AXIORY

ANTI-MONEY LAUNDERING & COMBATING THE FINANCING OF TERRORISM POLICY

(Last updated on: 09 November 2021)

AXIORY

Table of Contents

PART A. LEGISLATIVE AND REGULATORY BACKGROUND

1. WHAT IS MONEY LAUNDERING?

The Anti-Money Laundering regulations require a fundamental understanding of the processes that can be involved in money laundering, and require that you respond appropriately to any knowledge or suspicions that these processes may be taking place. This section of the AML & CFT Policy (hereinafter the "Policy") explains what money laundering is, the offences and the penalties.

The main objective of money laundering is to exchange the initial proceeds of an illegal activity with a financial asset or other valuables to give legitimacy to such proceeds and to conceal the true source of the funds.

Simply put, money laundering is any process whereby funds derived from criminal activity, including terrorist financing, are given the appearance of being legitimate by being exchanged for "clean" money. Participating in the handling of such funds is illegal, and it can also be illegal to become involved with them "indirectly" through knowledge or suspicion.

The wider definition of money laundering and activities controlled by the statutory framework was introduced in the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017[1]; where money laundering was defined as:

- concealing, disguising, converting, transferring or removing criminal property;
- entering into or becoming concerned in an arrangement which a person knows or suspects facilitates the acquisition, retention, use or control of criminal property;
- acquiring criminal property, using criminal property; or possession of criminal property.

The process of money laundering can be divided into three sequential stages:

(1) *Placement*. At this stage funds are converted into financial instruments, such as checks, bank accounts, and money transfers, or can be used for purchasing high-value goods that can be resold. They can also be physically deposited into banks and non-bank institutions (e.g., currency exchangers). To avoid suspicion by a company, the launderer may as well make several deposits instead of depositing the whole sum at once, this form of placement is called smurfing.

(2) *Layering*. Funds are transferred or moved to other accounts and other financial instruments. It is performed to disguise the origin and disrupt the indication of the entity that made the multiple financial transactions. Moving funds around and changing in their form makes it complicated to trace the money being laundered.

(3) *Integration*. Funds get back into circulation as legitimate to purchase goods and services.

2. LEGISLATIVE REFERENCES

[1] UK government's formal guidance on rules on anti-money laundering, which implements the provisions of EU's 4th Directive on Money Laundering.

As a legal entity regulated in Mauritius, Tradit Ltd (hereinafter the "Company") is required to comply with local regulations.

Mauritius brought a number of amendments to its AML/CFT framework through the Finance (Miscellaneous Provisions) Act 2018, Act 11 of 2018, which was gazetted on 9 August 2018 in Government Gazette 71 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:

(a) enhancing the existing legal framework for preventive measures that apply to financial institutions and Designated Non-Financial Businesses and Professions ("DNFBPs");
(b) extending the scope of the Financial Intelligence and Anti-Money Laundering Act ("FIAMLA") to include proliferation financing;
(c) establishing a legal framework to support the National Risk Assessment exercise;
(d) 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 Financial Intelligence and Anti-Money Laundering Regulations ("FIAML Regulations 2018") were promulgated on 28 September 2018 and became effective on 01 October 2018. The FIAML Regulations 2018 revoked the Financial Intelligence and Anti-Money Laundering Regulations 2003 and address, inter alia, the following FATF requirements:

(a) Customer due diligence;
(b) Politically exposed persons;
(c) Correspondent banking;
(d) Money or value transfer services;
(e) New technologies;
(f) Wire transfers;
(g) Reliance on third parties; and
(h) Internal control and foreign branches and subsidiaries.

On 21 May 2019, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 and the Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019 were enacted and both acts came into operation on the 29 May 2019.

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019enables Mauritius to implement the measures under all the United Nations Security Council Resolutions and deal with other matters of international concern, and to give effect to Article 41 of the Charter of the United Nations.

3. REGULATORY REFERENCES

The requirements to prevent and detect money laundering and to counter terrorist financing arise from the FIAMLA and the FIAML Regulations 2018.

4. INDUSTRY GUIDANCE

The AML and CFT regulatory requirements are largely pulled together by a set of industry guidance notes, provisions of which the Company aims to incorporate into its policies, procedures, and day-to-day operations.

The Company is adhering to the following guidance documents:

(1) UK Financial Conduct Authority (FCA);
- FCA's Financial Crime: a guide for firms, Parts I & II, 2016
- FCA's Systems and Controls (SYSC) Rules that require senior management to establish appropriate procedures and controls to implement the requirements of the Money Laundering, Terrorist Financing and Transfer of Funds Regulations (MLR), and to manage the risks of the Company's products and services being used for purposes of financial crime;

(2) Joint Money Laundering Steering Group (JMLSG) Guidance for the UK Financial Sector Parts I, II, and III, 2017

(3) Financial Action Task Force (FATF) Recommendations that are recognised as the international standard for combating money laundering and the financing of terrorism and proliferation of weapons of mass destruction.

5. OFFENCES, PENALTIES AND DEFENCES

5.1. Offences and Penalties

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.
(3) Sections 150, 151 and Part X of the Criminal Procedure Act and the Probation of Offenders Act shall not apply to a conviction under this Part.

Section 16(3) (A) of FIAMLA states:

Legal consequences of reporting

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 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 FIAMLA states:

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

(1) Any bank, cash dealer, financial institution or member of a relevant profession or occupation or any director, employee, agent or other legal representative thereof, who, knowingly or without reasonable excuse –
    (a) fails to –
        i. supply any any information requested by the FIU under section 13(2) or 13(3) within the date specified in the request;
        ii. make a report under section 14; or

iii. any person who fails to comply with sections 17 to 17G shall commit an offence and shall, on conviction, be liable to a fine not exceeding 10 million rupees and to imprisonment for a term not exceeding 5 years.

(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 of FIAMLA states:

Duty to provide information

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:

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.

5.2. Defences

There are certain defences available for some of the offences listed above. The main defence relevant to the Company's employees is the defence of having made an 'authorized disclosure', which is a disclosure made:

- before an offence is committed;
- while it is being committed but an employee started the act at a time when, because they did not know or suspect that the property constituted or represented a person's benefit from criminal conduct, the act was not an offence, and the disclosure is made on the employee's own initiative and as soon as practicable to make it;
- after the offence was committed, but there is a good reason for the employee's failure to make the disclosure before the act was done, and the disclosure is made on the employee's own initiative and as soon as it is practicable to make it.

If an employee makes a disclosure to the MLCO in accordance with the Procedure for Internal Suspicious Activity Reporting as specified in the AML & CFT Procedures Manual, then that disclosure will be sufficient for the employee to rely on this defence, provided a disclosure is made before any offence has been committed. This is why it is so important for all employees to read this Policy carefully, comply with its requirements and act quickly.

The MLCO will then decide whether to report the suspicion to the Financial Intelligence Unit (FIU). Where a suspicion is reported, if the MLCO does not receive a "refusal to proceed" from the FIU within a 7-day period then the employee can proceed with that transaction. Where a "refusal to proceed" is received there is a further period of 30 days for the FIU to follow up their refusal with further instructions. If no further information is received within 31 days, the employee can proceed with the transaction.

If the MLCO submits suspicious activity report to the FIU, an employee must discuss with the MLCO what information can be given to the client, so that this does not result in an offence of tipping off.

6. SANCTIONS REGIME

There is a separate but related sanctions regime that imposes restrictions on the Company's ability to do business with those persons and entities on UN and European Union sanctions lists. Some entries on the lists are specific to a particular person or entity and others are general financial sanctions on all persons and entities in a particular jurisdiction. Screening of all clients against sanctions lists in World-Check[2] is an integral part of the Company's KYC and Client Due Diligence procedures, and is done, both, when accepting an application from a new client, and, regularly during the business relationship with the client. The Company's Client Acceptance Policy (CAP) stipulates that application from a client, where they are identified as true match on the sanctions list during the KYC procedure, shall be rejected and no business activity shall be initiated.

PART B. OVERVIEW AND POLICY FRAMEWORK

7. INTRODUCTION

It is of critical importance for the Company's integrity and reputation, to be able to identify, report, and take precautions to guard against money laundering and financing of terrorism. The nature of the Company's business requires it to abide by anti-money laundering (AML) and countering the financing of terrorism (CFT) legislation and regulation that apply to the trading activities. In addition, the Company may be particularly attractive to individuals seeking to clean-up money due to non-face-to-face nature of the services.

In order to prevent the criminals from using the Company's products and services for laundering the proceeds of crime, it is required to establish appropriate and proportionate to

[2] World-Check is a database and a tool that is used by financial institutions globally, to efficiently screen clients, associates, transactions and employees for potential risk. The Database covers politically exposed persons, persons on sanction lists and other potentially high-risk individuals worldwide.

the level of risk, systems and controls, and ensure their effective implementation. Therefore, this Policy is designed to ensure that the Company has a defined and approved by senior management overarching framework to comply with all applicable anti-money laundering and countering the financing of terrorism legislation and regulations.

The Policy is supplemented by AML & CFT Procedures Manual and other Associated Policies and Procedures, full list of which can be found in Appendix 1 to this Policy, designed to ensure AML & CFT compliance during the day-to-day operations of the Company.

8. PURPOSE AND SCOPE

The principal objectives of this Policy are to:

- prevent the Company from being used by money launderers to further their illicit business;
- define a framework to enable the Company to assist law enforcement agencies in identifying and tracking down money launderers and their criminal property;
- ensure that the Company remains compliant with all relevant AML, CFT and sanctions legislation and regulations;
- inform all relevant employees about the obligations of the Company and their obligations in relation to complying with AML and CFT laws and regulations.

This Policy applies to all employees of the Company, its vendors, partners, and any external parties involved in client referral, client onboarding and transaction processing.

PART C. GOVERNANCE, AML AND CFT SYSTEMS AND CONTROLS

9. GOVERNANCE AND CORE RESPONSIBILITIES

9.1. Wider Governance Arrangements

This Policy is part of the Company's risk management framework, alongside its arrangements for assessing and mitigating risks (including financial crime risks), senior management's formalized roles and responsibilities, regular reporting to the board, KYE Policy and Procedures, employee training and awareness arrangements. These arrangements are collectively designed to ensure that the Company:

- conducts its business in line with the law and proper standards;
- pro-actively identifies and prevents financial crime risks it is exposed to.

9.2. Core Responsibilities

Approval:

This Policy was approved by decision of the Company's Executive Board. The Chief Executive Officer ensures the Policy is reviewed annually, and, ad-hoc, as legislative and regulatory developments dictate, and, taking into account regular compliance reviews and audit reports.

Delegated authority to make updates and amendments:

The Chief Risk & Compliance Officer is responsible for updating the Policy, subject to an approval from Executive Board, to:

- reflect changes in relevant legislation, regulations and external guidance, where these do not require significant changes in the Company's internal practices and processes;
- update job titles and roles;
- update the list of associated policies and procedures;
- make minor drafting and presentational changes;
- make any other changes that do not substantively change the provisions of the Policy or result in or require significantly different practices and procedures.

In addition, the Chief Risk & Compliance Officer may issue clarifying instructions and guidance materials as to the scope of the Policy and its operation.

Implementation:

The responsibilities for approving and implementing the Anti-Money Laundering, Combating the Financing of Terrorism and sanctions policies are outlined below:

(1) The Executive Board:
   - reviews the financial crime policies and procedures, suggest changes and approves them;
   - reviews regular financial crime reports and annual report prepared by Money Laundering Compliance Officer;
   - reviews the adequacy and effectiveness of the AML and CFT systems and controls employed.

(2) The Chair of the Executive Board it responsible for:
   - the Company's policies and procedures for countering the risk that it might be used to further financial crime.

(3) The Chief Risk & Compliance Officer[3] is responsible for:
   - appointing the Money Laundering Compliance Officer, and providing direction to, and oversight of the Company's AML & CFT strategy;
   - commissioning at least annually a report from the MLCO on the operation and effectiveness of the firm's systems and controls to combat money laundering and terrorist financing, and taking any necessary action to remedy deficiencies identified by the report in a timely manner;
   - reviewing the performance of the MLCO;
   - establishing appropriate policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing;
   - ensuring AML and CFT policies and procedures are kept up-to-date;
   - overseeing the development and reviewing all financial crime and compliance policies including AML & CFT Policy;
   - monitoring compliance with all relevant laws, regulations and policies and reporting any material or relevant non-compliance to the Executive Board.

(4) MLCO:
   - oversees the the Company's compliance with the rules on systems and controls against money laundering;

[3] Whenever this responsibility is shared, the annual MLCO report and MLCO performance is to be reviewed by the higher standing senior manager

- ensures the establishment and maintenance of adequate and effective AML & CFT risk management systems and controls;
- monitors day-to-day compliance with the AML & CFT policies and procedures;
- acts as the focal point for all issues related to ML and TF and primary interface with the regulatory authorities and law enforcement agencies.

The senior managers' prescribed responsibilities and key responsibilities are formalised in the Company's Senior Management Structure, Roles & Responsibilities Statement.

All relevant employees[4] are required at all times to comply with this Policy, associated AML and CFT Procedures Manual and Operational Guidelines. Non-compliance by employees with these policies and procedures may be considered as gross misconduct and could result in a disciplinary offence which could lead to dismissal and depending on the nature of the issue, the employee will possibly be subjected to criminal proceedings.

10. RISK MANAGEMENT FRAMEWORK

To facilitate and ensure compliance with AML & CFT laws and regulations and sanctions regime, the Company is actively implementing a set of measures, consisting of policies, procedures, internal systems and controls. The development and implementation of such adequate measures and their effectiveness, is managed and overseen by the Company's senior management. These measures are applicable to the Company, its vendors, partners, and any external parties involved in client referral, client onboarding and transaction processing.

This section of the Policy provides an overview of the internal adopted measures, while the more detailed procedures are outlined in the AML & CFT Procedures Manual and shall be complied with by all relevant employees, alongside this Policy document.

Below is the summary of internal measures and controls, adopted by the Company and governing its day- to-day operations:

- the Company's governance structure allows for adequate segregation of functions between senior managers in charge of oversight and effective management of all matters related to financial crime risks, and is properly formalized in the Statement of Roles & Responsibilities document;
- the senior managers' roles and assigned responsibilities in relation to managing financial crime risks, developing and providing oversight over the firm's internal systems and controls are clearly defined in the Statement of Roles & Responsibilities approved by the Company's Executive Board and Supervisory Board (if applicable);
- the financial crime risks are identified and assessed as part of the Company's business-wide risk assessments and AML risk assessments, which are produced annually and, when necessary, or as required by the senior management. The priority is given to the risks that have a greater chance of materializing, and may cause a bigger impact for the Company, and, to adequate allocation of resources required to manage the risks effectively;

[4] A relevant employee, is one whose work is: relevant to the firm's compliance with any requirement in the ML Regulations; or otherwise capable of contributing to the: a) identification or mitigation of the risks of ML/TF to which the firm's business is subject; or b) prevention or detection of ML/TF in relation to the firm's business.

- the sufficient level of oversight on the part of the Executive Board is established through regularly produced management information, that also ensures the effectiveness of the development and implementation of the measures and remediation plans, designed to tackle the financial crime risks identified during risk assessments.

The following management information is produced internally:
- monthly high-level financial crime reports summarizing critical KPIs;
- quarterly detailed financial crime reports (incl. AML reports);
- money laundering risk assessments produced at least annually;
- annual report prepared by the MLCO and reviewed by the Executive Board;
- internal audit reports prepared annually or as often as required.

Company does not underestimate the importance of the role that its employees play in tackling money laundering and other financial crime risks, as well as safeguarding the integrity, reputation and high-standards of conduct within the Company. The Company's vetting process and KYE policies, therefore, ensure the integrity and expertise of all relevant employees on an ongoing basis. All relevant employees, including MLCO and senior managers, undergo regular AML training and awareness sessions and are kept aware of their responsibilities and obligations in respect to AML and CFT, as well as recent legislative and regulatory developments in this area, and any changes in the Company's policies and procedures.

11. CLIENT ONBOARDING AND ACCEPTANCE

The following are the broad guidelines in respect to client onboarding:

(a) the clients undergo identification document and face match verification through an automated system, equipped with trusted computer vision technology, that uses machine learning to quickly and accurately ensure the authenticity and validity of the client's ID and verify the client's identity. The detailed procedure is stipulated in the Client Identification and Due Diligence section of the AML & CFT Procedures Manual. It is considered that the automated client identity verification fully replaces face-to-face identity verification;

(b) all clients are screened against World-Check database, in order to ensure that the identity of the client in question does not match with any persons who are known to have criminal background or are subject to sanctions, or is associated with banned entities such as individual terrorists or terrorist organizations, etc. In addition, the clients are screened against records of PEPs (including their close associates and family members), which are also covered in the World-Check database;

(c) all clients are classified into different risk categories in line with the provisions of the Client Classification section of the AML & CFT Procedures Manual. The following risk factors, inter alia, are accounted for when considering the level of risk involved with each client relationship: cumulative amount of funds deposited into the client account/accounts, country of residence, nationality, results of World-Check screening etc. Depending on the level of risk assigned to the client, additional checks may be required for those clients, falling within higher risk categories. Enhanced due diligence is conducted for such clients, whereby the residential address, the source of funds and/or source of wealth, and any other information deemed necessary, are verified additionally to the checks conducted within the standard due diligence. The classification of clients, according to their risk

profile, then serves the Company to set the appropriate rules for ongoing monitoring of the relationship and transactions. The detailed Client Due Diligence procedures are laid out in the relevant section of the AML & CFT Procedures Manual;

(d) following the necessary checks, and, based on the perceived level of risk, associated with each client relationship, the decision is made to either proceed with a client's application or reject it. For all the clients classified as high-risk, an approval from either the MLCO, his deputy or the CEO is required;

(e) PEPs, their family members and close associates are classified as higher-risk and must undergo enhanced due diligence procedure;

(f) the Company's Client Acceptance Policy (CAP) lays down the criteria for accepting of the clients. The detailed provisions of CAP are specified in AML & CFT Procedures Manual. The following client categories, inter alia, are not accepted by the Company as clients (the list below is not exhaustive):

- where sufficient KYC information could not be obtained/confirmed or as per the risk categorization;
- the client matches the person in the sanction lists during World-Check screening and the match is confirmed to be a true match by the designated compliance officer or the MLCO;
- the client matches the person in the lists with criminal records during World-Check screening and the match is confirmed to be a true match by the designated compliance officer or the MLCO;
- clients from countries on the list of non-cooperatives jurisdictions with FATF;
- clients from USA and Mauritius;
- client accounts are in names of companies, the shares of which are in bearer form;
- the client is a Trust account.

12. ONGOING CLIENT MONITORING

The ongoing monitoring arrangements are comprised of two sets of measures:

(1) First, the client records are kept up-to date, KYC information and documents are updated regularly; these updates, for instance, include ongoing World-Check screening for all existing client base. The client information updates may result in re-classification of the client into a different risk category, in which case, the rules for ongoing monitoring over this client relationship are re-set to align with the updated risk category;

(2) In line with the risk classification of a client relationship, the transaction monitoring rules are designed for the specific client, and ongoing monitoring of that client's activity is conducted manually by the relevant employees, in "real-time" and retrospectively.

13. INTERNAL AND EXTERNAL REPORTING

All employees must be aware of their obligation on reporting suspicious activity where they have knowledge or grounds for suspicion. For further guidance on what constitutes grounds for suspicion and what constitutes suspicious activity, please refer to the "Recognition and Reporting of Suspicious Activity" section of the AML & CFT Procedures Manual.

In case of suspicion, all employees must fill in the Internal Suspicious Activity Report and send it directly to the MLCO for further investigation. No transacting with the client who is the subject of suspicion is allowed without the guidance from the MLCO. No disclosure is allowed, apart from the MLCO and the line manager, to anyone within the Company or to the client, for prevention of tipping-off and committing an offence. The detailed procedure for submitting Internal Suspicious Activity Report is outlined in the AML Procedures Manual.

The MLCO is responsible for reviewing all internal reports submitted to him and making a judgement when the report to the FIU must be made.

If no report to FIU is made, the reason must be recorded by the MLCO. The MLCO or deputy MLCO will commit a criminal offence if they know or suspect, or have reasonable grounds to do so, through a disclosure being made to them, that another person is engaged in money laundering and/or terrorist financing, and they do not disclose this as soon as practicable to the FIU.

14. RECORD KEEPING

The retention of relevant records is done in line with the regulatory obligations in Mauritius, and in line with the Company's internal policy, outlined in the AML Procedures Manual.

The MLCO is in charge of keeping records of all referrals received and any action taken to ensure an audit trail is maintained. All information obtained for the purposes of money laundering checks and referrals must be kept up-to-date.

APPENDICES

APPENDIX 1. ASSOCIATED POLICIES AND PROCEDURES

1. AML & CFT Procedures Manual
2. Client Acceptance Policy (CAP)
3. Procedure for Internal Suspicious Activity Reporting
4. KYC and Client Due Diligence procedures
5. Know Your Employee (KYE) Policy
6. Operational guidelines for relevant business divisions
7. Document Retention Policy
8. Senior Management Structure, Roles and Responsibilities Statement

APPENDIX 2. GLOSSARY

AML	Anti-Money Laundering
CAP	Client Acceptance Policy
CEO	Chief Executive Officer
CFT	Combatting the Financing of Terrorism
DD	Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FIU	Finance Intelligence Unit (of Mauritius)
JMLSG	Joint Money Laundering Steering Group
KYC	Know Your Client
KYE	Know Your Employee
MLCO	Money Laundering Compliance Officer
PEP	Politically Exposed Person
SYSC	FCA's Systems and Controls
UN	United Nations