OCTOBER 2025

Mercato Brokers

Anti-Money Laundering and Countering the Financing of Terrorism and Proliferation Policy (AML/CFT Policy)

INTRODUCTION

The purpose of this manual is to provide guidance on the Procedures surrounding Anti-Money Laundering, Financing of Terrorism and Proliferation of weapons of mass destruction as applicable for Mercato Brokers (hereinafter referred to as 'the Company').

Mauritius is a founder member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) which is an associate member of the Financial Action Task Force (FATF). In December 1997, Mauritius committed itself to the 40 Recommendations of the FATF and to the Mutual Evaluation procedure. Mauritius has also ratified and acceded to numerous international conventions, protocols and treaties to express its commitment towards the international community to combat money laundering and terrorism financing.

Following the drive to consolidate Mauritius as an international financial centre of high repute and the commitment to international initiatives to combat money laundering and terrorist financing, several pieces of legislations have been enacted since the year 2000 to combat money laundering and terrorism financing. These include namely the Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA) and the then Prevention of Corruption Act 2002 (POCA).

In 2023, the Financial Crimes Commission Act was enacted, to further combat financial crimes in Mauritius, with the establishment of the Financial Crimes Commission which will be the apex agency in Mauritius to detect, investigate and prosecute financial crimes such as corruption offences, money laundering offences, fraud offences, the financing of drug dealing offences and any other ancillary offence connected thereto. A number of legislations including the POCA and Part II of the FIAMLA has been repealed and replaced with the coming of this new Act.

The legal framework was further enhanced in 2018 with a view to aligning it with the 2012 FATF Standards, amongst others. The relevant legislative enhancements were aimed at strengthening the AML/CFT framework and has also extended the scope of the FIAMLA to include the financing of proliferation and the vesting of AML/CFT designated Supervisors with

the powers to supervise and enforce compliance by members of relevant professions or occupations falling under their purview with AML/CFT requirements imposed under the relevant guidelines, code, FIALMLA and other laws.

Mauritius has also adopted a National Strategy for Combating Money Laundering and the Financing of Terrorism and Proliferation 2019-2022 which sets out the approach which Mauritius will adopt to tackle money laundering (ML), terrorist financing (TF) and proliferation financing (PF) threats over the next three years. In addition, it describes the priorities and objectives in addressing financial crime and assists Mauritius in meeting international obligations set by the FATF. The Strategy is based on the findings of the National Risk Assessment (NRA) and the gaps identified in the AML/CFT Mutual Evaluation Report (MER) of Mauritius, which was published in September 2018.

The Financial Services Commission (FSC) has its AML/CFT Handbook which consolidates the FSC guidance on anti-money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction.

This manual has been drafted based on the licencing requirements of the Company, and in line with the provisions of the FIAMLA, the Financial Intelligence and Anti-Money Laundering Regulations 2018 ("FIAMLA Regulations"), the FSC AML/CFT Handbook and the relevant legislations issued by FSC. The Company will be deemed a "financial institution" under the FIAMLA and a "reporting person" under the Financial intelligence and Anti-Money Laundering Regulations 2018 ('FIAML Regulations 2018').

The objective of this Manual is to provide guidance and create awareness on practical issues to manage the risks of being exposed to Money Laundering and the financing of terrorism and proliferation. The Manual is also designed to provide guidelines for the Company and its employees to avoid any contravention to the relevant laws, rules, regulations and standards while providing services, especially in relation to money laundering and terrorist financing.

This manual has been designed to help management, senior and junior level members of staff

with a guidance to follow a risk-based approach for more effectiveness, risk-based approach and outcome focussed approach as regards to AML/CFT.

The Company is advised that guidance in this Manual should be applied in a risk-based proportionate way. This includes taking into account the size, nature and complexity of a financial institution when deciding whether a certain example of good or poor practice is relevant to its business.

The Board of the Company has duly approved the content of this Manual and the following core principles:

- Application of customer due diligence measures prior to establishing any business relationship with clients,
- Appointment of Money Laundering Reporting Officer, Compliance Officer and document internal system of suspicious transaction reporting,
- Implementation of effective on-going Customer Due Diligence measures, ongoing monitoring of transactions, activity, and risk profiling procedures,
- Provision of AML/CFT training to new staffs and on-going training to existing staffs,
- Implementation and maintenance of effective record keeping systems, and
- Reducing potentially damaging risks including reputational risk, legal risk and regulatory sanctions.

CHAPTER 1

An overview of Compliance

1.1. Introduction

The manual aims at assisting the Company, administrators and trustee in the prevention and detection of money laundering and the financing of financing of terrorism and proliferation with the implementation of strict procedures and effective systems and controls including sound Client Due Diligence (CDD) measures based on international standards.

1.2. Legislative Framework

Mauritius has taken several steps in the past years in strengthening the country's legislation against money laundering and terrorist financing.

Mauritius brought a number of amendments to its AML/CFT framework through the Finance (Miscellaneous Provisions) Act 2018, Act 11 of 2018. The relevant amendments introduced by the Finance (Miscellaneous Provisions) Act 2018 are in force and aim at strengthening the national AML/CFT framework by, inter alia:

- enhancing the existing legal framework for preventive measures that apply to financial institutions and Designated Non-Financial Businesses and Professions ('DNFBPs');
- extending the scope of the FIAMLA to include proliferation financing;
- establishing a legal framework to support the National Risk Assessment exercise; and
- providing a general penalty for contravention of those provisions of the FIAMLA for which no specific penalty was set out.

In addition, a new set of regulations, namely, the FIAML Regulations 2018 became effective on 01 October 2018, revoking the previous FIAML Regulations 2003. The FIAML Regulations namely amongst others addressed FATF requirements relating to Customer Due Diligence and Politically exposed persons.

On 21 May 2019, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 ('UN Sanctions Act') was enacted, and it came into operation on the 29 May 2019. The UN Sanctions Act enables the Government of Mauritius to implement targeted sanctions, including financial sanctions, arms embargo and travel ban, and other measures imposed by the United Nations Security Council under Chapter VII of the Charter of the United Nations, with a view to addressing threats to international peace and security, including terrorism, the financing of terrorism and proliferation of weapons of mass destruction.

1.3. Failure to comply with FIAMLA and the FIAML Regulations 2018

Both Section 32A of the FIAMLA and Regulation 33 of the FIAML Regulations 2018 set out the offences for contravening the requirements of the FIAMLA and FIAML Regulations 2018 respectively. Also, failure to comply with the FIAMLA and the FIAML Regulations 2018 may result in regulatory actions from the FSC, and depending on the severity of the breach, may result in revocation of a licence of a business. Actions under the Administrative Penalties Regulatory Framework (approved by the Board of the FSC on 24 July 2019 and issued on 19 August 2019) may also apply as appropriate

The FSC has in its AML/CFT Handbook highlighted that failure to comply with the minimum requirements of the FIAMLA and the FIAML Regulations 2018 may be regarded by the FSC as an indication of:

a) conduct that is not in the best economic interests, or which damages the reputation of Mauritius; and/or

b) lack of fitness and propriety.

The FSC has also highlighted that it shall take its AML/CFT Handbook into account when assessing the level of compliance with the FIAMLA and the FIAML Regulations 2018 at the time of conducting its onsite visits.

1.4. Compliance culture

The Board and senior management of the Company have a responsibility to ensure that the Company's systems and controls are appropriately designed and implemented, and are effectively operated to reduce the risk of the business being used in connection with ML/TF.

The board or senior management of the Company is therefore required to establish documented systems and controls which:

- undertake risk assessments of its business and its customers;
- determine the true identity of customers and any beneficial owners and controllers;
- determine the nature of the business that the customer expects to conduct and the commercial rationale for the business relationship;
- require identification information to be accurate and relevant;
- require business relationships and transactions to be effectively monitored on an ongoing basis with particular attention to transactions which are complex, both large and unusual, or an unusual pattern of transactions which have no apparent economic or lawful purpose;
- compare expected activity of a customer against actual activity;
- apply increased vigilance to transactions and relationships posing higher risks of AML/CFT;
- ensure adequate resources are given to the Compliance Officer to enable the AML/CFT standards and requirements within this Manual to be adequately implemented and periodically monitored and tested;
- ensure procedures are established and maintained which allow the Money Laundering Reporting Officer ('MLRO') and the Deputy Money Laundering Reporting Officer ('DMLRO');
- to have access to all relevant information, which may be of assistance to them in

considering suspicious transaction reports ("STRs");

- require a disclosure to the Financial Intelligence Unit ("FIU") when there is knowledge or suspicion or reasonable grounds for knowing or suspecting ML and/or TF, including attempted ML and/or TF; and
- maintain records for the prescribed periods of time.

1.5. Risk Based Approach

The FATF Recommendations provides for AML/CFT requirements allowing a business to adopt a risk-based approach towards the prevention and detection of money laundering and terrorism financing.

The FIAMLA and FIAML Regulations 2018 requires that risks posed by customers, products and systems are identified, mitigated and the mitigating factors documented and reviewed periodically. The legislations do not prohibit or prevent any type of business, customers, or systems from operating unless they are involved in ML/TF.

To demonstrate that a financial institution acted reasonably, an assessment of risk should always be documented, reasonably and objectively justifiable and sufficiently robust. Finally, while a risk-based approach grants a wide degree of discretion, parameters set by law or regulation may limit that discretion. The Company therefore shall always document its assessment of risk and ensure that it is kept up to date.

1.5.1. What is risk?

Risk can be seen as a function of three factors and ideally, a risk assessment involves making judgments about all three of these elements:

- **THREAT -** person or group of people, an object or an activity with the potential to cause harm. The threats may vary across customers, countries, geographic areas, products/services and delivery channels.
- **VULNERABILITY -** that which can be exploited by the threat or that may support or

facilitate its activities, such as size and volume of the business and client base profile.

- **CONSEQUENCE -** the impact or harm that ML or TF may cause, such as the impact on reputation and imposition of regulatory sanctions.

1.5.2. What is mitigation?

The Company must then take appropriate steps to mitigate any risks that have been identified. This will involve determining the necessary controls or procedures that need to be in place in relation to a particular part of the business in order to reduce the risk identified. The documented risk assessments that are required to be undertaken by the FIAMLA will assist the business to develop a risk-based approach.

Systems and controls may not always prevent and detect all ML/TF. A risk-based approach will, however, serve to balance the cost burden placed on the Company and its customers, with a realistic assessment of the threat of a business being used in connection with ML/TF. It focuses effort where it is needed and has most impact.

1.6. Assessing Compliance using a Risk-Based Approach

Finance institutions should avoid internal control systems that are repetitive for all clients which is counterproductive but rather implement a thorough thought process which will be more efficient. Internal systems should focus on risks posed by individual clients and relationships to mitigate appropriately and document the thought process.

The Company should properly demonstrate how it has documented risks assessed and how they have been mitigated and controlled.

In accordance with Regulation 31 of the FIAML Regulations 2018, any risk assessment system should be regularly reviewed to ensure effective system is in place and swift actions should be taken to remedy any identified deficiencies.

1.7. Importance of this Manual and Notes for the Compliance Officer

Section 17(A) of FIAMLA provides for the requirement to establish policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorism financing and implementation of the said policies, controls and procedures must be monitored, regularly reviewed, updated and, where necessary, enhanced.

The Compliance Officer must ensure that a copy of this Manual detailing the compliance arrangements is kept at the registered principal office in Mauritius and that it is available to relevant employees and to the relevant authorities upon inspection.

The Compliance Officer must ensure relevant employees are comfortable with their awareness of the legislation, and rules and regulations which affect them. The Compliance Officer may direct relevant employees to omit sections not relevant to their role and might decide to provide additional training/guidance in respect of certain areas of the Manual.

The Compliance Officer will also be responsible for undertaking day-to-day oversight of the program for combatting money laundering and terrorism financing and regular reporting including reporting of non-compliance to the Board and senior management.

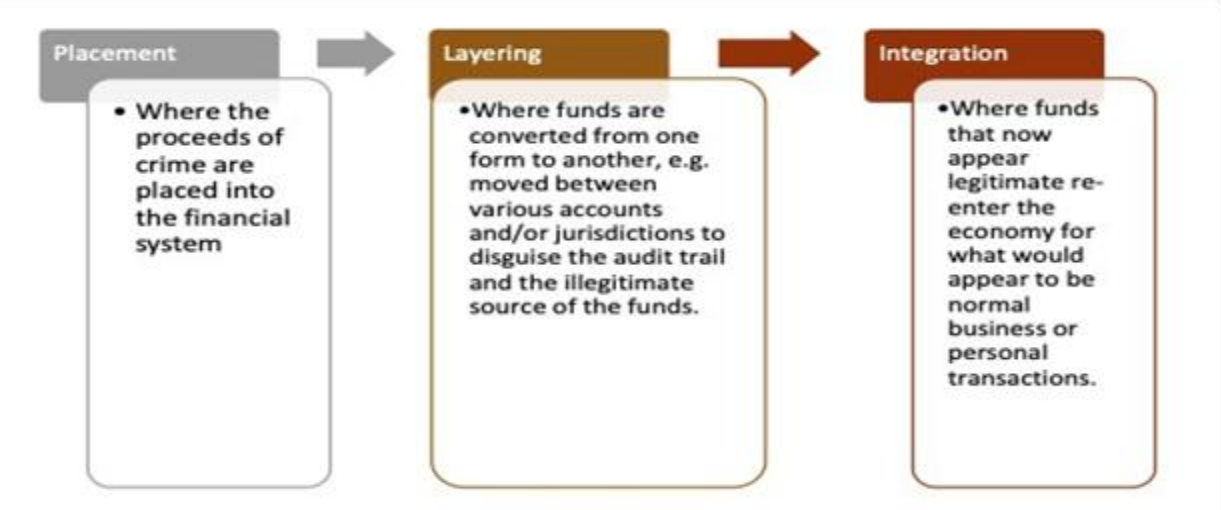
CHAPTER 2

Money Laundering, Terrorist Financing and Proliferation Offences

2.1. Money Laundering

In general terms, money laundering (ML) is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities. If successful, the criminal property can lose its criminal identity and appear legitimate, meaning that criminals can benefit from their crimes without the fear of being caught by tracing their money or assets back to a crime. Illegal arms sales, smuggling, and the activities of organised crime, including for example, drug trafficking and prostitution, can generate huge profits. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimise" the ill-gotten gains through ML.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds or assets to a place where they are less likely to attract attention and disguising ownership and control. Money laundering will often involve a complex series of transactions, traditionally represented in three separate phases:



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

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

III. **Integration -** This is the final stage in a complete money laundering operation. It involves reintroducing the illegal funds into the legitimate economy. The funds now appear as clean income.

2.2. Terrorist Financing

'Financing of terrorism' is defined under the UN (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act (2019) as the financing of terrorist, terrorist acts and terrorist organisations.

Terrorist financing is the act of providing financial support to acts of terror, terrorists or terrorist organisations to enable them to carry out terrorist acts. Unlike other criminal organisations, the primary aim of terrorist groups is non-financial. Yet, as with all organisations, terrorist groups require funds in order to carry out their primary activities.

TF differs from ML in that the source of funds can either be legitimate, such as an individual's salary, or illegitimate, like the proceeds of crimes such as selling pirate DVDs, fraud or drug trafficking. However, it should be noted that terrorist financing, while an offence in itself, is also a predicate offence for money laundering. Terrorist financing often involves a complex series of transactions, and this could be sourced through various means for example through seeking donations, carrying out criminal acts and from genuine charities.

The Company and its employees should at all times be aware of the above and protect themselves from being used as a conduit for such activities and make use of their already existing due diligence requirements, along with current policies and procedures on ML and enhance them where necessary to detect transactions that may involve terrorist funds.

2.3. Proliferation Financing

'Proliferation' and **'Proliferation financing'** have been defined in the FIAMLA as follows:

"proliferation" means -

a) *the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer, import, export, transshipment or use of -*
   - *nuclear weapons;*
   - *Chemical weapons;*
   - *biological weapons;*
   - *such other materials, as may be prescribed, which are related to nuclear weapons, chemical weapons or biological weapons; or*

b) *the provision of technical training, advice, service, brokering or assistance related to any of the activities specified in paragraph (a);*

"proliferation financing", in relation to a person, means the person who -

a) *makes available an asset;*
b) *provides a financial service; or*
c) *conducts a financial transaction; and knows that, or is reckless as to whether, the asset, financial service or financial transaction is intended to, in whole or in part, facilitate proliferation regardless of whether the specified activity occurs or is attempted.*

Proliferation of weapons of mass destruction 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 organisations or acting as representatives or intermediaries.

Moreover, the practical undertaking of proliferation financing often uses the same channels as terrorist financing. Measures to be applied in order to disrupt proliferation financing would therefore often be similar to the measures applied to counter terrorist financing.

2.4. The consequence of money laundering, terrorist financing and proliferation financing

Increased abuse of the financial system by criminal actors leads to increased criminal activity and less safety for everyone in the country and around the world. ML/TF can have serious negative consequences for the economy, national security and society in general. Some of these consequences may include:

- reputational damage from being perceived as being a haven for money launderers and terrorist financiers, leading to legitimate business taking their business elsewhere;
- attracting criminals including terrorists and their financiers to move to or establish new business relationships within the jurisdiction;
- damaging the legitimate private sector who may be unable to compete against front companies;
- weakening of financial institutions which may come to rely on the proceeds of crime for managing their assets, liabilities and operations, plus additional costs of investigations, seizures, fines, lawsuits etc;
- economic distortion and instability; or
- increased social costs to deal with additional criminality such as policing costs or hospital costs for treating drug addicts.

Also, Proliferation of weapons of mass destruction 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).

2.5. Anti-Money Laundering and Combating Terrorist and Proliferation Financing Framework in Mauritius

In Mauritius, the securities sector is regulated by the FSC for AML/CFT purposes. The AML/CFT framework and laws/regulations in relation to AML/CFT are more fully set out below.

A. FIAMLA and FIAML Regulations 2018

The FIAMLA and FIAML Regulations 2018 states offences which are related to ML and TF. Below are few salient provisions of the FIAMLA and FIAML Regulations 2018 which are applicable to the Company:

Section 3 of the FIAMLA states:

(1) Any person who -

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

b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime, where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime, shall commit an offence.

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

(3) In FIAMLA, reference to concealing or disguising property which is, or in whole or in part, directly or indirectly, represents, the proceeds of any crime, shall include concealing or

disguising its true nature, source, location, disposition, movement or ownership of or rights with respect to it.

Section 4 of the FIAMLA states:

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

Section 5 of the FIAMLA states:

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

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

Section 8 of the FIAMLA states:

(1) Any person who -

a) commits an offence under this Part; or

b) disposes or otherwise deals with property subject to a forfeiture order under subsection (2), shall, on conviction, be liable to a fine not exceeding 2 million rupees and to penal servitude for a term not exceeding 10 years.

(2) Any property belonging to or in the possession or under the control of any person who is convicted of an offence under this Part shall be deemed, unless the contrary is proved, to be derived from a crime and the Court may, in addition to any penalty imposed, order that the property be forfeited.

Section 16 of the FIAMLA states:

Legal consequences of reporting

(1) Any reporting person and auditor, and any of their officers shall not disclose to any person that a suspicious transaction report is being or has been filed, or that related information is being or has been requested by, furnished or submitted to FIU.

(3A) Any person who fails to comply with subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years.

Section 17(C)(6) of the FIAMLA states:

Customer due diligence requirements

Any person who knowingly provides any false or misleading information to a reporting person in connection with CDD requirements under the FIAMLA or any guidelines issued under this Act shall commit an offence and shall, on conviction, be liable to a fine not exceeding 500, 000 rupees and to imprisonment for a term not exceeding 5 years.

Section 19 of the FIAMLA states:

Offences relating to obligation to report and keep records and to disclosure of Information prejudicial to a request

(1) Any reporting person or any director, employee, agent or other legal representative of a reporting person, who, knowingly or without reasonable excuse -

a) fails to comply with section 17, 17A, 17B, 17C, 17D, 17E, 17F or 17G;

b) destroys or removes any record, register or document which is required under FIAMLA or any regulations;

c) *facilitates or permits the performance under a false identity of any transaction falling within this Part, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5*

years.

(2) Any person who –

a) falsifies, conceals, destroys or otherwise disposes of or causes or permits the falsification, concealment, destruction or disposal of any information, document or material which is or is likely to be relevant to a request to under the Mutual Assistance in Criminal and Related Matters Act 2003; or

b) knowing or suspecting that an investigation into a money laundering offence has been or is about to be conducted, divulges that fact or other information to another person whereby the making or execution of a request to under the Mutual Assistance in Criminal and Related Matters Act 2003 is likely to be prejudiced,

shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Section 19E(4) of the FIAMLA states:

Duty to provide information for purpose of conducting risk assessment

Any person who fails to comply with a request made under subsection (2)(b) shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

FIAML Regulations 2018

The FIAML Regulations 2018 made under section 17C, 17D, 17E and 35 of the Financial Intelligence and Anti Money Laundering Act provides further details on the requirements of a reporting person, the Company being a reporting person.

In this respect, the definition of "beneficial owner", "PEP" and "senior management" among others are further detailed in Regulations 2. Furthermore, the appointment and functions/duties of a compliance officer and those of the MLRO and deputy MLRO are more explicitly provided therein.

Regulation 33 states that any person who contravenes these regulations shall commit an offence and shall on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

B. FSC AML/CFT Handbook:

Paragraph 1.3 of the FSC AML/CFT Handbook set out the scope of the said document. It aims to enhance the understanding of FSC's expectations and help financial institutions assess the adequacy of their internal systems and controls and remedy deficiencies with the aim of combatting laundering of criminal proceeds, the financing of terrorism and the financing of proliferation of weapons of mass destruction. The Company shall stand guided by the fact that the FSC AML/CFT Handbook does not aim to prescribe an exhaustive list of recommended AML/CFT practices. The FSC AML/CFT Handbook specifically states that guidance set out in the FSC AML/CFT Handbook should be applied in a risk-based proportionate way.

Moreover, the FSC requires that if a financial institution already has its own systems and procedures in place which are not identical to those outlined in the FSC AML/CFT Handbook, then that financial institution should ensure that these systems and procedures in place are at least equal to if not higher than those requirements contained in the FSC AML/CFT Handbook. The Company shall stand guided therewith.

2.6. Other general Statutory framework in Mauritius

A. Financial Services Act 2007

The Company is licensed by the Financial Services Commission which is a body corporate established under the Financial Services Act (the 'FSA'). The FSC is mandated to inter alia ensure the orderly administration of the financial services and global business activities and ensure the sound conduct of business in the financial services sector and in the global business sector.

The FSC can also elaborate policies which are directed to ensure fairness, efficiency and transparency of financial and capital markets in Mauritius. The Company will have to ensure compliance with those polices as may be applicable to it.

B. Securities Act 2005

The Securities Act 2005 coupled with the Securities (licensing) Rules 2007 remain the main legal framework governing the provisions and setting the parameters within which a GBC with an Investment Dealer license can operate. There are different categories of Investment Dealer license and Securities (licensing) Rules 2007 clearly set out the activities authorized to be carried out under each category.

The Company being licensed by the FSC as an Investment Dealer (Full Service) excluding underwriting licence under the Securities Act 2005 will have to abide with the requirement of the law and regulations issued thereunder comply with new requirements as and when they come into force and ultimately, establish controls to always ensure compliance.

C. Companies Act 2001

The Companies Act 2001 provides for a core statement of company law that applies to all companies whether domestic or those with a global business licence. The Company is incorporated as a domestic company in Mauritius.

The Companies Act 2001 has been regularly amended to keep track of the changes in law having an incidence on Mauritius incorporated companies and has also kept abreast with the Financial Services Act 2007, which has had a direct bearing on Global Business Companies in Mauritius.

CHAPTER 3

Corporate Governance, Internal Controls and Risk-Based Approach

3.1. Introduction

The National code of corporate governance for Mauritius (2016) highlights the importance of the Board and senior management to inculcate a culture of compliance together by pursuing objectives that are in the best interests of the Company and its shareholders. They should provide for the effective monitoring of the Company for compliance with its AML and CFT obligations.

The implementation of sound corporate governance is key with an individual company as well as within the macroeconomic environment in building an environment of trust, transparency and accountability.

3.2. Board responsibility and oversight

In terms of the FSC AML/CFT Handbook, the Board of Directors of the Company is responsible for managing the Company effectively and is in the best position to understand and evaluate all potential risks to the Company, including those of ML and TF.

The responsibility for the assessment of business risk and ensure they are maintained and updated lies within the board and they should evaluate potential risks to the Company. This will be more fully detailed in this Manual and the Risk management Manual. The Board of Directors of the Company recognizes and acknowledges its responsibility for the system of AML/CFT internal control. The Company's policy on business conduct, which covers ethical behaviour, compliance with AML/CFT legislation and sound AML/CFT practice, underpins the internal AML/CFT control process.

The responsibilities and oversight of the Board of Directors of the Company should align with international best practices. The responsibilities of the Board shall include the following (non exhaustive requirements):

a) Approving the AML/CFT programme including all AML/CFT policies and procedures;

b) Ensuring the establishment of appropriate mechanisms for the periodic review of the AML/CFT policies and procedures to ensure their continued relevance in line with changes in the Company's products and services and to address new and emerging ML/TF risks;

c) Ensuring the establishment of an appropriate AML/CFT risk management framework with clearly defined lines of authority and responsibility for AML/CFT;

d) Ensuring that the Board receives the requisite training on AML/CFT and understand the Company's specific AML/CFT risks and controls;

e) Ensuring that the Board receives information about ML/TF risk assessment in a timely, complete, understandable and accurate manner so that it is equipped to make informed decisions. The reports escalated to the Board should include, inter alia, the following:

i. Internal / External audit reports and supervisory reports on AML/CFT

ii. Remedial action plans, if any, to address the results of compliance testing and self-identified instances of non-compliance with AML/CFT requirements, the findings of internal and/ or external audits; and regulatory reports received from the FSC and other regulators on their assessment of the Company's AML/CFT programme;

iii. Recent developments in AML/CFT laws and regulations and implications if any, to the Company;

iv. Details of recent significant risk events and potential impact on the Company; and

v. Statistics, including on statutory reporting to the FIU, orders from law enforcement agencies, sanctions imposed by regulators, refused or declined business and derisked relationships.

The Board should establish a formal strategy to counter money laundering and terrorist financing through policies and procedures and apportioning responsibilities in relation to the Compliance Officer and MLRO.

The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for ML and TF, and, in particular, responsibilities of the MLRO and Compliance Officer.

The responsibility for operating the AML/CFT system is delegated to executive management who confirm that they have reviewed its effectiveness. They consider that it is appropriately designed to provide reasonable, but not absolute, assurance that assets are safeguarded against material loss or unauthorised use and transactions are properly authorised and recorded. The effectiveness of the AML/CFT internal control system is monitored through management reviews, and a comprehensive program of internal audits.

3.3. Policies, controls and Procedures

Section 17A of the FIAMLA requires that every reporting person establish and maintain a record in writing of the policies, controls and procedures established to mitigate and manage effectively the risks of money laundering and terrorism financing. In that regard, the Company has established this Policy.

Furthermore, the implementation of the policies, controls and procedures must be regularly reviewed, updated and, where necessary, enhanced to reflect any legislative changes. The FSC AML/CFT Handbook specifically provides that policies established shall include provision as to the extent and frequency of compliance reviews taking a risk-based approach, which in the case of the Company; review will be done on an annual basis.

Any changes to those policies, controls and procedures made as a result of the review and update must also be recorded in writing. In this respect, the Compliance Officer of the Company shall maintain the Log for the review of this Manual as well as the date the changes have been notified to the staff of the Company. A template of the AML/CFT Policy review log is provided at ***Annex I***.

The FSC AML/CFT Handbook requires that the Company must establish written internal policies and procedures as well as comprehensive manual so that, in the event of a suspicious activity being discovered, all staff members are aware of the reporting chain and the

procedures to follow.

Along this line, all staff of the Company will be required to confirm that they have read and understood their obligations, upon both initial receipt and following any material changes made to this Manual thereafter, by completing and signing an Acknowledgement Form, in the template set forth at ***Annex II***.

The Company shall prepare and provide to employees a copy, in any format, of its policies, procedures and controls manual for AML and CFT; and ensure employees are fully aware of all applicable legislative requirements.

3.4. Appointment of Compliance Officer, Money Laundering Reporting Officer and Deputy Money Laundering Reporting Officer

As part of the internal controls and in terms of the FIAMLA, a Compliance Officer, a MLRO and a DMLRO must be appointed by the Company. It is imperative that all Board members and employees are made aware of the identity of the MLRO and DMLRO (so as to facilitate the reporting of suspicious transactions).

Paragraph 3.2 of the FSC AML/CFT Handbook further provides that the Board must clearly apportion responsibilities for countering money laundering and financing of terrorism, and in particular, responsibilities of the Compliance Officer, DMLRO and MLRO.

3.4.1. Appointment of a Compliance Officer

Financial institutions are required to appoint a Compliance Officer at Senior Management level in accordance with Regulation 22(1)(a) of the FIAML Regulations 2018, who will bear the responsibility for implementation and ongoing compliance of the financial institution with internal programmes, procedures and controls relating to money laundering and the financing of terrorism activities. The Compliance Officer should also have oversight of any monitoring and testing being conducted by the Company.

The Compliance Officer appointed by the Company must:

a) be a natural person;

b) be of at least senior management level as defined under FIAML Regulations 2018;

c) be an approved officer under Section 24 of the Financial Services Act; and

d) have the appropriate qualification, knowledge, skill and experience to fulfil a compliance role within the Company;

In accordance with Regulations 22(3) of the FIAML Regulations 2018, the functions of the Compliance Officer 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 Company 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 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.

Where the Compliance Officer holds additional functions or is responsible for other aspects of the Company's operations, the Company must ensure that any conflicts of interest between the responsibilities of the Compliance Officer's role and those of any other functions are identified, documented and appropriately managed. The Compliance Officer however should be independent of the core operating activities of the Company and that the Compliance Officer should not be engaged in soliciting business.

For the avoidance of doubt, the same individual can be appointed to the positions of MLRO and Compliance Officer, provided the Company considers this appropriate with regards to the respective demands of the two roles and whether the individual has sufficient time and

resources to fulfil both roles effectively. The Compliance Officer shall have unrestricted access upon request to all books, records and employees of the Company as necessary for the performance of his functions.

In accordance with Paragraph 3.4.1 of the FSC AML/CFT Handbook, the Company must ensure that the Compliance Officer:

a) has timely and unrestricted access to the records of the Company;

b) has sufficient resources to perform his or her duties;

c) has the full co-operation of the Company staff;

d) is fully aware of his or her obligations and those of the Company; and

e) reports directly to, and has regular contact with, the Board so as to enable the Board to satisfy itself that all statutory obligations and provisions in FIAMLA and FIAML Regulations 2018, and the FSC AML/CFT Handbook are being met and that the Company is taking sufficiently robust measures to protect itself against the potential risk of being used for ML and TF.

3.4.2. Appointment of a Money Laundering Reporting Officer and a Deputy Money Laundering Reporting Officer

Regulation 26 (1) of the FIAML Regulations 2018 requires that a financial institution 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 ML or TF.

Pursuant to Regulation 26 (2) of the FIAML Regulations 2018, financial institutions are required to appoint a DMLRO to perform the duties of the MLRO in his absence. Further to this, Regulation 26 (4) of the FIAML Regulations 2018 requires that the MLRO and the DMLRO shall –

a) be sufficiently senior in the organisation of the financial institution or have sufficient experience and authority; and

b) have a right of direct access to the board of directors of the financial institution and have sufficient time and resources to effectively discharge his functions.

In this context, the Company shall ensure that it has a MLRO and a DMLRO who shall:

a) be a natural person;

b) be an approved officer under Section 24 of the FSA; and

c) have the appropriate knowledge, skill and experience in accordance with the Competency Standards issued by the FSC in October 2014 (as amended);

The Company must ensure that the MLRO:

a) is the main point of contact with the FIU in the handling of disclosures (more details on these responsibilities are set out in Chapter 7 - Reporting of Suspicious Transaction);

b) has unrestricted access to the CDD information of the Company's customers, including the beneficial owners thereof;

c) has sufficient resources to perform his or her duties;

d) is available on a day-to-day basis;

e) reports directly to, and has regular contact with, the Board or equivalent of the Company; and

f) is fully aware of both his or her personal obligations and those of the Company under FIAMLA and FIAML Regulations 2018 and the Handbook.

The Company's employee shall be aware of the identity of the MLRO and of the DMLRO and the procedures to follow when making an internal disclosure report to the MLRO.

It is incumbent on the MLRO, on behalf of the Company, to make Suspicious Transaction Reports to the FIU. Moreover, the duties and responsibilities of the MLRO will lie on the DMLRO, in the absence of the MLRO.

3.4.2.1. Functions of the MLRO

The MLRO is the person who is nominated to ultimately receive internal disclosures and who considers any report to determine whether an external disclosure is required. He is the main point of contact with financial intelligence unit (FIU) for handling of disclosures.

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

a) implementing and monitoring the day-to-day operation of the AML/CFT policy and procedures;

b) reporting to the Board of Directors or a committee of the Board on any material breaches of the internal AML/CFT policy and procedures and of the AML/CFT laws, codes and standards of good practice;

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

    i. the adequacy/shortcomings of internal controls and other AML/CFT procedures implemented,

    ii. Recommendations to remedy the deficiencies identified above, the number of internal reports made by staff, and the number of reports made to the FIU.

d) have regular contact with the Board so as to enable the Board to satisfy itself that all statutory obligations and provisions and that the Company is taking sufficiently robust measures to protect itself against the potential risk of being used for Money laundering and terrorist financing.

Specific responsibilities of the MLRO and/or the DMLRO with regards to reporting requirements are set out under the section on Reporting Suspicious Transactions.

For avoidance of doubt, the duties and responsibilities of the MLRO will lie on the DMLRO, in the absence of the MLRO.

The Company shall ensure that at all times, it has in post a MLRO and a DMLRO which is based in Mauritius.

3.5. Compliance Monitoring records

Records of Compliance Monitoring in line with the functions set out above must be kept accordingly and this will aid in the monitoring of compliance requirements. Such records will also help the Company in reviewing the compliance policy, procedures and internal controls and maintaining an adequately resourced audit function.

Records include:

a) reports by the MLRO to the Board and senior management;

b) records of consideration of those reports and of any action taken as a consequence; and

c) any records made within the Company or by other parties in respect of compliance of the Company with the relevant AML/CFT laws and guidelines.

3.6. Independent Audit

Along with the requirements to have comprehensive procedures, policies and controls, the FSC AML/CFT Handbook also states that in addition to appointing a Compliance Officer, an independent audit function to test the anti-money laundering and combatting terrorist financing policies, procedures and controls of the financial institution should be maintained.

Thus, to satisfy the above requirement and in line with Regulation 22 of the FIAML Regulations 2018, the Company shall annually conduct an independent compliance review of its business to enable it to determine the effectiveness of its compliance and monitoring procedures, compliance with the provisions of the FIAML Regulations 2018 and relevant legislations.

The scope of the independent audit exercise is mainly a verification of the AML/CFT risk faced by the Company, where the independent audit shall mandatorily test compliance in the following non- exhaustive areas:

- AML/CFT policies and procedures;

- Internal Risk Assessment;
- Risk Assessment on the use of third-party service providers (Outsourcing);
- Compliance Officer function and effectiveness;
- MLRO function and effectiveness;
- Implementation and Effectiveness of Mitigating Controls, including customer due diligence and enhanced measures;
- AML/CFT Training;
- Record Keeping Obligations;
- Targeted Financial Sanctions; and
- Suspicious Transaction Monitoring and Reporting.

The Company shall ensure that that the person or firm conducting the audit should be independent and must not be involved in the development of Company's AML/CFT risk assessment, or the establishment, implementation or maintenance of its AML/CFT programme. The audit function shall be independent of and separate from the operational and executive team dealing with the AML/CFT processes of the Company.

The Company must be satisfied and able to demonstrate and ensure that the person function responsible for risk assessment and AML/CFT programme is not subject to any conflicts of interest. The Company shall ensure that the audit professional does not have financial interest in the company or have any relationship with any shareholder, director, senior management and or employees.

The Company shall conduct appropriate due diligence to confirm the proposed or selected professional auditor has the requisite competence and the criteria considered by the Company when assessing the independence and relevant experience of the external audit professional to effectively perform the audit, shall be properly documented and shall be made available to the FSC upon request.

The frequency and extent of the review should be commensurate with the Company's size, nature, context, complexity and internal risk assessment.

It is the responsibility of the board of directors of the Company to take appropriate corrective actions to remediate any issues identified in the independent audit report within the specified timelines. The Company shall file its independent audit report for a specified period, upon the request of the FSC.

All independent audit documentation, including, inter alia, work plan, audit scope, transaction testing, shall also be properly documented and shall be made available to the FSC, in accordance, with Section 13 of the FSC AML/CFT Handbook for the reason that the FSC may request specific information in regard to the audit from the Company.

3.7. Adopting a risk-based approach and risk profiling

3.7.1. Risk Based Approach

There is an overriding requirement for the Company to adopt a risk-based approach. The FSC AML/CFT Handbook provides that for adopting a risk-based approach, a financial institution must start with the identification and assessment of the risk that has to be managed.

Thus, the Company must assess the risks of how it might be involved in money laundering and terrorist financing, taking into account its customers (and the beneficial owners of customers), countries and geographic areas, the products, services and transactions it offers or undertakes, and the delivery channels by which it provides those products, services and/or transactions.

A risk-based approach prescribes the following procedural steps to manage the money laundering and terrorist financing risks faced by the Company:

a) identifying the specific threats posed;

b) assessing the likelihood of those threats occurring and the potential impact of them;

c) mitigating the likelihood of occurrence of identified threats and the potential for damage

to be caused;

d) managing the residual risks arising from the threats and vulnerabilities; and

e) reviewing and monitoring those risks to identify whether there have been any changes in the threats posed to the Company which necessitate changes to its policies, procedures and controls.

Adopting a risk-based approach shall help the Company in understanding the nature of the customer in a way that matches its risk and therefore the Company can allocate resources for the prudential conduct of business accordingly. The risk-based approach enables the Company to identify risks of being used for money laundering and terrorist financing and concurrently helps to adopt and implement appropriate and effective policies, procedures and controls to manage and mitigate the money laundering and terrorist financing risks.

3.7.2. Business Risk Assessment

Section 17 of the FIAMLA requires that appropriate steps be taken to identify, assess and understand the money laundering and terrorism financing risks for customers, countries or geographic areas and products, services, transactions or delivery channels.

Furthermore, all relevant risk factors must be considered before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied. The nature and extent of any said assessment shall be appropriate having regard to the nature and size of the business of the Company.

The Company must monitor the implementation of, regularly review, update and, where necessary, enhance the, policies, controls and procedures put in place to mitigate and manage the risks of money laundering and terrorism financing identified.

Regulation 31 of the FIAML Regulations 2018 sets the requirement for the Company have a robust and documented arrangements in place for managing the risks identified by the business risk assessment conducted in accordance with section 17 of FIAMLA and as detailed

above. Prompt action must be taken to remedy any deficiencies in those arrangements should be identified.

Section 17(2) of the FIAMLA requires businesses to assess 6 key areas when undertaking the business risk assessment amongst other risk factors. Thus, the Company shall assess:

a) the nature, scale and complexity of activities;

b) the products and services provided;

c) the persons to whom and the manner in which the products and services are provided;

d) the nature, scale, complexity and location of the customer's activities;

e) reliance on third parties for elements of the customer due diligence process; and

f) technological developments.

3.7.3. Customer Risk Assessment

As part of adopting a risk based approach, the Company must also identify the potential risk which a business relationship with a customer will pose. It also involves assessing the potential risks the Company would be exposed to in conducting business with a client. These risks include:

a) **Criminal risk** (i.e., the probability of being embroiled in a crime such as money laundering for example),

b) **Reputational risk** (i.e., the probability of the Company's reputation being undermined),

c) **Legal risk** (i.e., the possibility of the Company being prosecuted or involved in legal proceedings),

d) **Credit risk** (i.e., the risk of financial loss),

e) **Regulatory risk** (i.e., the risk of facing regulatory sanctions), and

f) **Operational risk** (i.e., the probability of disruption in the normal flow of business

operations).

Need for documented policies and procedures:

The overriding requirement is for the Company to undertake a risk assessment prior to establishing a business relationship or carrying out occasional transaction with a customer so as to determine the level of risk associated with doing business with that customer.

This is done via the Company's 'Customer Onboarding Checklist" – which will continuously be revised and approved by Senior Management and/or Board to ensure that it is appropriate and adequate to the business needs of the Company, and covering the below areas (as minimum):

- Client Risk
- Geographic Risk
- Service Risk
- Industry Risk
- Delivery Channel Risk

In line with section 17 (4) of FIAMLA, the Company must document the risk assessments undertaken in writing and keep it up to date. The policies in place must be in line with the nature and complexity of the Company's operations. The Company must record and document its risk assessment in order to be able to demonstrate its basis. Thus, identification of risks, its assessment, steps used to mitigate and manage those risks must be kept in writing.

Regarding frequency of the reviews, customer risk assessments should be reviewed:

- at least every 6 months for higher risk customers or whenever a transaction with a high risk country or high risk customer occurs (however, at least every 3 months for PEP clients);
- at least on an annual basis for standard risk customers subject to sector specific guidance (medium risk);

- at least on a biennial basis (2 years basis) for low risk customers and
- at the point of a material change in the customer's circumstances, for example establishing connections with a higher risk jurisdiction or engaging in a higher risk business.

The Company shall implement a Risk Management Framework in place, along with a Risk Profiling Policy, which may be updated from time to time, as necessary. These will be more fully detailed in the Risk Management Manual.

Risk factor and weightage:

The FSC AML/CFT Handbook provides that when assessing the risks posed by a customer, the Company must consider all risk factors that are known. The risk assessment conducted by the Company shall amongst others consider the following factors:

a) The type of client (individual, company etc.),

b) The type of product/service being sought by the client,

c) The business rationale for the relationship,

d) How the client was introduced to the Company,

e) The geographical location of the client's residence,

f) The geographical location of the client's business interests and/or assets,

g) The nature and value of the assets concerned in the relationship,

h) The client's source of funds and where necessary the source of wealth, and

i) Whether there is any adverse information on the client and/or its Principals where applicable.

To note that the risk factors are not exhaustive and are not prescribed as a checklist. It will be for the Company to determine what is appropriate in its case and it is not expected that all factors will be considered in all cases.

Each risk factor must be assessed and detailed to demonstrate how the conclusion of each

risk assessment conducted has been reached and accordingly a weight associated to it in the risk assessment policy.

The Company must also take appropriate steps to mitigate the opportunity for those risks to materialise. In this context, when weighting risk factors, the Company should ensure that:

a) weighting is not unduly influenced by just one factor;

b) economic or profit considerations do not influence the risk rating;

c) weighting does not lead to a situation where it is impossible for any business relationship or occasional transaction to be classified as a high-risk relationship;

d) the provisions of Regulation 12(1) of FIAML Regulations 2018 setting out the situations which will present a high risk (for example, the involvement of Politically Exposed Persons or in event of suspicious activity) cannot be over-ruled by the Company's weighting; and

e) the Company is able to override any automatically generated risk scores where necessary.

Furthermore, where the Company is overriding any automatically generated scores, the rationale for the decision to override such scores should be documented appropriately.

ML/FT risks relative to CFDs on Cryptocurrencies:

In the context of CFDs, where traders speculate on the price movements of cryptocurrencies without owning the underlying assets, there is a heightened risk of criminals exploiting these instruments to launder proceeds of crime or finance terrorist activities. The pseudonymous nature of cryptocurrency transactions and the ease with which funds can be transferred across borders further exacerbate the ML/FT risks associated with Crypto CFDs. Moreover, the volatile nature of cryptocurrency markets and the potential for rapid price fluctuations create opportunities for criminals to exploit price differentials and conceal illicit transactions within the complexity of trading activity, making detection and mitigation of ML/FT risks particularly challenging in this context.

It is imperative to mitigate ML/FT risks when dealing with Crypto CFDs to safeguard the

integrity of financial markets and protect against the proliferation of illicit activities. Failure to address these risks not only exposes the Company to legal and regulatory sanctions but also undermines trust and confidence in the broader financial system. The interconnected nature of financial markets means that illicit funds laundered through Crypto CFDs can potentially flow into other sectors, posing systemic risks and facilitating further criminal activities. Moreover, the reputational damage resulting from association with ML/FT activities can have far-reaching consequences, including loss of customer trust, regulatory scrutiny, and damage to brand reputation.

The Company is alive to the fact that when offering the trading of CFDs on Cryptocurrencies, it may be exposed to more diverse ML/FT risks. While recognising the unique characteristics of such products, the Company will inter alia consider the following:

a) the inherent volatility of cryptocurrency, including rapid price fluctuations,

b) the customer's profile,

c) the customer’s transactional behaviour, and

d) the nature of the customer’s cryptocurrency CFD trading activities and if they have prior knowledge of such product,

when carrying out the customer risk assessment,

CHAPTER 4

Customer Due Diligence

4.1. Introduction

Customer Due Diligence (CDD) is a crucial process for the Company to know its customers for the prevention of money laundering and combating the financing of terrorism. CDD is a key element of an internal AML/CFT system. The CDD requirement for any financial institution must be based on a risk-based approach to decide the type and extent of CDD measures to apply to a different type of customers, products and services.

In this respect, the Company must identify its customers and their beneficial owners and verify their identities and investigate their beneficial owners. CDD information on the customer and the beneficial owners must be kept up to date.

Identification and verification refer to establishing and verifying a customer's identity. Verification refers to the verification of elements of the identification information, by using independent reliable sources, which may include material obtained from the customer such as a passport to verify the customer's name. It is essentially the concept of the Company satisfying itself that its customer is who they say they are.

The Company, as an Investment Dealer (Full Service) excluding Underwriting Licence holder, before a new client is accepted, should inter alia carry out vetting procedures on such owners, promoters, controllers, directors or shareholders of an applicant company as may be appropriate. A controller is defined as meaning in relation to a body corporate, a person who either alone or with any associate or associates, is entitled to exercise or control the voting power at any general meeting of that body corporate or another body corporate of which it is a subsidiary. A written record of the findings must be retained on file.

The inadequacy or absence of satisfactory CDD measures can subject the Company to serious customer and counterparty risks, as well as reputational, operational, legal and regulatory risks, any of which can result in significant financial cost to its business.

Effective CDD measures are vital because they:

a) help to protect the Company and, more widely, the integrity of the financial system of the jurisdiction and globally, by reducing the likelihood of the Company's business becoming a vehicle for, or a victim of, financial crime;

b) assist law enforcement agency, by providing it with relevant information ascertained via CDD in the event of a suspicious transaction report ('STR'); and

c) constitute an essential part of sound risk management, for example by providing the basis for identifying, limiting and controlling the risk posed by particular customers or classes of customers.

4.2. General Identification Requirements

The Company must, on the basis of the relevant CDD information collected, make an analysis of the information provided and make such appropriate verification using external database or source, and consider whether it is appropriate to collect further CDD information.

CDD information comprises both identification and verification information and customer relationship information.

In this respect and in line with the Regulation 3 of the FIAML Regulations 2018, the Company shall –

a) identify its client whether permanent or occasional and verify the identity of its client using reliable, independent source documents, data or information;

b) verify that any person purporting to act on behalf of a client is so authorised, and shall identify and verify the identity of that person;

c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner of the client, using relevant information or data obtained from a reliable source such that the reporting person is satisfied that he knows who the beneficial owner is;

d) understand and obtain adequate and relevant information on the purpose and intended nature of a business relationship or occasional transaction.

e) conduct ongoing due diligence on the business relationship and scrutiny of transactions throughout its course, to ensure that the transactions in which the customer is engaged are consistent with the Company's knowledge of the customer and his risk profile (including the source of funds); and

f) ensure that all material collected under the CDD process is kept relevant and up to date (for example undertaking reactive reviews in response to trigger events, and by undertaking regular planned reviews of existing records at intervals determined by risk rating, with higher risk customers warranting more frequent reviews).

The Company shall conduct the CDD process on its prospective customers and current customers and requests for documents from them as shown in the table below.

KYC Documents requirement based on Customer type	
<u>High Risk</u> • Jewellery, Import-export, Mining, Shipping, Agriculturist etc • Trusts/Charities/Non-government organisations receiving donations • Companies with close family shareholding & Beneficial ownership • Firms with sleeping partners • Politically Exposed Person (PEPs)	**<u>Basic KYC</u>** • Identity Proof * • Company incorporation documents / Partnership deed, trust deed * • Address proof (Optional) **<u>Enhanced KYC</u>** • Proof of Income
<u>Low Risk</u> • Salaried • Business with licence / under strict supervision	**<u>Basic KYC</u>** • Identity Proof * • Address proof (Optional)

• Professional	

As per the AML/CFT Handbook, 'beneficial owner(s)' is defined as the natural person(s) who ultimately owns or has control over a customer or the person(s) on whose behalf a transaction is being conducted. This also includes those natural persons who exercise ultimate control over a legal person or arrangement and such other persons as may be specified in Regulations 6 and 7 of the FIAML Regulations 2018.

CDD Procedures are also maintained to help the Staff of the Company to identify those unusual transactions. In this respect, as per the FSC AML/CFT Handbook, the Company must also have in place clear, documented procedures governing how they will:

a) identify and verify the identity of their applicants for business and existing customers on a risk-based approach (including identifying and verifying the identity of any connected individuals such as beneficial owners and controllers of the applicant);

b) determine whether or not an applicant for business is acting or intending to act for a third party; and

c) where the Company is unable to determine whether the applicant is acting for a third party or not, make a suspicious activity report pursuant to section 14 of the FIAMLA to the Financial Intelligence Unit.

These procedures must be brought to the knowledge of and be readily available to all relevant staff for the creation of an effective internal compliance culture and all staff will be aware of the reporting chain and procedures to follow.

4.3. Customer due diligence requirements

Pursuant to Section 17C of the FIAMLA, the Company, as a reporting person, shall inter alia undertake CDD measures as may be prescribed and in the following circumstances -

a) when establishing a business relationship with, and/or carrying out any business

transaction for or on behalf of the applicant for business;

b) whenever doubts exist about the veracity or adequacy of previously obtained customer identification information;

c) whenever there is a suspicion of money laundering or terrorism financing involving the customer or the customer's account at any point in time;

The Company shall, with respect to each customer and business relationship, when applying CDD measures, consider the outcome of the national risk assessment.

When the risks are higher, the Company shall conduct enhanced due diligence measures consistent with the risks identified, as morefully described in this Manual.

Furthermore, the Company must ensure that there is consistency between the information they hold on the applicant /customer and the nature of transactions or proposed transactions.

Where there is any indication of abnormal or potentially suspicious activity within the context of the product or service being provided, or any other event occurs to cast doubt on the CDD held by the Company, then the Company must take additional measures to verify the information already obtained and to obtain such further information as may be necessary to pursue the transaction.

4.4. Identification and Verification of Natural Persons

Regulation 4 of the FIAML Regulations 2018 lays down specific requirements for natural persons (applicants or beneficial owners/controllers of applicants). In line therewith, the Company shall obtain and verify -

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;

e) details of employment or professional occupation, or any public position held, and

f) details on the activity or transaction that generated the funds/property to be invested/managed and

g) such other information as may be specified.

The data to be collected and the permissible methods for verifying the same are set out hereunder:

Data to be collected	**Document to be requested (In Original or Certified True Copy)**
1. Legal name (including any former names, aliases and any other names used) **2.** Sex **3.** Data of birth **4.** Place of birth **5.** Nationality	• Current valid passport, or • Valid National Identity Card, or • Current Valid driving licence (where the Company is satisfied that the driving licensing authority carries out a check on the holder's identity before issuing the licence). • Government issued personal identification number or other government issued unique identifier for example National Identity Card (NIC) number or passport number ***Note: The document used must incorporate photographic evidence of identity of the natural person***
6. Current residential address and mailing address	• A recent utility bill issued to the individual by name, or • A recent bank or credit card statement, or • A recent reference or letter of introduction from

7. Permanent residential address (if different to current residential address)	a) a financial institution that is regulated in Mauritius, b) A regulated financial services business which is operating in an equivalent jurisdiction or a jurisdiction that complies with the FATF standards; or c) 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. ***Note:*** • ***Recent means within the last three months*** • ***PO Box Addresses are not acceptable.***
8. Professional Reference	• Recent Bank reference letter, or • Recent reference letter issued by a professional person, who has known the applicant for business in his professional capacity. **Note: Recent means within the last three months.**
9. Occupation type **10.** Name of employer or nature of self-employment/nature of business.	• Information on the profession of the natural person including adequate documentary evidence supporting the same, • Updated CV on the Natural Person. If the client holds/have held public position, the Company shall request for evidence or confirmation,

	where appropriate: • Nature of the employment, • The name of the employer, • Letter or other written confirmation of the individual's status from the public body, or • A letter or other written confirmation of employment.
11. Source of Funds / Source of Wealth	• A declaration on the source of funds/ source of wealth of the natural person, • Adequate and relevant supporting evidence on the source of funds/ source of wealth.

In addition, as per the FSC AML/CFT Handbook, the Company must collect and analyse the identification data on a natural person, and verify that data, in accordance with the following:

a) The data to be collected applies to both standard and high-risk applicants for business.

b) The appropriate number of methods for verifying the data will vary depending on whether the customer is standard or high risk.

4.5. Identification and Verification of Legal Persons or Legal Arrangements

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

a) **"legal arrangements"** means an express trust or other similar arrangement;

b) **"legal persons"** means any entity other than a natural person that can establish a permanent business relationship with a reporting person or otherwise own property, including a company, body corporate, foundation, or any other similar entity, partnership or an association or other similar entities;

Where the customer is a legal person or legal arrangement, the Company shall –

a) with respect to the customer, understand and document –

   (i) the nature of his business, and

   (ii) his ownership and control structure.

b) identify the customer and verify his identity by obtaining the following information –

   (i) name, legal form and proof of existence, incorporation/ registration number and date of same;

   (ii) country of incorporation;

   (iii) powers that regulate and bind the customer;

   (iv) names of the relevant persons having a senior management position in the legal person or arrangement; and

   (v) the address of the registered office and, if different, a principal place of business.

Furthermore, the FSC AML/CFT Handbook provides that for express trusts, the CDD information should provide the type of trust (e.g. discretionary), the structure of any underlying legal bodies (if applicable) and nature of activities undertaken by the trust and any underlying legal bodies. And, this should also include the classes of beneficiaries and classes within an expression of wishes.

In instances where the customer is a legal person or legal arrangement, the Company shall also identify and take reasonable measures to verify the identity of beneficial owners by obtaining information on the identity of all the natural persons who ultimately have an ownership interest of 20 per cent or more in the legal person.

To the extent that there is doubt as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person(s) exert control through ownership interests, the identity of the relevant person who holds the position of senior managing official must be established.

Furthermore, a structure chart showing the ownership and control of the applicant for

business must be submitted. The Company shall ensure that it keeps a register of beneficial owners - the Beneficial Owner Register, template of which is set out in ***Annex III***.

The data to be collected and the permissible methods for verifying the same as regards to legal persons are set out hereunder:

Data to be collected	**Document to be requested** **(In Original or Certified True Copy)**
1. Legal name **2.** Any trading names **3.** Date and country of incorporation/ registration **4.** Official identification number (E.g. company number)	• Certificate of incorporation / registration (or equivalent document) • *Partnership:* Certificate of registration of the partnership (if registered) • *Société:* If the Société is registered, the certificate of registration • *Foundation:* If the Foundation is registered, certificate of registration
5. Legal status	• Certificate of current standing, or • Company registry search, including confirmation that it is not in the process of being dissolved, struck off, wound up or terminated.
6. Nature of business **7.** Powers that regulate the legal person	• Latest audited financial statements/annual report or equivalent • Constitution or Memorandum and Articles of Association • *Partnership:* Partnership Agreement/ Deed Société: Acte de Société

	• *Foundation:* Charter and/or Articles of the Foundation.
8. Registered office address **9.** Mailing address (if different from registered office address) **10.** Principal place of business	• Personal visit to principal place of business • Reputable and satisfactory third-party verification or confirmation on the office address/principal place of business (e.g. utility bill, lease agreement, etc) • Any constitutive documents of the legal person/arrangements establishing the same
11. Identity and verification of underlying principals **12.** Identity of all the natural persons who ultimately have a controlling ownership interest in the legal person.	• Updated Register of directors • Updated Register of shareholders • Updated Structure Chart • *Partnership:* Register of Partners • *Société:* Latest Register (or equivalent document) showing the names, addresses and holding of partners or associés. • *Foundation:* Register or equivalent document showing the names and addresses of the members of the Foundation's Council, the Founder and any person who may have endowed assets to the Foundation. ***Note: When seeking to identify and verify the identity of underlying principals, reference should be made to the identification and verification requirements for natural persons.***

The data to be collected and the permissible methods for verifying the same as regards to legal arrangements are set out hereunder:

Data to be collected	**Document to be requested (**For Trust**)** **(In Original or Certified True Copy)**
1. Legal name **2.** Legal status **3.** Any trading names	If the Legal Arrangement is registered, certificate of registration
4. Nature of business	• Trust Deed or equivalent document • Information on the purpose of the Trust.
5. Source of funds/wealth	• Declaration of source of funds and/or wealth • Relevant supporting documents (as may be required by the Company) • Information on the origins of the trust assets
6. Registered office address, if applicable **7.** Mailing address (if different from registered office address), **8.** Principal place of business	• Details of the registered office and place of business of the trustee.
9. Identity of principals	*Identity and verification of:* • Settlor • Trustee • Beneficiaries/class of beneficiaries • Protector (where applicable)

	• Any other natural person exercising ultimate effective control over the trust, including through a chain of control or ownership need to be verified. ***Note: For other types of legal arrangements, the identity of the persons in equivalent or similar position need be identified and verified in likewise manner.***

4.6. Individuals acting on behalf of clients – Authorised Signatories

Individuals authorised to act on behalf of clients may be for example, a person authorised to instruct the Company to transfer funds on the customer's behalf and authority may derive from a number of possible sources: for example, a power of attorney, or an authorised signatory mandate form or Board resolution, or a trust instrument (authorised signatories").

Such authorised persons pose a risk to the Company It is common trend and typology for money laundering criminals to divest the direct ownership and corporate control of their entity using nominee directors and shareholders, but they keep the control of the accounts by being inscribed as authorized signatories for example.

The Company requires that the same diligence as expected for a director of an applicant for business would be expected for authorized signatories.

4.7. Screening

As part of identification measures, the Company shall perform searches and screen prospective clients and all their Principals (in the case of legal persons/arrangements) against independent and reliable databases to ascertain whether:

a) they have any connections to organized crime, drug trafficking, arms & weapons dealing, human trafficking, foreign official corruption, violent crime, or terrorism;

b) they are or have been subject to any convictions or allegations of any fraudulent or criminal/questionable activities;

c) there is any negative press, i.e., any given negative information, whether alleged or factual; or

d) they are Politically Exposed Persons (PEP), or on any international sanctions/ watch lists.

Consideration shall be given to the credibility of the source of information, the severity of the negative press, how recent the information is and the potential impact the negative press would have on the business relationship with that customer.

Following the screening, the Company shall document:

a) the source and date of the search,

b) actions taken to confirm or discount any potential match,

c) details of the negative press report,

d) any actions taken to verify, disprove or discount the claims/reports, and

e) any additional actions taken as a result of this information such as treating the customer as high risk and/or seeking more details on proof of source of wealth/funds, etc.

In the event the screening results indicate that the client and/or any of its Principals falls within any of the categories listed above, the Company shall conduct Enhanced CDD measures by requesting for further information.

4.8. Targeted Financial Sanctions

Pursuant to section 41 of the UN Sanctions Act, the Company must implement internal controls and other procedures to enable it to effectively comply with its obligations under the UN Sanctions Act. These obligations may be categorised as follows:

A. Screening of sanctions:

i. Customer Screening

Section 25 of the UN Sanctions Act requires that, every reporting person must verify whether the details of a listed party match with the particulars of any customer, and if so, to identify whether the customer owns any funds or other assets in Mauritius. All

customers and transactions must therefore be screened against sanctions lists for potential matches.

When establishing a new business relationship, as part of the screening process, the Company shall therefore ascertain whether the prospective client and its Principals (where applicable) are listed on the UN Sanctions List or list issued by the National Sanctions Committee, or if they are connected to persons who are listed on such lists.

The above also applies, when conducting on-going monitoring during the course of the business relationship with a client. Therefore, as part of the screening process for the purpose of on-going monitoring, the Company shall verify whether the client and its Principals (where applicable) are listed on the UN Sanctions List or list issued by the National Sanctions Committee, or if they are connected to persons who are listed on such lists.

ii. Transaction monitoring

Pursuant to section 23(1) of the UN Sanctions Act, it is an offence to deal with the funds/other assets of a person listed on the UN Sanctions List or list issued by the National Sanctions Committee established under the UN Sanctions Act.

Screening against the UN Sanctions List and list issued by the National Sanctions Committee must also be done for each incoming and outgoing transaction before carrying out the transaction on the parties involved in the transaction (i.e., on the remitter, beneficiary, intermediaries and any other party involved in the transaction).

In addition, the following data points must be verified when conducting transaction monitoring:

- The parties involved in the transaction (i.e., the remitter, beneficiary, intermediaries and other parties involved in the transaction),
- Bank names, bank identifier codes and other routing codes,

- Free text fields (such as payment reference/purpose detail).

iii. Sanctions Match and Resolving False Positives

During the screening process if a match is detected (i.e., if it is found that a client, a Principal of a client or a party to transaction is listed or is connected to a person listed on the UN Sanctions List or list issued by the National Sanctions Committee), the Company must immediately:

- halt the transaction in question to avoid committing an offence under section 23 of the UN Sanctions Act, and
- Investigate further based on the information available to the Company and the identifying information provided in the sanctions list to confirm the match.
- Report the positive match, or document any discounting thereof.

B. Reporting obligations:

In case the Company detects a positive match (i.e., particulars of a client or Principal of a client match the details of a person listed on the UN Sanctions List or list issued by the National Sanctions Committee), the Company is required under section 25(2) of the UN Sanctions Act to make a report to the National Sanctions Secretariat using the template to be downloaded from the website of the National Sanctions Secretariat (http://nssec.govmu.org) to the following email address nssec@govmu.org.

Where the Company makes a report to the National Sanctions Secretariat under section 25(2) of the UN Sanctions Act as per above, it must also report the same to the FSC.

Furthermore, in line with section 39 of the UN Sanctions Act the Company must immediately submit a STR to the FIU if it has any information related to a person listed on UN Sanctions List or list issued by the National Sanctions Committee. Therefore, following screening if it is discovered that a client or a Principal of a client is listed on UN Sanctions List or list issued by the National Sanctions Committee and where the one

carrying the screening is not the MLRO, an internal suspicious transaction report must be submitted to the MLRO of the Company for onward action.

4.9. Source of funds and Source of Wealth

The FSC AML/CFT Handbook requires that the Company scrutinise the source of funds and source of wealth of the customer to understand the origin or provenance of funds or property underlying a business relationship with a customer.

The source of funds normally refers to the origin of the particular funds or assets which are the subject of the business relationship between the Company and its client and the transactions the Company is required to undertake on the client's behalf (e.g., the amounts being invested, deposited or remitted). The source of funds requirement refers to where the funds are coming from in order to fund the relationship or transaction. This does not refer to every payment going through the account; however, the Company must comply with the ongoing monitoring provisions laid down in this Manual.

On the other hand, the source of wealth is distinct from source of funds and describes the origins of a customer's financial standing or total net worth i.e., those activities which have generated a customer's funds and property. Where so applicable, the Customer is required to hold sufficient information to establish the source of wealth and this information must be obtained for all higher risk customers (including higher risk domestic PEPs) and all foreign PEPs and all other relationships where the type of product or service being offered makes it appropriate to do so because of its risk profile. The Company requires prospective customers to declare their source of wealth on the application form and provide the supporting documents to prove this at onboarding stage.

The Company shall ensure that there is consistency between the information it holds on the applicant for business and the nature of transactions or proposed transactions.

Where there is any indication of abnormal or potentially suspicious activity within the context

of the product or service being provided, the Company must take additional measures to verify the information obtained. In such cases, the Company shall also consider obtaining information regarding an applicant's or a customer's source of wealth. This is one of the Enhanced Due Diligence measures which must be applied in cases of high-risk relationships.

The Company shall not proceed further with the on boarding if it is not satisfied that the source of funds is properly identified, or if the funds are derived from an illegitimate source, in which case a STR must be filed.

CHAPTER 5

Enhanced/Simplified Customer Due Diligence

5.1. Introduction

Regulation 12(1) of the FIAML Regulations 2018 requires that the Company perform Enhanced Customer Due Diligence (Enhanced CDD) in inter alia the following circumstances:

a) where a higher risk of money laundering or terrorist financing has been identified;

b) where through supervisory guidance, a high risk of money laundering or terrorist financing has been identified;

c) where a customer or an applicant for business is from a high risk third country;

d) where the customer or the applicant for business is a political exposed person;

e) where a reporting person discovers that a customer has provided false or stolen identification documentation or information and the reporting person proposes to continue to deal with that customer;

f) in the event of any unusual or suspicious activity.

When the ML/TF risks are identified to be higher, the Company shall take Enhanced CDD measures to mitigate and manage those risks. The Company must assign a high-risk rating to the applicant for businesses where high risk of ML and TF has been identified.

Pursuant to Regulation 12(2) of the FIAML Regulations 2018, the Enhanced CDD measures that the Company may apply for higher risk business relationships include the below:

a) Requesting additional information on the customer (e.g. occupation, volume of assets, information available through public databases or internet, etc) and updating on a frequent basis the identification data of the customer or beneficial owner,

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

c) obtaining information and documentary evidence on the purpose and reasons for

intended or performed transactions,

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

e) 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,

f) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards as that of Mauritius, and

g) any other measures a financial institution may undertake with relation to a high-risk relationship.

Note that the above list is not exhaustive and staff of the Company is encouraged to assess risks on a case-by-case basis.

Where the client is an individual, the Company shall establish and obtain evidence of the individual's source of wealth as an Enhanced CDD measure. Source of wealth is defined as the activity/event which generated the individual's net worth. Hence, over and above information required above, the Company shall obtain a duly completed and signed Declaration of Source of Wealth Form from the client together with the relevant supporting document.

Where the Company is unable to perform the enhanced CDD, it shall terminate the business relationship and file a suspicious transaction report under section 14 of the FIAMLA.

5.2. High Risk Jurisdictions

Responding to the threat posed by high-risk and non-cooperative jurisdictions is a key objective of the FATF's mission for promoting the global implementation of its AML/CFT standards.

Worldwide compliance with the standards protects the integrity of the international financial system and enhances international co-operation on AML/CFT. FATF regularly publishes the

following lists:

- Jurisdictions that have strategic AML/CFT deficiencies and to which counter-measures apply, and
- Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies.

Regulation 24(1) of the FIAML Regulations 2018 provides that, in identifying a high risk country, due consideration shall be given to:

a) strategic deficiencies in the anti-money laundering and combating the financing of terrorism legal and institutional framework, in particular in relation to –

   i. criminalisation of money laundering and terrorism financing;

   ii. measures relating to CDD;

   iii. requirements relating to record-keeping;

   iv. requirements to report suspicious transactions; and

   v. the availability of accurate and timely information of the beneficial ownership of legal persons and arrangements to competent authorities;

b) the powers and procedures of the country's competent authorities for the purposes of combating money laundering and terrorist financing including appropriately effective, proportionate and dissuasive sanctions, as well as the country's practice in cooperation and exchange of information with overseas competent authorities;

c) the effectiveness of the country's system for combating money laundering and terrorism financing in addressing money laundering or terrorist financing risks.

Section 17H (1) of the FIAMLA provides that where a jurisdiction is identified by the FATF as having significant or strategic deficiencies in its AML/CFT measures, the Minister of Financial Services and Good Governance ('Minister') may, on the recommendation of the National

Committee for Anti-Money Laundering and Combating the Financing of Terrorism (National Committee), identify that jurisdiction as a high risk country. In this respect, in light of the jurisdictions identified by FATF in its statement, "High-Risk Jurisdictions subject to a call for action" dated 21 February 2020, and on the recommendation of the National Committee for AML/CFT, the Minister has, on 4 May 2020, published a General Notice (Notice) entitled "Identification of high risk country by the Minister of Financial Services and Good Governance under section 17H (1) of the Financial Intelligence and Anti-Money Laundering Act", wherein the Democratic People's Republic of Korea (DPRK) and Iran have been identified as high-risk countries.

The Company, as a reporting person, is therefore required to apply such enhanced CDD measures as prescribed in the FIAML Regulations 2018 with respect to business relationships or transactions involving those high risk countries. In addition, it shall, where applicable and proportionate to the risks, apply one or more of the following additional mitigating measures to persons and legal entities carrying out transactions involving those high-risk countries –

- the application of additional elements of enhanced due diligence;
- the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions;
- the limitation of business relationships or transactions with natural persons or legal entities from those high-risk countries.

5.3. Politically Exposed Persons (PEPs)

In line with the FIAMLA and the FIAML Regulations 2018, the definition for a PEP includes any individual who are or who have been entrusted with prominent public functions including:

(1) Heads of state, heads of government, ministers and deputy or assistant ministers;

(2) Members of Parliament or National Legislatures;

(3) Senior officials of major political parties;

(4) Senior judicial officials, i.e. members of supreme courts, constitutional courts or other

high-level judicial bodies;

(5) Members of the Boards of Central Banks;

(6) Senior members of the Diplomatic Corps e.g. ambassadors and charges d'affaires;

(7) Heads and high-ranking officers holding senior positions in the armed forces;

(8) Senior Executives of State-owned enterprises i.e. members of the administrative, management or supervisory bodies; and

(9) Heads of Supranational Organisations e.g. United Nations; International Monetary Fund; World Bank.

Holders of public functions that do not meet the above-referenced standards of seniority, prominence or importance (and are therefore not automatically categorised as PEPs) e.g. middle ranking or more junior officials, could still represent a heightened reputational and/or ML risk and should be assessed on a case by case basis when identifying PEPs, either when establishing or during the course of an ongoing business relationship.

Regulation 2 of the FIAML Regulations 2018 set out the following definition:

"politically exposed person" *or* ***"PEP"*** *means a foreign PEP, a domestic PEP and an international organisation PEP;*

"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;*

"foreign PEP" *means a natural person who is or has been entrusted with prominent public functions by a foreign country, including Heads of State or 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;

"international organisation PEP" *means a person who is or has been entrusted with a prominent function by an international organisation and includes 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 persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;*

"Close associates" *of PEP is an individual who is closely connected to a PEP, either socially or professionally and includes any other person as may be specified by a supervisory authority or regulatory body;*

"family members" *means an individual who is related to a PEP either directly through consanguinity or through marriage or similar civil forms of partnership.*

Business relationships with PEPs pose a greater than normal money laundering risk to the Company, 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. Thus, these types of relationships will be deemed high risk.

In this respect, the Company as enhanced CDD measures with respect to PEP must consider:

a) seeking relevant information from the applicant as well as refer to publicly available information;
b) developing a clear policy on the acceptance of business relationships with PEPs;
c) obtain the approval of senior management prior to establishing relationships with PEPs;
d) where applicants have been accepted and the said applicant or its beneficial owner is subsequently found to be, or subsequently becomes, a PEP, obtain the approval of senior management to continue such business relationships;

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

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

g) conduct enhanced ongoing monitoring of the business relationships involving PEPs, family members or close associates of PEPs.

The Company shall also at all times have in place a PEP Register wherein all clients who are PEP will be recorded. The PEP Register shall be maintained accurately by the Compliance Officer and a template of the PEP Register is provided at ***Annex IV***.

Furthermore, PEPs shall also cease to be considered as such, one year, after they have left the office which qualified them as PEPs and after approval of the Board of Directors of the Company (which shall take other matters incidental thereto when making the determination). Furthermore, as highlighted above, all PEPs, members of their families or associates need senior management approval before acceptance as a client.

Staff members are reminded that failure to comply with this paragraph could lead to reputational risk if clients have been accepted and paid fees, only to have their business turned down and fees refunded by the Compliance Officer prior to makeover.

5.4. Non face-to-face business relationships

The business conducted by the Company may also be conducted on a non face-to-face basis, that is, where there is no face to face contact with the customer or connected person such as the beneficial owner or controllers.

Examples might be where identification information is provided through a trustee or by a legal body about the persons who are connected with a trust, or by a legal body about the persons who are its the beneficial owner and controllers or through identification documents received through electronic means. A further example may be where, although there is face-

to-face contact with a customer, the supporting identification and verification documentation is provided at a time when the customer is not present.

In the above circumstances, the Company must apply appropriate Enhanced CDD measures on a risk-sensitive basis where an applicant for business or customer (or any connected person, such as a beneficial owner or controller) is unable to be identified and when the Company is unsure of the authenticity of the documents in non-face-to-face relationships.

5.5. Connected persons who are PEPs

'Connected person' include underlying principals such as beneficial owners and controllers. Organisations must apply appropriate Enhanced CDD measures on a risk sensitivity basis where an applicant for a business or customer (or any connected person such as beneficial owners or controller) is a PEP and must ensure adequate policies, procedures and controls to comply with this requirement.

Procedures that the Company should comply when dealing with PEP are to:

- develop and document a clear policy on the acceptance of business relationships or one-off transactions with such persons, and ensure this is appropriately documented,
- obtain and document the approval of senior management prior to establish such relationships,
- ensure that Enhanced CDD measures to establish source of wealth and source of funds of such persons, or
- where such persons are discovered to be so only after a relationship has commenced, thoroughly review the relationship and obtain senior management approval for its continuance

5.6. Simplified/Reduced Customer Due Diligence

Section 17C (4) of FIAMLA along with Regulation 11 of the FIAML Regulations 2018 provides that where the risks of money laundering and terrorism financing are low, the Company may conduct simplified due diligence. It additionally mentions that the simplified due diligence shall be commensurate with the lower risk factors and any guidelines issued by the regulator.

Simplified measures can include obtaining less information (e.g., not requiring information on the address or the occupation of the potential client), and/or seeking less robust verification, of the customer's identity and the purpose and intended nature of the business relationship or postponing the verification of the customer's identity.

In any case, where the Company decides to adopt simplified due diligence, Chapter 7 of the FSC AML/CFT Handbook provides that the decision and reasons to adopt simplified due diligence must be documented. Review must also be undertaken to ascertain that it is appropriate to continue applying simplified due diligence.

To note however that simplified due diligence shall not be applicable in cases where:

a) there are grounds for knowing or suspecting that a customer or an applicant for business is engaged in money laundering or terrorism financing;

b) that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in money laundering or terrorist financing; or

c) in specified higher risk categories.

Furthermore, while the legislative framework in Mauritius allows for the application of simplified CDD measures in low risk scenarios, it must be highlighted that the NRA Report 2019 has not identified any low risk sectors. As such, the application of simplified CDD measures does not arise in the current risk environment.

The Company is therefore requested to always assess the prevailing risk environment, and act under the guidance of the FSC in the application of simplified/reduced CDD.

5.7. Third Party Reliance

Pursuant to Section 17D of FIAMLA and Regulation 21 of the FIAML Regulations 2018, the Company may, subject to such terms and conditions as may be prescribed, rely on third parties to perform CDD measures. Furthermore, Section 17D(2) of the FIAMLA also specified that in such circumstances, the ultimate responsibility and accountability of CDD measures shall rest on the Company.

5.7.1. Requirements to have arrangement in writing

The FSC AML/CFT Handbook provides that in case of relying on third parties to complete certain CDD measures, there must be a contractual arrangement in place with the third party. The Company must also ensure that the identification information sought from the third party is adequate and accurate.

Furthermore, the Company needs also to determine the extent and conditions on which it shall rely on an eligible introducer.

The FSC AML/CFT Handbook sets out that the Company should at the time of establishing the introducer relationship, carry out a risk analysis of this relationship and monitor the introducer relationship. The Company is required to establish clear procedures to determine an acceptable level of reliability on the eligible/group introducer.

5.7.2. Reliance for CDD Measures

The Company may rely on third parties to undertake the following CDD measures:

a) Establish and verify the identity of clients using reliable, independent source documents, data or information;

b) Establish and verify the identity of the beneficial owner; and

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

The Company shall however not rely on third parties to identify the source of wealth or source of funds, or to carry out the ongoing monitoring of dealings with a customer. There are certain circumstances where the Company will not be able to rely on third parties to undertake CDD measures or introduce business. These include the following:

a) The client is acting as a nominee, agent or trustee on behalf of undisclosed underlying persons, or

b) The introducer will enter into transactions with the Company on behalf of the client.

c) The third party is based in a high-risk country. (to note that the FSC Handbook provides that high risk countries are not only those identified by the FATF as having strategic deficiencies. A high-risk country can also be those countries that are vulnerable to corruption and which are politically unstable and these examples are not exhaustive).

5.7.3. Conditions for Third Party Reliance

The Company should also establish procedures to be satisfied that:

a) The third party applies CDD measures and keeps records to a standard equivalent to the FATF Recommendations;

b) The third party will provide, immediately upon request, relevant copies of identification data in accordance with Regulation 21(2)(b) of the FIAML Regulations 2018; and

c) The quality of the third party's CDD measures is such that it can be relied upon.

The Company can rely on eligible/group introducers to perform its CDD obligations provided that the following criteria are met:

a) The introducer is regulated for money laundering purposes, or is subject to rules of professional conduct pertaining to money laundering and terrorist financing - evidence of regulation/ supervision must be sought;

b) The introducer has measures in place for compliance with CDD measures and record keeping requirement in line with the exigencies of FIAMLA and the Company must satisfy

itself independently of same;

c) The AML-CFT procedures followed by the introducer are equivalent to the requirements of the FSC;

d) The introducer must provide the Company a completed, signed and dated Eligible Introducer Certificate /Group Introducer Certificate;

e) The introducer maintains identification data and other relevant CDD documentation on the client (including the beneficial owner(s)) and such data will be retained by the introducer and will not be disposed of without the Company's consent;

f) The Company will be given timely access to the CDD documentation kept by the introducer;

g) The Company will be provided with the CDD documents (or certified true copies thereof) kept by the introducer upon request without delay (to note that the FSC recommends that regular assurance testing is carried out to ensure same);

h) The CDD documents kept by the introducer are accurate at the time the Company relies upon them;

i) such data will be promptly transferred to the custody of the Company, if the introducer ceases to act in that capacity.

CHAPTER 6

Transaction and Activity Monitoring

6.1. Introduction

The regular monitoring of a business relationship, including any transactions and other activities carried out as part of that relationship, is one of the most important aspects of effective ongoing CDD measures.

It is therefore important that the Company understands its customer's background and is aware of changes in the circumstances of the customer and beneficial owner through the life cycle of a business relationship. The Company can usually only determine when it might have reasonable grounds for knowing or suspecting that ML/TF is occurring if it has the means of assessing when a transaction or activity falls outside the normal expectations for a particular business relationship.

6.2. The legislative framework

Pursuant to Regulation 3(e) of the FIAML Regulations 2018, the Company is required to conduct ongoing monitoring of all its business relationships. The FIAML Regulations 2018 further provides that ongoing monitoring of business relationships should include:

a) scrutiny of transactions undertaken throughout the course of the business relationship to ensure that the transactions are consistent with his knowledge of the customer and the business and risk profile of the customer; and

b) ensuring that documents data or information collected under the CDD process are kept up to date and relevant by undertaking reviews of existing records, in particular for higher risk categories of customers.

In terms of Regulation 12(2) of the FIAML Regulations 2018, the enhanced CDD measures that may be applied for higher risk business relationships include conducting enhanced monitoring of the business relationship, increasing the number and timing of controls applied, and

selecting patterns of transactions that need further examination.

Regulation 15 of the FIAML Regulations 2018 requires that the Company conduct enhanced ongoing monitoring in addition to performing CDD measures, in relation to a foreign PEP whether as customer or beneficial owner.

Furthermore, Regulation 12 of the FIAML Regulations 2018 sets out that where a financial institution is unable to perform enhanced CDD as required under the FIAML Regulations, it should terminate the business relationship and file a suspicious transaction report in terms of section 14 of the FIAMLA.

6.3. CDD Monitoring

Monitoring procedures should involve a combination of real-time and post-event monitoring. Real-time monitoring focuses on transactions and activity where information or instructions are received before or as the instruction is processed. Post-event monitoring involves periodic, for example monthly, reviews of transactions and activity which have occurred over the preceding period.

The Company should ensure that all documents, data or information collected under the CDD process are kept relevant and up-to-date by undertaking reviews of existing records, using a risk-based approach particularly for higher risk categories of customers or business relationships. This may be achieved by using reliable, independently sourced documents, data or information (this is intended through the use of commercial databases and public information) and ensuring that all material collected under the CDD process is kept relevant and up to date (for example undertaking reactive reviews in response to trigger events, and by undertaking regular planned reviews of existing records at intervals determined by risk rating, with higher risk customers warranting more frequent reviews).

6.4. PEP Relationships

The system of monitoring used by the financial institution must provide for the ability to identify where a customer or beneficial owner becomes a PEP during the course of the business relationship and whether that person is a foreign PEP, domestic PEP or international organisation PEP. This is to be read in conjunction with Paragraph 5.3 of this Manual.

In accordance with Regulation 15(1) (b) of FIAML Regulations 2018, where a customer or beneficial owner becomes a foreign PEP during the course of an existing business relationship, as part of the Enhanced CDD measures subsequently applied the Company shall obtain senior management approval to continue that relationship.

The same requirement applies in cases when there is higher risk business relationship with a domestic PEP or an international organisation PEP.

The Company should be aware that it is possible that family members and/or associates may not inform the Company or even be aware of their PEP status. Therefore, it is important that independent screening and monitoring should be conducted.

It is also possible that an individual's PEP status may change during the business relationship. It is therefore important that ongoing monitoring exists in order to identify changes of status and risk classification.

6.5. High Risk Transaction or Activity

When conducting ongoing monitoring, the below extracts are example of red flags which may indicate high risk transactions or activity within a business relationship:

a) Unusual transactions in the context of the client activities (abnormal size or frequency or party recipient of the funds),

b) Funds originating or destined for an unusual location either specific to an individual business relationship or product type,

c) transactions or activity unexpectedly occurring after a period of dormancy,

d) unusual patterns of transactions or activity which have no apparent economic or lawful purpose,

e) an instruction to effect payments for advisory or consulting activities with no apparent connection to the known activities of the customer or their business,

f) the involvement of charitable or political donations or sponsorship, or

g) a relevant connection with a country or territory that has significant levels of corruption, or provides funding or support for terrorist activities.

6.6. Transactions Monitoring

Regulation 3(e) of the FIAML Regulations 2018 sets out that a financial institution must understand and obtain adequate and relevant information on the purpose and intended nature of a business relationship or occasional transaction in order to be in a position to detect and subsequently report suspicious activity, if any.

To monitor ongoing transactions, supporting documents relating to transactions (transactional records) undertaken for or by a client shall be kept on records for on-going monitoring purposes. The transactional records to be maintained are as per the CDD/Enhanced CDD carried for the customer. All documents, data or information collected under the CDD processes should be kept up to date.

In all cases, sufficient information shall be recorded to enable the reconstruction of a transaction. Transactional documents/data, including identity and verification information shall be kept for the duration of the business relationship and a period of seven years after the relationship has ended.

The Company should have a monitoring process which analyses transactions with respect to its size, activities and complexity together with the assessment of risks within the acceptable risk profile.

The Company should adapt the parameters of its processes, in particular the extent and frequency of monitoring on the basis of materiality and risk including high risk relationships. The Company should:

a) understand how the systems works and how to use the system,

b) understand the system coverage such as activities covered, and parties being monitored,

c) understand the sources of data, and

d) set clear procedures for dealing with potential matches based on risk profile.

Factors such as a person's intuition; direct contact with a customer either face-to-face or on the telephone; and the ability, through practical experience, to recognise transactions and activities which do not seem to have a lawful or economic purpose, or make sense for a particular customer, cannot be automated.

Particular attention should be paid to high risk relationships (for example, those involving PEPs), high risk countries and territories and high risk transactions. In this regard, as a minimum, and in line with the provisions of the FSC AML/CFT Handbook, periodic client reviews may be performed in accordance with the following time periods:

- **Very high/high risk:** on a six months basis;
- **Medium risk:** within one (1) years; and
- **Low risk:** within two (2) years.

Moreover, the Company should also scrutinise complex transactions - all those transactions which are complex, unusual large transactions and all unusual patterns of transactions, especially those which appear to have no economic or visible lawful purpose, or those not consistent with the customer's normal and expected transactions as per business plan or normal practice. Certain types of transactions should alert the Company to the possibility that the customer is conducting complex, unusual or suspicious activities. Therefore, in addition,

the following areas should also be monitored:

a) the nature and type of the transaction (transactions that do not appear to make economic or commercial sense);

b) the frequency and nature of a series or pattern of transactions (transactions that involve small cash deposits made frequently or transactions that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer);

c) the amount of any transactions, paying particular attention to particularly large transactions (very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account);

d) the geographical origin/destination of a transaction (jurisdictions that pose a higher risk to their particular sector or customer type;

e) the parties concerned with a view to ensuring that there are no payments to or from a person on a sanctions list or relating to any restricted activities;

f) transactions made by customers which pose higher money laundering and terrorism financing risks, such as High Net Worth Individuals, PEPs, cash intensive businesses, amongst others.

Where the basis of the business relationship changes significantly, the Company is required to undertake a new assessment to reassess the customer's risk profile to ensure that the revised risk and basis of the relationship is fully understood, this could include further CDD procedures where necessary.

6.7. Oversight of Monitoring Process by the Compliance Officer

The Compliance Officer should have access to, and familiarise himself/herself with, the results and output from the Company's monitoring processes.

Output from the monitoring processes should be reviewed by the Compliance Officer who in turn should report regularly to the Board, providing relevant management information such as statistics and key performance indicators, together with details of any trends and actions taken where concerns or discrepancies have been identified.

The Board should consider the appropriateness and effectiveness of the Company's monitoring processes as part of its annual review of the Company's business risk assessments and associated policies, procedures and controls. This should include consideration of the extent and frequency of such monitoring, based on materiality and risk as set out in the business risk assessments.

Where the Company identifies weaknesses within its monitoring arrangements, it should ensure that these are rectified in a timely manner.

CHAPTER 7

Reporting of Suspicious Transaction

7.1. Introduction

A fundamental element of an effective system to combat ML/TF/PF is the requirement that financial institutions should identify and file suspicious transaction reports (STRs) with their national financial intelligence unit.

Section 2 of the FIAMLA defines a 'suspicious transaction' as a transaction which –

a) gives rise to a reasonable suspicious that it may involve –

   (i) the laundering of money or the proceeds of any crime; or

   (ii) funds linked or related to, or to be used for, terrorism or acts of terrorism or by proscribed organisations whether or not the funds represent the proceeds of a crime;

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

c) appears to have no economic justification or lawful objective;

d) is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or

e) gives rise to suspicion for any reason.

For the purpose of the definition of a suspicious transaction, the Company should also note that a transaction would also include a proposed or attempted transaction.

The Company is therefore required to report suspicious transactions to the FIU. In this respect, the Company is required to stand guided by the Guidance Note issued by the FIU pursuant to section 10(2)(c) of the FIAMLA. The Guidance Note is intended to assist and guide financial institutions in completing the STR form issued by the FIU.

Section 14 of the FIAMLA stipulates that every financial institution should, as soon as practicable but not later than 5 working days from the day on which it becomes aware of a transaction which it has reason to believe may be a suspicious transaction, make a report to

the FIU of such transaction.

Section 16(1) of the FIAMLA further requires the Company and its officers not to disclose to any person that a STR is being or has been filed, or that related information is being or has been requested by, furnished or submitted to the FIU.

7.2. Unusual Activity and Potential Red Flags

Regulation 28(2) of the FIAML Regulations 2018 requires the Company to conduct 'appropriate scrutiny' of any unusual activity and to obtain Enhanced CDD.

The activity should be looked at in detail in conjunction with additional information such as the customer's CDD, expected activity, an explanation of the activity from the customer, supporting documentary evidence or information from independent data sources. CDD provides the basis for recognising unusual activity therefore it is imperative that CDD is satisfactory on all customers and that business relationships are monitored appropriately.

Paragraph 10.5 of the FSC AML/CFT Handbook sets out the list of Potential Red Flags as applicable to the Company.

In this regard, the list below illustrates a series of transactions which could be possible signs of ML and TF (Suspicious transactions) that the Company should be mindful when dealing with a business relationship:

a) The deposit or withdrawal of unusually large amounts of cash from an account,

b) Unwillingness to provide CDD documentation on beneficial owners/ controllers,

c) Deposits or withdrawals at a frequency that is inconsistent with the Company's understanding of that customer and their circumstances,

d) Transactions involving the unexplained movement of funds, either as cash or wire transfers,

e) Payments received from, or requests to make payments to, unknown or un-associated third parties,

f) Personal and business-related money flows that are difficult to distinguish from each

other,

g) Financial activity which is inconsistent with the legitimate or expected activity of the customer,

h) An account or business relationship becomes active after a period of dormancy,

i) The customer is unable or reluctant to provide details or credible explanations for establishing a business relationship, opening an account or conducting a transaction,

j) The customer holds multiple accounts for no apparent commercial or other reason,

k) Bank drafts cashed in for foreign currency,

l) Funds transferred to a charity or NPO with suspected links to a terrorist organisation,

m) Large amounts of cash from unexplained sources,

The above list is non-exhaustive. However, there may be legitimate reasons why a customer has acted in the manner identified, and the Company is expected to know the reasons why and document same where so required.

7.3. Terminating a business relationship

Regulation 12(3) of the FIAML Regulations 2018 provides that where a reporting person is unable to perform enhanced CDD where required under these regulations, he shall terminate the business relationship and shall file a suspicious transaction report under section 14 of the FIAMLA.

According to Regulation 28(2) of the FIAML Regulations 2018, where the Company identifies any unusual activity in the course of a business relationship or occasional transaction the Company must:

a) perform appropriate scrutiny of the activity;

b) obtain Enhanced CDD only if this will not tip off the client; and

c) consider whether to make an internal disclosure in accordance with the reporting procedures established under Regulation 27 of the FIAML Regulations 2018.

The Company should consider the evidence and documentation identified to decide whether to terminate a business relationship where in cannot perform Enhanced CDD and comply with the FIAML Regulations 2018 when:

a) It becomes apparent that elements of their criminal activity are known to the Company.

b) When the Company fails to gather Enhanced CDD despite several interactions with the clients.

7.4. Role of the MLRO/DMLRO

The MLRO shall be the main point of contact of the Company with the FIU. The officers and employees of the Company are strictly prohibited from disclosing to any person information or any other matter which is likely to prejudice an investigation on a suspicious transaction.

In this context, the MLRO shall report to the Board of Directors on an annual basis on:

a) The number of internal suspicious transaction/activity reports made by employees of the Company,

b) The number of STRs made to the FIU,

c) Breaches to AML-CFT measures,

d) The adequacy or shortcomings of the AML-CFT measures, and

e) Recommendations to remedy any shortcomings identified,

For the purposes of the reporting of suspicious transactions, the MLRO shall keep the following records on the suspicious reports being received and filed:

a) internal suspicious transactions reports received by the MLRO;

b) records of actions taken following receipt of internal suspicious transactions reports;

c) records of actions taken to assess whether the transactions reported are suspicious or not;

d) records of the information that was examined to assess whether the transactions reported are suspicious or not; and

e) where after examination the MLRO decided not to make a STR to the FIU, a record of the reason for the decision not to make a report to the FIU.

The MLRO and DMLRO are also required to be registered with the FIU for the purposes of raising STRs thereto.

For avoidance of doubt, the DMLRO is required to perform the above MLRO functions in the absence of the MLRO.

7.5. Internal disclosure of suspicious transactions

Where suspicious activity is identified, staff members are required to make an internal disclosure to the MLRO in accordance with Regulation 28(1) of the FIAML Regulations 2018.

Also, it is the responsibility of the MLRO (or if appropriate, the DMLRO) to consider all internal disclosures he/she receives in the light of full access to all relevant documentation. Thus, where an internal suspicious transaction/activity report is made to the MLRO or the DMLRO, he/she shall be given access to all the relevant information/documentation or records to assess whether the transaction/ activity is suspicious or not. The MLRO shall assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to money laundering, terrorist financing or proliferation financing.

The MLRO shall acknowledge receipt of the internal disclosure and at the same time, provide a reminder to the relevant staff members of the obligation to do nothing that might prejudice enquiries, such as tipping off the Client or any third party. Staff members are reminded that all disclosure reports must reach the MLRO without any undue delay. All relevant persons must ensure that the MLRO receives full cooperation from all staff and full access to all relevant documentation so that he/she is in a position to decide whether there are reasonable grounds to suspect money laundering or terrorist financing. The predicate offence need not be known or suspected, reasonable grounds to suspect should suffice.

Reporting lines should be as short as possible with the minimum number of people between

the employee with suspicion and the MLRO/DMLRO.

The MLRO shall forthwith file an STR report where he knows or has reason to believe that an internal disclosure may be suspicious. The MLRO shall make an external disclosure as soon as practicable but not later than 5 working days from the day on which it becomes aware of a transaction if the MLRO knows (as per paragraph 7.6 below); or has reasonable grounds to believe, that an internal disclosure may be suspicious.

Failure by the MLRO to diligently consider all relevant material may lead to vital information being overlooked and the suspicious transaction or activity not being externally disclosed to the. As a result, the MLRO must document internal disclosures made by employees to record the results of the assessment of each disclosure. The evaluation process should be fully documented. A template of the internal disclosure register is provided at ***Annex V***.

In order to ease the above requirement, the Company must ensure that all employees are made aware of the identity of the MLRO/DMLRO, and the procedures to follow when making an internal disclosure report to the MLRO/DMLRO.

7.6. External Disclosures to the FIU

Regulation 29(1) of the FIAML Regulations 2018 requires that, where an internal disclosure has been made, the MLRO shall access the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to money laundering, terrorism financing or proliferation financing.

Furthermore, Regulation 29(2) of the FIAML Regulations 2018 and Section 14 of the FIAMLA requires the MLRO to make an external disclosure as soon as practicable but not later than 5 working days from the day on which it becomes aware of a transaction if the MLRO knows, or has reasonable grounds to believe that an internal disclosure may be suspicious. The Company is also required to keep a STR log wherein all STR filed by the Company and the relevant details shall be recorded. A template of the STR register is provided at ***Annex VI***.

Section 15 of the FIAMLA provides that all STRs are to be raised with the FIU. The STR shall be in the form prescribed and approved by the FIU under Section1 5(2) of the FIAMLA and shall include:

a) the identification of the party or parties to the transaction;
b) the amount of the transaction, the description of the nature of the transaction and all the circumstances giving rise to the suspicion;
c) the business relationship of the suspect with the Company;
d) where the suspect is an insider, any information as to whether the suspect is still affiliated with the Company;
e) any voluntary statement as to the origin, source or destination of the proceeds;
f) the impact of the suspicious activity on the financial soundness of the Company; and
g) the names of all the officers, employees or agents of the Company dealing with the transaction.

7.7. Register of Reports

Pursuant to Regulation 30 of the FIAML Regulations 2018, the Company is required to establish and maintain separate registers of all internal disclosures and all external disclosures. The register must include details of the date the report was made, the person who made the report, whether the report was made to the MLRO or DMLRO and information to allow the papers and relevant documentation to be located.

A template of the registers is provided in Annex of this Manual which may be used by the Company.

The Company should however ensure that the name of the Customer who is subject to the STR is not listed in the register to ensure confidentiality of the report.

CHAPTER 8

Employee Screening and Training

8.1. Introduction

One of the most important tools available to the Company, to assist in the prevention and detection of financial crime, is to have appropriately screened employees who are alert to the potential risks of ML and TF and who are well trained with respect to the CDD requirements and the identification of unusual activity, which may prove to be suspicious.

The effective application of even the best designed systems, policies, procedures and controls can be quickly compromised if employees lack competence or probity, are unaware of, or fail to apply, the appropriate policies, procedures and controls or are not adequately trained. Regulation 22(1)(b) of the FIAML Regulations 2018 requires the Company to implement programmes for screening procedures so that high standards are maintained when hiring employees.

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

(i) assist them in recognising 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 sub subparagraph (i).

8.2. Board Oversight for Screening and Training

The Board oversight and responsibilities are detailed at Paragraph 3.2 of this Manual. In conjunction thereto, the Board of the Company is required to be aware of the obligations of the Company in relation to employee screening and training.

The Company must ensure that training provided to employees is comprehensive and ongoing and that the officers and employees are aware of ML and TF, the associated risks and vulnerabilities of the Company, and their corresponding obligations. The Company is also required to establish and maintain mechanisms to measure the effectiveness of the AML and CFT training provided to relevant employees and on a risk-based approach.

To measure the effectiveness of AML and CFT training, the Company could also consider it appropriate to incorporate an exam or some form of assessment into its on-going training programme, either as part of the periodic training provided to employees or during the intervening period between training.

Regardless of the methods utilised, the board should ensure that it is provided with adequate information on a sufficiently regular basis to satisfy itself that the Company's employees are suitably trained to fulfil their personal and corporate responsibilities.

8.3. Screening Requirements

Pursuant to Paragraph 12.4 of the FSC AML/CFT Handbook, the Company shall, at the time of recruitment of employees, ensure that appropriate screening measures are applied to ensure that the employees are of the required standard of competence, including the following:

a) obtaining and confirming details of employment history, qualifications and professional memberships;

b) obtaining and confirming appropriate references;

c) obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective employee;

d) obtaining and confirming details of any criminal convictions, including the provision of a

check of the prospective employee's criminal record; and

e) screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

The Company is also required to carry out periodic ongoing screening of its employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

8.4. Training of employees

Regulation 22(1)(c) of FIAML Regulations 2018 states that an ongoing training programme for its directors, officers and employees to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to -

a) assist them in recognising transactions and actions that may be linked to money laundering or terrorism financing; and

b) instruct them in the procedures to be followed where any links have been identified.

In this context, the Company should ensure that all of its employees are well trained with respect to anti-money laundering and combatting terrorist financing requirements, CDD requirements, and the identification of unusual activity which may prove to be suspicious and their corresponding obligations.

The Company should therefore take appropriate measures to make its directors, officers and employees aware of:

a) an understanding of ML/TF risk related to clients, products, services, delivery channels and geography, how the monitoring of these risks should occur and what mitigation measures should be applied when these risks are identified.

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

c) the legal requirements contained in the relevant legislations, namely FIAMLA, the Prevention of Corruption Act 2002, the Prevention of Terrorism Act 2002, the Convention for the Suppression of the Financing of Terrorism Act 2003, and the UN Sanctions Act and Regulations, guidelines and instructions made thereunder,

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

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

f) the procedures to follow when working with law enforcement or the FIU on an investigation,

g) the completion of unusual and suspicious transaction reports; Treatment of incomplete or declined transactions.

The Company shall also devise and maintain regular schedule of new and refresher programmes, appropriate to their risk profile, for the different types of training required by new employees, agents, board/senior management and MLRO/Compliance employees. Training is to be provided at least once every year.

The Compliance Officer is required to receive in depth training on all aspects of the prevention and detection of ML/TF to be able to assume his/her functions accordingly. Thus, the trainings must include, but not be limited to, addressing the monitoring and testing of compliance systems and controls (including details of the Company's policies and procedures) in place to prevent and detect of money laundering and terrorist financing.

8.4.1. Training for the MLRO/DMLRO

There is a specific requirement for MLRO and DMLRO to have ongoing professional development, including participating in professional associations and conferences in line with the competency standards set out by the FSC.

Given that MLROs and DMLROs have significant responsibility handling and where appropriate external reporting of suspicious transactions to the FIU, they must be given additional training to comprehensively cover amongst others the following:

a) the recognition and handling of suspicious transactions;

b) liaising with law enforcement agencies; and

c) the management of the risk of tipping off.

Paragraph 12.8.2 of the FSC AML/CFT Handbook lists down the aspects on which the MLRO/ DMLRO should receive training, which are as follows:

a) AML/CFT legislative and regulatory requirements;
b) the international standards and requirements on which the Mauritius' strategy is based, namely the FATF 40 Recommendations and ML/TF typology reports that are relevant to their business;
c) the identification and management of ML/TF risk;
d) the design and implementation of internal systems of AML/CFT control;
e) the design and implementation of AML/CFT compliance testing and monitoring programs;
f) the identification and handling of suspicious activity and arrangements and suspicious attempted activity and arrangements;
g) the money laundering and terrorist financing vulnerabilities of relevant services and products;
h) the handling and validation of internal disclosures;
i) the process of submitting an external disclosure;

j) liaising with law enforcement agencies;

k) money laundering and terrorist financing trends and typologies; and

l) managing the risk of tipping off.

8.5. Contents of Training

In terms of Paragraph 12.7 of the FSC AML/CFT Handbook, the Company must ensure that the ongoing training provided to directors, officers and employees covers, to a minimum:

a) the requirements for the internal and external disclosing of suspicion;

b) the criminal and regulatory sanctions in place, both in respect of the liability of the Company and personal liability for individuals, for failing to report information in accordance with the policies, procedures and controls of the Company;

c) the identity and responsibilities of the MLRO, Compliance Officer and DMLRO;

d) dealing with business relationships or occasional transactions subject to an internal disclosure, including managing the risk of tipping off and handling questions from customers;

e) those aspects of the Company's business deemed to pose the greatest Money laundering and terrorist financing risks, together with the principal vulnerabilities of the products and services offered by the Company, including any new products, services or delivery channels and any technological developments;

f) new developments in Money laundering and terrorist financing, including information on current techniques, methods, trends and typologies;

g) the Company's policies, procedures and controls surrounding risk and risk awareness, particularly in relation to the application of CDD measures and the management of high risk and existing business relationships;

h) the identification and examination of unusual transactions or activity outside of that expected for a customer;

i) the nature of terrorism funding and terrorist activity in order that employees are alert to

transactions or activity that might be terrorist-related;

j) the vulnerabilities of the Company to financial misuse by PEPs, including the effective identification of PEPs and the understanding, assessing and handling of the potential risks associated with PEPs; and

k) potential risks associated with PEPs; and UN, EU and other sanctions and the Company's controls to identify and handle natural persons, legal persons and other entities subject to sanction.

8.6. Training Records

The Company shall also maintain a record of all anti-money laundering training delivered to its employees in the form of a Training Log (template of which is provided in ***Annex VII***).

This acts as evidence of sufficient training and prevents any employee from claiming that an absence of suspicion is attributable to failure by the Company to make adequate training provision. Such records shall include:

a) Details of the content of the training programmes provided,

b) The names of employees who have received the training,

c) The date on which the training was delivered,

d) The mode of the training (face to face, or online),

e) The results of any testing carried out to measure employees understanding of the AML/CFT requirements, and

f) An on-going training plan.

Records of any AML/CFT training shall be kept for at least 7 years.

Furthermore, the Company should also obtain an acknowledgement from each employees on the training received, to assess the effectiveness thereof and elaborate on further training and a reaffirmed acknowledgement of this AML/CFT Manual.

CHAPTER 9

Record Keeping

9.1. Introduction

Record keeping is an essential component of the combat against ML/TF in the sense that an audit trail is required. In this sense, the Company is required to play an important role in ML/TF investigation by providing the relevant records particularly where a complex web of transactions specifically for the purpose of confusing the audit trail has been used.

The records at the Company are primarily kept in hard copies, but the Company may also implement an integrated computerised system, which replicates the records kept in hard copies. In any case, where there are copies kept on the Company's computerised system should be seen as a complement to the physical files and not as a replacement.

Pursuant to Section 17F of the FIAMLA, the Company is required to maintain, and keep for the specified period, all books and records with respect to his customers and transactions as set out hereunder:

a) all records obtained through CDD measures, including account files, business correspondence and copies of all documents evidencing the identity of customers and beneficial owners, and records and the results of any analysis undertaken in accordance with the FIAMLA, all of which shall be maintained for a period of not less than 7 years after the business relationship has ended;

b) records on transactions, both domestic and international, that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders, which shall be maintained for a period of 7 years after the completion of the transaction; and

c) copies of all suspicious transaction reports made pursuant to section 14 of the FIAMLA or other reports made to FIU in accordance with that Act, including any accompanying

documentation, which shall be maintained for a period of at least 7 years from the date the report was made.

Regulation 6(2) of the FIAML Regulations 2018 requires the Company to keep records of actions taken to verify the identity of the beneficial owner of their customers which are legal persons pursuant to Regulation 6(1), as well as any difficulties encountered during the verification process.

In addition, pursuant to Regulation 14 of the FIAML Regulations 2018, the Company must keep and maintain all necessary records relating to transactions in such a form which enables the prompt reconstruction of each individual transaction.

In line with section 29 of the FSA 2007, the Company must keep and maintain internal records of the identity of each of its customers and records pertaining to the clients' business activities (which shall include accounts files and business correspondence) which should be in the English or French language.

Furthermore, the Company must keep on record these documents for a period of at least 7 years after the completion of the transaction to which it relates. The records maintained may prove to be very valuable where the Company suspects an applicant for business or where there is an investigation into the conduct of an applicant for business (whether in Mauritius or elsewhere).

9.2. Records to be kept by the Company

The Company must maintain all books and records with respect to his customers and transactions.

Where the records are being held electronically, the Company should ensure that the working documents should be legible and in a usable filing system, so that they can be retrieved/found without undue delay and produced on a timely basis especially where the originals are not to be retained.

All CDD documentation required by the Company to identify and verify the identity of customers and of beneficial owners in accordance with applicable laws and regulations and this Manual must be retained for a period of not less than 7 years after the completion of the transaction to which it relates, closure of the account or cessation of the business relationship with the customer concerned.

Likewise, records of the measures taken to verify the identity of beneficial owners as well as any difficulties encountered during the verification process should be properly documented and retained for a similar period.

Transaction records in whatever form they were used need also be maintained for a period of not less than 7 years after the completion of the transactions concerned, in such a manner to enable competent authorities to compile a satisfactory audit trail for suspected laundered and terrorist money and establish a financial profile of any suspect account.

Records of all internal reports made to the MLRO and all reports made by the MLRO to the FIU should be retained for a period of not less than 7 years after the date on which the report was made. In addition, any analysis or findings relating to the background and purpose of complex, unusual or suspicious transactions should also be retained for a period of not less than 7 years after the date on which the finding was made. Similarly, any determination on internal disclosures should also be retained.

Records of a suspicious transaction made under section1 4 of the FIAMLA, including any accompanying documentation should be maintained for a period of at least 7 years from the date the report was made.

9.3. Records relating to ongoing Investigations

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

ANNEX I

AML/CFT POLICY REVIEW LOG

Mercato Brokers AML/CFT Policy Review Log			
Name of Compliance Officer	*Date of last review*	*Relevant sections that have been amended*	*Date on which changes were disseminated to the staff*

ANNEX II

ACKNOWLEDGEMENT FORM FOR AML/CFT MANUAL

I, ……..……., hereby acknowledge that I have read, understood, and will adhere to the rules, codes, and regulations laid down in the Company's AML/CFT Manual.

The fundamental elements contained within the AML/CFT Manual are listed below:

I. Legal obligations to be compliant with the Financial Intelligence and Anti-Money Laundering Act 2002 and regulations made thereunder, the Financial Services Commission AML/CFT Handbook, and other relevant Anti-Money laundering and Combatting Terrorist Financing obligations prevailing in Mauritius,
II. The identity of Compliance Officer, Money Laundering Reporting Officer and Deputy Money Laundering Reporting Officer,
III. Customer Due Diligence and Know Your Client measures,
IV. Suspicious transaction and the handling thereof,
V. The importance of Reporting, and
VI. Record Keeping requirements.

Additionally, I understand that it is my responsibility to act when I become suspicious of a particular transaction. I must follow the procedure laid down in the AML/CFT Manual to report a suspicious transaction.

…….. **……..**
Signature **Date**

ANNEX III

AML/CFT POLICY REVIEW LOG

Mercato Brokers Beneficial Owner Register			
Date	*Client Name*	*Name of Beneficial Owner*	*Any other information*

ANNEX IV

POLITICALLY EXPOSED PERSONS (PEP) REGISTER

Mercato Brokers Politically Exposed Persons (PEP) Register						
Date	*Client Name*	*Name of PEP*	*Relationship of PEP with Client*	*PEP Nature*	*Enhanced Due Diligence Measures*	*Board of Directors/ Senior Management Approval (Yes/No)*

ANNEX V

Register of Internal Disclosure Reports on Money Laundering and Financing of Terrorism made to the MLRO or DMLRO

Mercato Brokers Beneficial Owner Register				
Date on which the report is made	*Person who made the report*	*Whether the report is made to the MLRO or the DMLRO*	*Information sufficient to identify the relevant papers to the suspicion*	*Action taken regarding the internal disclosure*

ANNEX VI

Register of External Disclosures on Money Laundering and Financing of Terrorism made to the FIU (STR Register)

Mercato Brokers STR Register				
Date on which the report is made	*Person who made the report*	*Information sufficient to identify the relevant papers for the reporting*	*Reference number allocated by the FIU after submission of STR*	*Any feedback received/additional request from the FIU*

ANNEX VII

TRAINING LOG

Mercato Brokers Training Log						
Date	*Name of employee*	*Position*	*Training attended*	*Number of hours*	*CPD Points (if applicable)*	*Other comments*