulation 22 (1) (c) of the FIAMLR)

- Describe how you will comply with training requirements including:
  - How you will screen against UN Sanctions List?
  - How you will report to the National Sanctions Secretariat?
  - How you will report to the FIU?

Policies and procedures (Section 22 (1) (c) of the FIAMLR)

Describe the following regarding your policies and procedures:

- How you will communicate the policies and procedures to employees and staff as well as branches and subsidiaries
- How you will reflect changes to AML/CTF legislative and regulatory requirements
- How often you will update your policies and procedures

CONTACT DETAILS

Financial Intelligence Unit
Compliance Division

10th Floor SICOM Tower
Ebene Cybercity
Republic of Mauritius
Telephone: (230) 454 1423
Fax: (230) 466 2431
Email:compliance@fiumauritius.org