AUGUST 2025

MODMOUNT SERVICES LIMITED

Anti-Money Laundering / Combating the Financing of Terrorism and Compliance Manual

Version 2.0

TABLE OF CONTENTS

Table of Acronyms

AML	Anti-Money Laundering
AML Regs	Anti-Money Laundering Regulations 2020
BO	Beneficial Owner
CAP	Customer Acceptance Policy
CBS	Central Bank of Seychelles
CDD	Customer due Diligence
CEO	Chief Executive Officer
CFT	Countering the Financing of Terrorism (also used for *Combating the Financing of Terrorism*)
CFWP	Combatting the Financing of Weapons Proliferation
CO	Compliance Officer
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSA	Financial Services Authority
KYC	Know Your Customer
ML	Money Laundering
NPO	Non-Profit Organization
PEP	Politically Exposed Person
PTA	Prevention of Terrorism Act 2004
PTA Regs	Prevention of Terrorism (Implementation of United Nations Security Council Resolutions) 2015
RBA	Risk-Based Approach
SCR	Seychelles Rupees
SOF	Source of Funds
SOW	Source of Wealth
SPA	Special Power of Attorney
STR	Suspicious Transaction Report
TF	Terrorist Financing
UNSCRs	United Nations Security Council Resolution 1267 and its subsequent Resolutions & United Nations Security Council Resolution 1373

Table of Definitions and Interpretations

For the purposes of this Manual, unless the context shall prescribe otherwise:

"Beneficial Owner" shall have the meaning set out under Part I, Section 2 of the AML and CFT Act, 2020;

"Board" means the Board of Directors of **MODMOUNT SERVICES LIMITED**;

"Business Relationship" shall have the meaning set out under Part I, Section 2 of the Anti-Money AML and CFT Act, 2020;

"Company" means **MODMOUNT SERVICES LIMITED** which is formed and registered in the Republic of Seychelles under the Companies Act 1972;

"Court" means the Supreme Court of the Republic of Seychelles;

"Criminal conduct" shall have the meaning set out under Part II, Section 3(9) of the AML and CFT Act, 2020 and includes the financing of terrorism;

"Customer" shall have the meaning set out Part I, Section 2 of the AML and CFT Act, 2020;

"Data" means representations in any form of information or concepts;

"Employee" means a person employed by **MODMOUNT SERVICES LIMITED** at non-executive level;

"FATF" means the intergovernmental body known as the Financial Action Task Force, which develops and promotes policies and international standards to protect the global financial system against money laundering, terrorism financing and proliferation financing. The Financial Action Task Force has issued 40 Recommendations and Interpretive Notes for combating money laundering, terrorism financing and proliferation financing;

"Financing of Terrorism" shall have the meaning as referred to in the Prevention of Terrorism Act;

"Manual" means **MODMOUNT SERVICES LIMITED**'s Anti-Money Laundering & Combatting the Financing of Terrorism Compliance Manual & Policy;

"Monetary threshold" is defined as SCR 100,000 for all electronics transactions or SCR 50,000 in cash transactions. That monetary threshold does not apply in existing business relationships and only applies to one off transactions. However, **MODMOUNT SERVICES LIMITED** must still be vigilant in monitoring its customers' transactions for suspicious activity;

"Money Laundering" shall have the meaning set out under Part II, Section 3 (1) of the Anti-Money Act 20;

"One-off transaction" shall have the meaning set out under Section 49 (2) of the AML and CFT Act, 2020;

"Officer" means a person employed by **MODMOUNT SERVICES LIMITED** at executive level;

"PEP" shall have the meaning set out under Section 36 of the AML and CFT Act, 2020;

"Person" shall have the meaning set out under Part I, Section 2 of the AML and CFT Act, 2020;

"Property" shall have the meaning set out under Part I, Section 2 of the AML and CFT Act, 2020;

"Regulated Person" shall have the meaning set out under Section 42 (3) of the AML and CFT Act, 2020;

"Republic" means the Republic of Seychelles;

"Residential Address" means the physical address in any country where an individual has been residing within the last 3 months, at the time this individual instructs **MODMOUNT SERVICES LIMITED** to carry out a service;

"Shell Bank" shall have the meaning set out under Section 38 (2) (a) of the AML and CFT Act, 2020

"Source of Funds" means the origin and the means of transfer for funds that are directly involved in the transaction (for example, business activities, proceeds of sale, corporate dividends);

"Source of Wealth" means the activities that have generated the total net worth of the customer (that is, the activities that produced the customer` s funds and property);

"Suspicious Transactions Report" means a report made or to be made by the company under Section 48 of the AML and CFT Act, 2020;

"Tipping Off" occurs where without lawful excuse, an act is carried out which notifies or disclose to a customer or unauthorized third parties' information or that fact that a report has been made to the FIU under Section 50 of the AML and CFT Act, 2020 or that an investigation is taking place;

Words importing one gender include all other genders and words importing the singular include the plural and vice versa.

Table of Laws and Regulations

The relevant regulatory requirements to whom **MODMOUNT SERVICES LIMITED** must comply with, are as follows:

Legislation

i. AML and CFT Act, 2020 and its subsequent amendments
ii. Anti-Money Laundering Regulations, 2020
iii. Companies Act 1972
iv. Beneficial Ownership Act, 2020
v. Financial Institutions (Application of Act) Regulations, 2010
vi. Prevention of Terrorism Act, 2004 (and subsequent amendments)
vii. Prevention of Terrorism Regulations, 2015

Additional Guidance of interpretation and good practices to whom MODMOUNT SERVICES LIMITED may refer to, are as follows:

i. Guidance on Transparency and Beneficial Ownership issued by the FATF October, 2014
ii. Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities in Seychelles (updated) June, 2015

1. Introduction

The purpose of the Manual is to lay down the Company's internal practice, measures, procedures and controls relevant to the prevention of ML and TF.

The Manual is developed and periodically updated by the CO based on the general principles set up by the Board in relation to the prevention of ML and TF.

All amendments and/or changes of the Manual shall be approved by the Board. Thereafter, the changes will be presented to the Authority (FSA) for its approval.

The Manual shall be communicated by the CO to all the employees of the Company that manage, monitor or control in any way the customers' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined herein.

The Manual has been prepared to comply with the applicable legislative and regulatory provisions, relevant guidelines and good practices.

2. Manual Applicability

This Manual applies to all company officers, employees, appointed contractors, agents, products and services offered by the Company. All business units within the company will cooperate to create a cohesive effort in the fight against ML. Each business unit has implemented risk-based procedures reasonably expected to detect and prevent the reporting of transactions. All efforts exerted will be documented and retained.

The CO is responsible for initiating STRs or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Manual shall be directed to the CO.

In this respect, the CO shall be responsible to update the Manual so as to comply with FSA's future requirements, as applicable, regarding the customer identification and due diligence procedures which the Company must follow.

All employees who are involved with investor services and cash management have been made aware of the Company's policies and procedures relating to AML/CFT and are aware of the consequences, if the Company is not in compliance with the applicable AML and CFT Act 2020 and AML Regs.

The senior officers within the firm will continually monitor the applicable laws and regulations and will update the manuals should new regulations or laws be issued or if the firm becomes aware that we are not in compliance with the existing laws and regulations.

The Manual is designed to prevent the Company from forming business relationships or from carrying out one-off transactions with or for another person / entity /customer, unless the Company can:

(a) Clearly establish the identity of the person / entity /customer;
(b) Maintain record keeping procedures in accordance with applicable laws and regulations.

3. The responsibilities of the Board of Directors

The responsibilities of the Board in relation to the prevention of ML and TF include the following:

(a) to determine, record and approve the general policy principles of the Company in relation to the prevention of ML and TF and communicate them to the CO;
(b) to appoint an individual that possesses the skills, knowledge and expertise relevant to financial and other activities depending on the situation, who shall act as the CO and, where is necessary, alternate to the CO and determine their duties and responsibilities, which are recorded in this Manual;
(c) to approve the Manual;
(d) to ensure that all relevant requirements of the Laws and Regulations are applied, and assure that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirement;
(e) to ensure that the CO, alternate to the CO, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention of ML and TF (i.e. personnel of the Dealing and Operations Manager), have complete and timely access to all data and information concerning customers' identity, transactions' documents (as

and where applicable) and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties, as included herein;

(f) to ensure that all employees are aware of the person who has been assigned the duties of the CO to whom they report, any information concerning transactions and activities for which they have knowledge or suspicion that might be related to ML and TF;

(g) to establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the CO, either directly or through the alternate to the CO, if any, and notifies accordingly the CO for its explicit prescription in the Manual

(h) to ensure that the CO and the Dealing and Operations Manager have sufficient resources, including competent employees and technological equipment, for the effective discharge of their duties

(i) to assess and approve the CO's Annual Report of Section 6 of the Manual and take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the abovementioned report;

(j) to meet and decide the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected in the Internal Auditor's report in the manner described in Section 4 of the Manual. The minutes of the said decision of the Board and the Internal Auditor's report shall be submitted to the FSA no later than four (4) months after the end of the calendar year (i.e., the latest, by the end of April);

(k) to implement adequate and appropriate systems and processes to detect, prevent and deter money laundering arising from serious tax offences;

(l) to ensure that the Company's officials do not knowingly aid or abet customers in committing tax offences;

(m) approve the mandatory annual training program prepared by the CO,

(n) ensure that it receives adequate management information on the implementation of the company's AML/CFT training program; and

(o) ensure to be adequately trained to be well aware and up-to-date with the regulatory framework and the relevant responsibilities deriving from this.

4. Obligations of the Internal Auditor

Depending on the size and nature of the activities of the Company, an independent Internal Audit function should be established for the verification of policies, controls and procedures.
The Company is required by section 33(d) (e) of the AML and CFT Act, 2020 to implement independent audit arrangements to test its procedures and systems relating to anti-money laundering, and terrorist financing activities. The following obligations of the Internal Auditor are addressed specifically for the prevention of ML and TF:

(a) the Internal Auditor shall review and evaluate, at least on an annual basis, the appropriateness, effectiveness and adequacy of the policy, practices, measures, procedures and control mechanisms applied for the prevention of ML and TF mentioned in the Manual;

(b) The findings and observations of the Internal Auditor, in relation to point (a) above, shall be submitted, in a written report form, to the Board.

5. Compliance Officer

The CO shall belong hierarchically to the higher ranks of the Company's organizational structure so as to command the necessary authority. The CO shall lead the Company's AML/CFT compliance procedures and processes and report to the Board. The CO shall at all times be resident in Seychelles. In addition, an alternate to the CO be appointed to assume the prescribed responsibilities and duties in the CO`s absence.

As per section 34 of the Anti-Money Laundering and Countering the Financing of Terrorism Act, 2020, the Company shall within 30 days of the commencement of its operations:

(a) appoint the Compliance Officer who shall be responsible, for ensuring the compliance with the provisions of AML and CFT Act, 2020, with the approval of the respective supervisory authority:

(b) the CO appointed pursuant to this section will:

i. be a senior officer with the necessary qualifications and experience and able to respond adequately to enquiries relating to the Company and the conduct of its business;

ii. be a resident in Seychelles;

iii. be responsible for the implementation and on-going compliance of the company's internal programs, controls and procedures in relation to its business with the requirements of AML and CFT Act, 2020;

iv. be responsible for ensuring that Company's staff comply with the provisions of the AML and CFT Act, 2020 and any other law relating to ML or TF and the provisions of any manual of compliance procedures established; and

v. act as the liaison officer between the company and the supervising authority and the FIU in matters relating to compliance with the provisions the AML and CFT Act, 2020 and any other law with respect to ML or TF;

vi. be familiar with the provisions of the guidelines that may be issued by the FIU and the relevant supervisory authority;

vii. have unrestricted access on demand to all books, records and employees of the company as may be necessary to fulfil his or her responsibilities;

viii. receive and review reports of suspicious transactions, or suspicious activities made by the staff of the company and, if sufficient basis exists, report the same to the FIU in accordance with the AML and CFT Act, 2020; and

ix. implement record keeping and retention requirements under sections 47 of the AML and CFT Act, 2020;

x. implement the reporting requirements under section 48 of the AML and CFT Act, 2020, with regard reporting suspicious transaction or certain information;

xi. ensure the Company's officers and employees are aware of the laws and Regulations relating to ML and TF;

xii. ensure the Company's officers, employees and agents recognize suspicious transactions, trends in ML and TF activities and ML and TF risks within the Company's products, services and operations.

xiii. To develop a compliance culture —

a) to ensure that all directors and relevant staff are familiar with the laws and regulations of the Seychelles to combat money laundering and terrorist financing activities, which includes an understanding of the relevant compliance policies, procedures and systems of the company as well as,

the compliance officer imparts awareness of the need for compliance, thereby, developing within the company a robust compliance culture;

b) to monitor the developments and changes in the legislation, policies, standards and other guidelines issued by the international bodies in order to keep the company updated with the regulatory developments and changes in international requirements;

xiv. to implement the training program —

a) for directors and relevant staff which includes the training program on general anti-money laundering and countering the financing of terrorism awareness, client acceptance procedures, know your customer (KYC) procedures, remediation and suspicious activity reporting relevant to the company's activities;

b) at least once in every year and whenever there are changes in the laws, regulations or international requirements to ensure that the directors and related staff are aware of the latest developments in the anti-money laundering and countering the financing of terrorism activities;

c) to undergo additional training, in order to enhance his or her professional skills, at least once every year;

xv. to perform review of the compliance framework and make regular assessment reports to the senior management, identify the deficiencies and making recommendations for any updates or revisions;

xvi. to ensure the preparation and submission of an annual compliance report to the supervisory authority for information within 90 days after each calendar year.

(c) **MODMOUNT SERVICES LIMITED** shall appoint a senior official at management level as an alternate compliance officer, with the approval of the supervisory authority to act in the absence of a compliance officer. At the initial stage of the Company's operations, the Company might seek for an exemption to appoint an Alternate Money Laundering Officer, in case it shall have 5 or less than 5 people employed.

The level of remuneration of the CO or alternate to the CO shall not compromise his objectivity.

6. Annual Report of the Compliance Officer

The Annual Report of the CO or alternate to the CO is a significant tool for assessing the Company's level of compliance with its obligation laid down in the Laws and Regulations.

This Annual Report shall be prepared and be submitted to the Board for approval within two (2) months from the end of each calendar year (i.e., the latest, by the last day of the month of February of each calendar year). Following the Board's approval of the Annual Report, a copy of this Annual Report shall be submitted to the FSA together with the Audited Accounts. It is provided that minutes shall include the measures decided for the correction of any weaknesses and/or deficiencies identified in the Annual Report and the implementation timeframe of these measures.

The Annual Report deals with issues relating to ML and TF during the year under review and includes, inter alia, the following:

(a) information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Law and Regulations which took place during the year under review;

(b) information on the inspections and reviews performed by the CO or alternate to the CO, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Company applies for the prevention of ML and TF. In this respect, the report outlines the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation;

(c) the number of internal STRs submitted by Company personnel to the CO or alternate to the CO, and possible comments/observations thereon;

(d) the number of STRs submitted by the CO or alternate to the CO to the FIU, with information/details on the main reasons for suspicion and highlights of any particular trends;

(e) information, details or observations regarding the communication with the employees on ML and TF preventive issues;

(f) information on the policy, measures, practices, procedures and controls applied by the Company in relation to high-risk customers as well as the number and country of origin of high-risk customers with whom a business relationship is established or a one-off transaction has been executed;

(g) information on the systems and procedures applied by the Company for the ongoing monitoring of customer accounts and transactions, as and when applicable;

(h) information on the training courses/seminars attended by the CO or alternate to the CO and any other educational material received;

(i) information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organized, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organisation or consultants;

(j) results of the assessment of the adequacy and effectiveness of staff training;

(k) information on the recommended next year's training program;

(l) information on the structure and staffing of the department of the CO or alternate to the CO, as well as, recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against ML and TF; and

(m) an executive summary in respect to the key findings and weaknesses identified during the year under review.

7. Money Laundering and the Financing of Terrorism

7.1. Money Laundering

ML is the process by which criminals attempt to conceal the true origins and ownership of their proceeds of crime. It is generally recognized that there are traditionally three stages to ML. These are:

a) Placement – which is the stage at which money is placed into the financial systems (for example cash is deposited in a bank account);

b) Layering – the stage at which the money is "washed", by being moved through a complex web of transactions to hide their origins;

c) Integration – the stage at which the illegal origin of the funds is considered to be well hidden enough for it to re-enter the financial system through a legitimate source without the fear of it being detected, such as an investment vehicle.

MODMOUNT SERVICES LIMITED recognizes that its products and services can be used at any one of the three stages of ML.

7.2. The Offence of Money Laundering in Seychelles

Under section 3 of the AML and CFT Act, 2020, a person is guilty of ML if the person knowingly, or believing that property is or represents benefit from criminal conduct or is reckless to that fact, without lawful authority or excuse, -

a) Converts, transfers or handles the property or removes it from the Republic of Seychelles;
b) Conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights with respect to it;
c) Acquires, or uses that property.

A person who aids, abets, assists, attempts to, counsels, conspires, conceals or procures the commission of ML is also liable to be tried as a principal offender for the offence of ML.

Criminal conduct is often term predicate offence. The AML and CFT Act, 2020 take a threshold approach in defining criminal conduct as any act or omission against any law in the Republic or elsewhere that is punishable on conviction to a term of imprisonment exceeding 3 years and/or to a fine of SCR 50,000 or to both.

The nature of **MODMOUNT SERVICES LIMITED** business means that at any point, the Company can be susceptible to being used for ML, even in instances where the Company has no knowledge that it is participating in a crime. For this reason, the Company must at all times take precautionary measures and act in good faith when providing services or products to its customers.

7.3. Penalties for the offence of Money Laundering

ML is punishable on conviction to a term not exceeding 15 years imprisonment and/or to a fine not exceeding SCR 5,000,000 for a natural person and to a person other than a natural person to a fine not exceeding SCR 10,000,000.

In addition, where the Company or any of its officers, employees and agents fail without lawful excuse to comply with the requirements of the AML and CFT Act, 2020; the Company or any of its officers, employees and agents may be guilty of offences under the AML and CFT Act, 2020. **MODMOUNT SERVICES LIMITED** must therefore ensure that it:

a) implements internal rules and controls;
b) maintains business relationships in true names;
c) establishes the identify of its customers;
d) appoints a CO or alternate to the CO and provide training to officers, employees, agents and the Board;
e) reports suspicious activities or transactions related to ML or TF;
f) complies with a restraining order where the case requires;
g) does not tip off customers;
h) does not obstruct a member or representative of the FIU from making enquiries and carrying out investigations; and
i) maintains records for seven (7) years.

7.4. Financing of Terrorism

The objective of terrorist activity is to intimidate a population or compel a government to do something. This is done by intentionally killing, harming or endangering people, causing property or environmental damage, or by disrupting services, facilities, or systems. It covers a range of serious criminal offences (*including certain acts committed outside Seychelles*) by which a person, directly or indirectly, provides, collects or makes available funds, property, or a related financial service intending or knowing that they be used, or in the knowledge that they will be used in whole or in part, to facilitate the commission of a terrorist act or to benefit a person who is committing or facilitating the commission of a terrorist act.

Terrorism seeks to influence, compel or intimidate governments or a population through threats or violence, causing of damage to property or danger to life, creating of serious risks to public health or safety, or disrupting of important public services or infrastructure. The financing of terrorism is defined in s 2 of the PTA by reference to the provisions of the PTA.

TF is the acquiring of funds required by terrorists to carry out terrorism acts. Sources of terrorism financing may be legitimate or illegitimate. For example, they may be derived from;

a) *Criminal activities*: The sums needed to fund terrorist attacks are not always large and the associated transactions are not necessarily complex; and
b) *Legitimate sources*: such as income from legitimate business operations belonging to terrorist organizations and charitable donations.

The methods used by terrorist organizations or individuals to obtain, move, or conceal funds for their activities are similar to those used by criminal organizations to launder their funds. Alternatively non-profit organizations or charitable organizations may be infiltrated so as to divert a portion of donations to terrorist activities.

In relation to TF, the Company core obligation is to ensure that persons designated by the United Nation as terrorists under UNSCRs 1267 and designated under Seychelles' country list under the framework set up by the PTA Regs pursuant to UNSCRs 1373 are prevented from using the Company services and products. **MODMOUNT SERVICES LIMITED** complies with this obligation by screening its customers at the point of on-boarding of the customer against the list of designated persons and each time the customer requests to be provide with new products and services.

7.5. Money Laundering and Financing of Terrorism related risks

ML and TF can pose numerous risks to the Company. The four major areas of risks that are relevant are:

a) *Regulatory risk*: where these represent the risk of regulatory actions and sanctions being taken against the Company, for non-compliance with or violation of rules, laws and regulations which are aimed at preventing ML/TF. This can be associated with poor practices such as ineffective internal controls, policies, procedures, poor ethical standards within the Company and can adversely impact of the Company's capital and earnings.

b) *Reputational risk*: where the Company's reputation within the financial services industry in general, amongst its customers, partners, officers, employees, agents and the public will be tainted by the occurrence of a risk event. The Company's reputation is considered as one of its most valuable corporate assets and the damage that such an event may cause may be irreparable.

c) *Operational risk*: the risk that any part of the Company's operation will fail because of human failure and/or systems or procedural failure. This type of risk arises where fraud and errors are not effectively controlled and an adverse effect occurs on the Company`s ability to deliver products and services and also on its ability to maintain a competitive position within the industry.

d) *Liquidity risk:* refers to the risk that the Company will not be able to meet its financial obligations as they arise. This type of risk is relevant to the Company in the context of ML/TF because possible occurrence of non-compliance or violations of laws and rules may result in fines being imposed on the Company thereby affecting its liquidity.

8. Preventive Measures

8.1. Application of a risk-based approach

The Company shall apply adequate and appropriate measures, policies, controls and procedures, depending on its nature and size, by adopting a RBA, in order to mitigate and effectively manage the risks of ML and TF; so as to focus its effort in those areas where the risk of ML and TF appears to be comparatively higher.

The Company shall take appropriate measures to identify and assess the risks of ML and TF, taking into account risk factors including those relating to its customers, countries or geographic areas, products, services, transactions or banking channels. Those measures should be proportionate to the size and nature of the Company.

The risk assessments referred above shall be documented, updated and made available to FSA.

The adopted RBA that is followed by the Company, and described in the Manual, has the following general characteristics:

(a) recognizes that the ML or TF threat varies across customers, countries, services and securities;
(b) allows the Board to differentiate between customers of the Company in a way that matches the risk of their particular business;
(c) allows the Board to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;
(d) helps to produce a more cost-effective system; and
(e) promotes the prioritization of effort and actions of the Company in response to the likelihood of ML and TF occurring through the use of the Securities and Dealing Services provided by the Company.

The RBA adopted by the Company, and described in the Manual, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the ML and TF risks faced by the Company.

Such measures include:

(a) identifying and assessing the ML and TF risks emanating from particular customers or types of customers, securities, services, and geographical areas of operation of its customers;
(b) managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
(c) continuously monitoring and improving the effective operation of the policies, procedures and controls;

(d) performing identification and due diligence in accordance with the provisions under Sections 15 and 16 of the AML Regs;
(e) record keeping, in accordance with the provisions under Section 47) of the AML and CFT Act, 2020;
(f) ensuring the existence of internal control, assessment and risk management in order to prevent ML and TF;
(g) undertaking a thorough examination of any transactions which, by their very nature, are particularly susceptible of being linked to ML or TF offenses, and in particular of any complex or abnormally large transactions and of all the unusual transactions occurring without obvious economic or clear legitimate reason;
(h) setting up risk management practices;
(i) setting up compliance management;
(j) ensuring that sufficient recruitment policy is in place and assessment of the employees' integrity;
(k) performing ongoing training of employees in the recognition and handling of transactions and activities which may be related to ML or TF.

The Board shall assess and evaluate the risks it faces, for usage of the services provided for the purpose of ML or TF. The particular circumstances that shall determine the suitable procedures and measures which need to be applied to counter and manage risks including identification, recording and evaluation of risk that the Company faces, presuppose to the finding of the risk posed by the customers' behavior, the way the customer communicate and the risk posed by the services and securities provided by the Company.
The application of appropriate measures, the nature and extent of the procedures on a RBA depends on different indicators.

Such indicators include inter alia the following:

- the scale and complexity of the services offered;
- geographical spread of the services, products and customers;
- the nature (e.g., non-face-to-face) and economic profile of customers as well as of securities and services offered;

- the distribution channels and practices of providing services;
- the volume and size of transactions;
- the degree of risk associated with each area of services;
- the country of origin and destination of customers' funds;
- deviations from the anticipated level of transactions; and
- the nature of business transactions.

The Company when assessing the risk of ML and TF shall take into account, among others, the Risk Factor Guidelines and any guidelines/guidance issued by the Financial Action Task Force (FATF).

The CO or alternate to the CO shall be responsible for the development of the policies, procedures and controls on an RBA. Further, the CO or alternate to the CO shall also be responsible for the adequate implementation of the policies, procedures and controls on a risk-based approach. The Internal Auditor shall be responsible for reviewing the adequate implementation of a risk-based approach by the CO or alternate to the CO, at least annually.

8.2. Identification of risks

The RBA adopted by the Company involves the identification, recording and evaluation of the risks that have to be managed.

The Company shall assess and evaluate the risks it faces, for the use of the Securities and Dealing Services for the purpose of ML or TF. The particular circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk. In this respect the Company has further established a non-exhaustive Risk Factor Assessment check list (Appendix 4 of this Manual).

In the cases where the Securities and Dealing Services and the securities that the Company provides are relatively simple, involving relatively few customers or customers with similar characteristics, then the Company shall apply such procedures which are able to focus on those customers who fall outside the 'norm'.

The Company shall be, at all times, in a position to demonstrate to FSA that the extent of measures and control procedures it applies are proportionate to the risk it faces for the use of the Securities and Dealing Services provided, for the purpose of ML and TF.

The Company shall take the following indicative risk variables into consideration while it determines the risks implicated as well as the categorization of the customers:

i. The purpose of the account or the relationship;
ii. The volume of assets that will be deposited by the customer or the size of the transactions; and
iii. The regularity or the duration of the business relationship.

8.3. Company risks

The following, inter alia, are sources of risks which the Company faces with respect to ML and TF:

(a) Risks based on the customer's nature:

- complexity of ownership structure of legal persons;
- companies with bearer shares;
- companies incorporated in offshore centers;
- PEPs;
- customers engaged in transactions which involves significant amounts of cash;
- customers from high-risk countries or countries known for high level of corruption or organized crime or drug trafficking; and
- unwillingness of customer to provide information on the BOs of a legal person.

(b) Risks based on the customer's behavior:

- customer transactions where there is no apparent legal financial/commercial rationale;
- situations where the SOW and/or SOF cannot be easily verified; and
- unwillingness of customers to provide information on the BOs of a legal person.

(c) Risks based on the customer's initial communication with the Company:

- non-face-to-face customers; and

- customers introduced by a third party.

(d) Risks based on the Company's services and securities:

- services that allow payments to third parties;
- large cash deposits or withdrawals; and
- products or transactions which may favor anonymity.

8.4. Measures/Procedures to manage and mitigate the risks

Taking into consideration the assessed risks, the Company shall determine the type and extent of measures it will adopt in order to manage and mitigate the identified risks in a cost-effective manner.

These measures and procedures include:

- adaption of the CDD procedures in respect of customers in line with their assessed ML and TF risks;
- requiring the quality and extent of required identification data for each type of customer to be of a certain standard (e.g., documents from independent and reliable sources, third party information, documentary evidence);
- obtaining additional data and information from the customers; where this is appropriate for the proper and complete understanding of their activities, and SOW for the effective management of any increased risk, emanating from the particular business relationship or the one-off transaction; and
- ongoing monitoring of high-risk customers' transactions and activities, as and when applicable.

The risk assessment and the implementation of the measures and procedures result in the categorization of customers according to their risk appetite. The categorization is based on criteria which reflect the possible risk causes and each category is accompanied with the relevant due diligence procedures, regular monitoring and controls.

The Company shall prepare and maintain a customer list, which contain, inter alias, the customers' names, account numbers, date of commencement of the business relationship and their risk classification. The respective list should be promptly updated with all new or existing

customers that the Company determined, in the light of additional information received, that fall under one of the risk categories.

In this respect, it is the duty of the CO or alternate to the CO to develop and constantly monitor and adjust the Company's policies and procedures with respect to the Customer Acceptance Policy, CDD and Identification Procedures, as well as via a random sampling exercise as regards existing customers.

8.5. Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Customers' activities change as well as the services and securities provided by the Company change. The same happens to the securities and the transactions used for ML or TF.

In this respect, it is the duty of the CO or alternate to the CO to undertake regular reviews of the characteristics of existing customers, new customers, services and securities and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics or circumstances. These reviews shall be duly documented, as applicable, and form part of the AML Report.

9. Customer Acceptance Policy

The CAP following the principles and guidelines described in this Manual, defines the criteria for accepting new customers and defines the customer categorization criteria which shall be followed by the Company and especially by the employees which shall be involved in the customer account opening process.

The CO or alternate to the CO shall be responsible for applying all the provisions of the CAP. In this respect, the Dealing and Operations Manager shall be assisting the CO or alternate to the CO with the implementation of the CAP, as applicable. The Internal Auditor shall review and evaluate the adequate implementation of the CAP and its relevant provisions, at least annually.

9.1. General Principles of the CAP

The general principles of the CAP are the following:

(a) the Company shall classify customers into various risk categories and based on the risk perception decide on the acceptance criteria for each category of customer;

(b) where the customer is a prospective customer, an account must be opened only after the relevant pre-account opening due diligence and identification measures and procedures have been conducted, according to the principles and procedures set out in this Manual;

(c) all documents and data described shall be collected before and/or during accepting a new customer;

(d) no account shall be opened in anonymous or fictitious name(s);

9.2. Criteria for accepting new customers (based on their respective risk)

This section describes the criteria for accepting new customers based on their risk categorization.

I. Low Risk Customers

The Company shall accept customers who are categorized as low risk customers as long as the general principles are followed. Moreover, the Company shall follow the Simplified CDD procedures for low-risk customers, according to section 15 of the AML Regs.

II. Normal Risk Customers

The Company shall accept customers who are categorized as normal risk customers as long as the general principles are followed.

III. High Risk Customers

The Company shall accept customers who are categorized as high-risk customers as long as the general principles are followed. Moreover, the Company shall apply the EDD measures for high-risk customers, according to section 16 of the AML Regs, as well as, apply the due diligence and identification procedures for the specific types of high-risk customers mentioned below, as applicable.

9.3. Not acceptable customers

The following list predetermines the type of customers who are not acceptable for establishing a business relationship or an execution of a one-off transaction with the Company:

(a) customers who fail or refuse to submit, the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification;

(b) customers included in Sanction Lists;

(c) shell banks – *the Company is prohibited from entering into, or continuing, a correspondent relationship with a shell bank. The Company shall take appropriate measures to ensure that it does not engage in or continue correspondent relationships with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank*.

9.4. Customer categorization factors

This section defines the criteria for the categorization of customers based on their risk. The CO or alternate to the CO shall be responsible for categorizing customers in one of the following three (3) categories based on the criteria of each category set below:

I. LOW RISK CUSTOMERS

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk:

(a) <u>Customer risk factors:</u>

i. Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;

ii. Public administrations or enterprises;

iii. Customer that are resident in geographical areas of lower risk.

(b) <u>Product, service, transaction or delivery channel risk factors:</u>

i. Life insurance policies for which the premium is low;

ii. Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;

iii. A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;

iv. Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes

v. products where the risks of ML and TF are managed by other factors such as purse limits or transparency of ownership (e.g., certain types of electronic money).

(c) Geographical risk factors:

i. The geographical location of the customer's residence;

ii. The geographical location of the customer's business interests and/or assets.

Finally, the Company shall do monitoring on ongoing basis the transactions of low-risk customers to ensure that there are no suspicious transactions.

II. NORMAL RISK CUSTOMERS

The following types of Customers can be classified as normal risk Customers with respect to the Money Laundering and Terrorist Financing risk which the Company faces:

i. any customer who does not fall under the 'Low Risk Customers' or 'High Risk Customers' categories;

ii. customers who are not physically present for identification purposes (non-face-to-face customers).

III. HIGH RISK CUSTOMERS

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk:

(a) Customer risk factors:

i. the business relationship is conducted in unusual circumstances;
ii. customers that are resident in geographical areas of higher risk;
iii. legal persons or arrangements that are personal asset-holding vehicles;
iv. companies that have nominee shareholders or shares in bearer form;
v. businesses that are cash-intensive;
vi. the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;
vii. PEPs;
viii. customers convicted for a prescribed offence (*and already served their sentence*);
ix. unwillingness of customer to provide information on the BOs of a legal person;
x. trust accounts;
xi. "customers' accounts" in the name of a third party;
xii. customers who are involved in electronic gambling/gaming activities through the internet;
xiii. customers from countries which inadequately apply FATF's recommendations;
xiv. any other customers that their nature entail a higher risk of ML or TF; and
xv. any other customer determined by the Company itself to be classified as such.

(b) Product, service, transaction or delivery channel risk factors:

i. private banking;
ii. products or transactions that might favor anonymity;
iii. non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
iv. payment received from unknown or non-associated third parties;
v. new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

(c) Geographical risk factors:

i. countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
ii. countries identified by credible sources as having significant levels of corruption or other criminal activity;
iii. countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;
iv. countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

(d) Risk based on the customer's behavior:

i. customer transactions where there is no apparent legal financial/commercial rationale.
ii. situations where the origin of wealth and/or source of funds cannot be easily verified.
iii. unwillingness of Customers to provide information on the Beneficial Owners of a legal person.

(e) Risk based on the customer's initial communication with the Company:

i. non-face-to-face Customer;
ii. customers introduced by a third party.

(f) Risk based on the company's services and securities:

i. services that allow payments to third parties;
ii. large cash deposits or withdrawals;
iii. products or transactions which may favor anonymity.

The Company shall perform the Risk Scoring Matrix to all its potential customers in order to assess the risks of ML and TF.

10. Customer identification and due diligence procedures

MODMOUNT SERVICES LIMITED shall ascertain, before or within a reasonable time after entering into a business relationship, the identity of a customer on the basis of any official or other identifying document.

The Company shall verify such identity on the basis of reliable and independent source documents, data or information or other evidence as is reasonably capable of verifying the identity of the customer —

(a) when establishing a business relationship;

(b) when carrying out one-off transaction that amounts to SCR 100,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(c) when there is a suspicion of ML or TF, regardless of the amount of the transaction in the provision of the relevant Securities and Dealing Services; and

(d) when there are doubts about the veracity or adequacy of previously customer identification data.

In this respect, it is the duty of the CO or alternate to the CO to apply all the relevant CDD identification procedures described in this Manual and the Company's CAP, as applicable. Furthermore, the Dealing and Operations Manager shall be responsible to collect and file the relevant customer identification documents, according to the recording keeping procedures described herein.

The Company may apply simplified due diligence measures in respect of customer relationship in case the business relationship or transaction is categorized as a lower degree of risk. The Company should obtain sufficient information in order to identify whether a business relationship or transaction is presenting lower risk.

The CDD measures to be applied can be further categorized as simplified, standard or enhanced CDD measures.

10.1. Simplified CDD procedures

Section 15 of the AML Regs allows for simplified CDD measures to be applied in respect of:

a) A licensed bank;
b) A recognized foreign bank;
c) The Central Bank of Seychelles;
d) A public body in Seychelles; and
e) A legal person which securities are listed on a recognized exchange.

This means that, if any customers fit those regulatory requirements allowing the exemptions, the Company, needs only to collect evidence of those requirements such as evidence that the customer is a regulated legal person as defined and verify that regulated status by checking the supervisory authorities' websites or listings. In other lower risk scenarios, the standard CDD of the Company may also be simplified.

With respect to the provisions of the said section for simplified CDD procedures, the following shall apply:

i. The Company may apply simplified CDD measures if previously satisfied that the business relationship or transaction has a lower degree of risk;
ii. The Company shall be adequately monitoring the relevant transactions and the business relationship, so that unusual or suspicious transactions can be traced;
iii. When assessing the risks of ML and TF related to customer categories, geographic areas and to specific products, services, transactions or delivery/service channels, the Company shall take into account at least the factors relating to the situations of potentially lower risk.

The Company's simplified CDD may include verifying the identity of the customer and the BO after the establishment of the business relationship (*e.g., if account transactions rise above a defined monetary threshold*); reducing the frequency of customer identification updates; reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold; not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

10.2. Standard CDD procedures

10.2.1. Natural Person

If the customer is a natural person, the following information shall be collected:

i. True name(s) used;
ii. Residential address, city code, telephone number;
iii. Business address;
iv. Date and place of birth;

Identity should be verified via one of the following:

i. Valid Passport;
ii. National ID Card;
iii. Current photo-card driving license.

The indicated documents should show a clear photograph of the customer.

The current residential address will be verified by one of the following:

i. A recent utility bill;
ii. Bank statement;
iii. Credit card statement (monthly).

*The utility bill, bank statement and credit card statement should **not** be older than 3 months from the filing date.*

The Company shall also be obtaining the below for FATCA / CRS purposes:

i. Tax Identification Numbers or Social Security Number or Government Service / Insurance System number.

For each account the Company shall also make reasonable effort, prior to the settlement of the initial transaction, to obtain the following information to the extent it is applicable to the account:

i. Occupation of customer;
ii. The customer's securities objective and other related information concerning the customer's financial situation and needs;
iii. Annual income, Assets or net worth.

10.2.2. Legal Person

Before establishing a business relationship, a company search and/or other commercial inquiries shall be made to ensure that the corporate/other business applicant has not been, or is not in the process of being dissolved, struck off, wound-up or terminated. In the event of doubt as to the identity of the company or its directors, or the business or its partners, a search or inquiry with the relevant Supervising Authority/Regulatory Agency shall be made.

The following relevant documents shall be obtained in respect of a legal person:

i. Copies of the Certificate of Registration, including Articles of Incorporation or Certificate of Partnership, as appropriate;
ii. Copies of the By-Laws and latest General Information Sheet, which lists the names of directors/partners and principal stockholders, and secondary licenses;
iii. Certificate of Directors, Certificate of Shareholders and Certificate of Registered Office – if these certificates are not available, please provide Certificate of Incumbency (including number of issued shares, registered address and all directors and shareholders)
iv. Board Resolution authorizing the corporation to open the account with the Company;
v. Any or all of the foregoing documents, where required, should be produced and submitted for verification;
    - Proof of identity for directors and shareholders (10%+): Copies of passports or national identity cards.
    - Proofs of address for directors and shareholders (10%+): copies of the utility bill or bank statement issued not more than 3 months ago.
vi. Where applicable, the Company may also require additional information about the nature of the business of customers, copies of identification documents of shareholders, directors, officers and all authorized signatories.

10.2.3. Trust Accounts

When the Company establishes a business relationship or carries out a One-off transaction with trusts, it shall ascertain the legal substance, the name and the date of establishment of the trust and verify the identity of the trustor, trustee and BOs, according to the customer identification procedures prescribed in throughout this Manual. Nevertheless, the Company shall receive

sufficient information about the beneficiary to ensure the Company is be able to identify the BO at the time of the payment or when the beneficiary exercises his acquired rights.

Furthermore, the Company shall ascertain the nature of activities and the purpose of establishment of the trust as well as the source and origin of funds requesting the relevant extracts from the trust deed and any other relevant information from the trustees. All relevant data and information shall be recorded and kept in the Customer's file.

The Company shall maintain a central register of BOs of trusts. The said register must hold adequate, accurate and current information on their beneficial ownership, including the identity of:

i. the trustee;
ii. the settlor;
iii. the protector;
iv. the beneficiaries or class of beneficiaries; and
v. Any other natural person exercising effective control over the trust.

10.2.4. Verification of Customer identity

The Company has implemented an integrated multilevel electronic system of information verification provided by the customer. This system documents and checks identification details of the customer, keeps and controls drill through reports of all the transactions.

If the Company concludes that the non-face-to-face business relationship or transaction, presents higher risk of money laundering or terrorist financing, it should apply enhanced customer due diligence measures. The said measures may be one the following:

i. Telephone contact of the applicant at an independently verifiable home or business number; or
ii. Direct confirmation of the establishment of a business relationship is obtained through direct personal contact, as well as, the true name, address and passport/identity card number of the customer, from a credit institution or a financial institution with which the customer cooperates; or

iii. Communication via video call with the customer, provided, the video recording and screenshot safeguards, apply to the communication.

The Company always requires its customers to submit information particularly on the SOFs. If the customer declares information that are not in line with his economic profile and/or when the customer performs a total number of deposits equal or over a specific threshold, the Company might request proof of source of funds for further examination. In addition, Company search on the website for registered companies is done to ensure that the corporate or other business applicant is an existing business entity.

10.2.5. Customer Screening

The Company utilises World Check to aid in the automated screening of clients, in order to detect and assess whether the client is subject to EU/UN and international sanctions, politically exposed person (PEP), convicted or suspected criminal.

The Company ensures that the screening system is appropriate to the nature, size and ML/TF risks of the Company. Screening is performed on clients before:

a) The establishment of a business relationship;
b) The provision of any services;
c) Undertaking any transactions for a customer.

Thereafter, monitoring is undertaken on an ongoing basis for customers and customers' related entities, directors and beneficial owners. Further to this the Company ensures:

- That customer data used for ongoing screening is up to date and correct;
- That there is a full understanding of the capabilities and limits of the automated screening system.
- That the automated screening system can be tailored to be in line with he Company's risk appetite and perform regular reviews of the calibration and rules to ensure its effective operation.

The Company has implemented controls that require referral to the AMLCO prior to dealing with flagged persons.

Upon identification of a match using World Check, the Back-Office staff investigate the potential match to ascertain if it is an actual match to the client or if it is a false positive. If a potential match is found, Back-Office staff refer to the AMLCO for further direction. The AMLCO will:

- Notify senior management;
- Freeze accounts where appropriate and where an actual target match is identified;
- Keep a clear, documented audit trail of the investigation of potential target matches and the decisions and actions taken, such as the rationale for deciding that a potential target match is a false positive.

10.2.6. Construction of an economic profile

The construction of the customer's economic profile needs to include/follow the principles below:

(a) The Company shall be satisfied that it's dealing with a real person and, for this reason, the Company shall obtain sufficient evidence of identity to verify that the person is who he claims to be. Furthermore, the Company shall verify the identity of the BO(s) of the customers' accounts. In the cases of legal persons, the Company shall obtain adequate data and information so as to understand the ownership and control structure of the customer. Irrespective of the customer type (e.g., natural or legal person, sole trader or partnership), the Company shall request and obtain sufficient data and information regarding the customer business activities and the expected pattern and level of transactions. However, it is noted that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative;

(b) The verification of the customers' identification shall be based on reliable data and information issued or obtained from independent and reliable sources, meaning those data, and information that are the most difficult to be amended or obtained illicitly;

(c) A person's residential and business address will be an essential part of his identity;

(d) The Company shall never use the same verification data or information for verifying the customer's identity and verifying its home address;

(e) The data and information that are collected before or during the establishment of the business relationship, with the aim of constructing the customer's economic profile and, as a minimum, shall include the following:

- the purpose and the reason for requesting the establishment of a business relationship;
- the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments;
- the customer's size of wealth and annual income and the clear description of the main business/professional activities/operations.

(f) The data and information that are used for the construction of the customer – legal person's economic profile shall include, inter alia, the following:

- the name of the company;
- the country of its incorporation;
- the head offices address;
- the names and the identification information of the BOs;
- the names and the identification information of the Directors;
- the names and the identification information of the authorized signatories;
- financial information;
- The ownership structure of the group that the customer – legal person may be a part of (*country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information*).

  The said data and information are recorded in a separate form designed for this purpose which is retained in the customer's file along with all other documents as well as all internal records of meetings with the respective customer. The said form is updated regularly or whenever new information emerges that needs to be added to the economic profile of the customer or alters existing information that makes up the economic profile of the customer.

(g) Identical data and information with the abovementioned shall be obtained in the case of a customer – natural person, and in general, the same procedures with the abovementioned shall be followed;

(h) Customer transactions transmitted for execution, shall be compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the customer and the data and information kept for the customer's economic profile. Significant deviations are investigated and the findings are recorded in the respective customer's file. Transactions that are not justified by the available information on the customer, are thoroughly examined so as to determine whether suspicions over ML or TF arise for the purposes of submitting an internal report to the CO or alternate to the CO.

For the purposes of the provisions relating to identification procedures and CDD requirements, proof of identity is satisfactory if:

(a) it is reasonable possible to establish that the customer is the person he claims to be, and,
(b) The person who examines the evidence is satisfied, in accordance with the procedures followed under the relevant legislations and regulations, that the customer is actually the person he claims to be.

The construction of the customer's economic profile according to the provisions above shall be undertaken by the CO or alternate to the CO. In this respect, the data and information collected for the construction of the economic profile shall be fully documented and filed.

In addition to the principles described above, the Company, and specifically the CO or alternate to the CO shall:

(a) ensure that the customer identification records remain completely updated with all relevant identification data and information throughout the business relationship;
(b) examine and check, on a regular basis, the validity and adequacy of the customer identification data and information that he maintains, especially those concerning high risk customers.

Despite the obligation described above and while taking into consideration the level of risk, if at any time during the business relationship, the Company becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the customer, then the Company shall take all necessary action, by applying the CDD procedures according to the

Manual, to collect the missing data and information, the soonest possible, so as to identify the customer and update and complete the customer's economic profile.

If, during the business relationship, a customer fails or refuses to submit, within a reasonable timeframe, and no later than 2 weeks, the required verification data and information, the Company shall terminate the business relationship and closes all the accounts of the customer while at the same time shall examine whether it is justified under the circumstances to submit a report to the FIU.

10.2.6.1. Failure or refusal to submit information for CDD

Failure or refusal by a customer to submit, before or during the establishment of a business relationship or the execution of a one-off transaction, the requisite data and information for the verification of his identity and the creation of his economic profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the customer is involved in ML or terrorist ML. In such an event, the Company shall not proceed with the establishment of the business relationship or the execution of the one-off transaction while at the same time the CO or alternate to the CO considers whether it is justified under the circumstances to submit a report to the FIU.

If, before or during the business relationship, a customer fails or refuses to submit, within a reasonable timeframe, and no longer than 2 weeks, the required verification data and information the Company and the CO or alternate to the CO shall terminate the business relationship and close all the accounts of the customer, taking also into account the specific circumstances of the customer in question and the risks faced by the Company on possible ML and/or TF, while at the same time examine whether it is justified under the circumstances to submit a report to FIU.

10.2.7. Customer approvals

Approval of Account is subject to the following terms and conditions:

a. The customer Onboarding Form is filled in completely;
b. The Terms and Conditions/ Client Service Agreement along with the rest of the legal documentation available on the Company's website are reviewed and duly acknowledged by the customer;

c. Clear photocopy of a valid ID with photo of the customer is obtained;
d. All KYC/DD documentation requested during the onboarding stage is provided;
e. Sufficient background check is conducted by our compliance team.

All applications are carefully examined by the CO or alternate to the CO, to ensure that all required information/ documents are gathered. The CO or alternate to the CO must verify the following:

i. The completeness of the required agreement/identification documents;
ii. The correctness, authenticity and completeness of the information provided by the applicant;
iii. The creditworthiness of the applicant, through a database search whenever this deems necessary;
iv. The probability that the applicant is involved in illegal or criminal activities; and
v. Reject all applications that do not include all the necessary information.

10.3. Enhanced Due Diligence Procedures

In addition to the customer due diligence measures required under section 41 of the AML and CFT Act, 2020, apply on a risk-sensitive basis enhanced customer due diligence measures and enhanced ongoing monitoring in any other situation which by its nature presents a higher risk of Money laundering, terrorist financing activities or other criminal conduct, or in respect of a business relationship with persons from, and transactions in, countries which do not apply or fully apply the Financial Action Task Force while assessing whether there is a high degree of risk of money laundering or terrorist financing in a particular situation, and the extent to which it is appropriate to apply enhanced customer due diligence measures in that situation, the company shall take into account specific risk factors including, amongst others:

i. customer risk factors, including whether the —
    a) business relationship is conducted in unusual circumstances;
    b) customer is a resident or is transacting in a geographical area of high risk;
    c) customer is a legal person or legal arrangement that is a vehicle for holding personal assets;

d) customer or potential customer, is a politically exposed person as per section 36 of the AML and CFT Act, 2020;
e) customer is a company that has nominee shareholders or shares in bearer form; customer is a business that is cash intensive;
f) corporate structure of the customer is unusual or excessively complex given the nature of the company's business;
g) customer is a foreign financial institution or non-bank financial institution;
h) customer is a non-profit organisation (hereinafter referred to as the NPO);
i) customer is a professional service provider; and customer is a or is associated with a high net worth individual.

ii. product, service, transaction or delivery channel risk factors, including whether the —
a) payments are being received from unassociated third parties;
b) service involves the provision of directorship services or nominee shareholders;
c) situation involves non-face-to-face business relationship or transactions without the necessary safeguards, specified by relevant supervisory authorities through the directions or guidelines;
d) situation involves reliance on regulated person under section 42 of the Act;
e) product involves private banking; product or transaction is one which might favour anonymity;
f) new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products;
g) product or service enables significant volumes of transactions to occur rapidly;
h) product or service allows the customer to engage in transactions with minimal oversight by the institution;
i) product or service has a high transaction or investment value; and
j) product or service has unusual complexity.

iii. geographical risk factors, includes —
a) the countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter the money laundering or terrorist financing activities;

b) the countries identified by credible sources such as mutual evaluations, detailed assessment reports or published follow up reports, as having significant levels of corruption or other criminal activity, such as terrorist financing activities, money laundering and the production and supply of illicit drugs; the countries subjected to sanctions, embargos or similar measures issued by the European Union or the United Nations and countries that feature on non-compliant lists (black and grey lists);
c) the countries providing funding or support for terrorism or have designated terrorist organisations operating within their country; and
d) other countries identified by the company as higher-risk because of its prior experiences or other factors.

Where the company applies enhanced customer due diligence, in addition to retaining sufficient information in order to demonstrate that the particular business relationship or transaction presents a higher degree of risk of money laundering and terrorist financing, it shall:

i. adjust the extent, or type of measures it undertakes to reflect the higher risk identified; and
ii. carry out enhanced on-going monitoring of any business relationship or transactions which are subject to those measures to enable it to identify any unusual or suspicious activities or transactions.

Enhanced customer due diligence measures required includes:

i. Automated scanning via Sanctions and PEP lists (e.g. WORLD-CHECK/COMPLIANCE-based automated application).
ii. If in doubt for the genuineness of any document (passport, identity card or any other documentary evidence) the Company may seek verification of identity from an Embassy or the consulate of the issuing country or a reputable credit or financial institution situated in the applicant's country of residence.
iii. taking adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or one-off transaction;
iv. seeking additional independent, reliable sources, to verify information provided or made available to the Company;

v. taking additional measures to understand the background, ownership and financial situation of the customer and other parties to the transaction;
vi. taking further steps to satisfy that the transaction is consistent with the purpose and intended nature of the business relationship;
vii. increasing the monitoring of the business relationship, including greater scrutiny of transactions; and
viii. applying such other measures provided in the guidelines issued by the respective supervisory authorities to identify the higher risk of money laundering, terrorist financing activities or other criminal conduct.

In the case, where the customer is an NPO associated with a high-risk jurisdiction or in any other case which by the nature of its activities may present a higher risk of money laundering and terrorist financing or any other criminal conduct, the company shall determine —

i. that the NPO is properly licensed or registered;
ii. the adequacy of the NPO's anti-money laundering and countering the financing of terrorism policies, procedures and controls; the NPO's legal, regulatory and supervisory status including requirements relating to regulatory disclosure, accounting, financial reporting and audit;
iii. the NPO's ownership and management structure, to include the possibility of politically exposed person's involvement;
iv. the nature and scope of the NPO's activities, nature of its donor base, and the beneficiaries of its activities and programs; and
v. thorough background checks on the NPO's key persons, senior management, branch or field managers, major donors and major beneficiaries and to screen for possible matches with targeted and other international financial sanctions lists, indications of criminal activity or any other adverse information.

10.3.1. High Risk Customers – Politically Exposed Persons

The Company will have a risk management system in place to determine if prospective or existing customers are PEPs thus shall conduct regular searches and checks for this purpose.

10.3.1.1. Measures to identify PEP

A politically exposed person means:

i. an individual who is or has been, during the preceding three years, entrusted with a prominent public function in:
    a) Seychelles; or
    b) any other country; or
    c) an international body or organisation;
ii. an immediate family member of a person referred to in paragraph (i); or
iii. a close associate of a person referred to in paragraph (i).

For the purposes of subsection (i) above, prominent public function includes —

a) heads of state, heads of government, ministers and other senior politicians;
b) senior government or judicial officials;
c) ambassadors and chargés d'affaires;
d) persons appointed as honorary consuls;
e) high-ranking officers in the armed forces;
f) members of the Boards of Central Banks;
g) members of the Boards of state-owned corporations; and
h) influential political party officials.

For the purposes of subsection (ii) above, immediate family member of a person specified in paragraph includes —

a) a spouse;
b) a partner, that is an individual considered by his or her national law as equivalent to a spouse;
c) children and their spouses or partners
d) parents; and
e) siblings.

For the purposes of subsection (iii) above, close associates of a person include —

a) any person who is known to have joint beneficial ownership of a legal person, partnership, trust or any other close business relations with that legal person, partnership or trust; and

b) any person who has sole beneficial ownership of a legal person, partnership or trust which is known to have been set up for the benefit of that legal person, partnership or trust.

In determining whether a person is a close associate of a person specified in subsection (iii) above, the company shall have regard to public information or such information that the company has in its possession including compliance-based automated application (e.g., Worldcheck).

10.3.1.2. Procedures when dealing with PEPS

For the purpose of subsection (iii), the Company shall, in addition to the measures provided in section 35 (1) of the AML and CFT Act, 2020 —

a) obtain the approval of the CEO before a business relationship is established with the customer;
b) take adequate measures to establish the source of wealth and source of funds when the client has reached the equivalent of 10,000 USD which are involved in the proposed business relationship or one-off transaction;
c) where the business relationship is entered into, conduct enhanced ongoing monitoring of the relationship; or apply such other measures provided for in the guidelines issued by the FIU or respective supervisory authority to compensate for the higher risk of money laundering, terrorist financing activities or other criminal conduct.

10.3.2. Enhanced customer scrutiny and rejection

Based on the risk, the Company shall analyse any logical inconsistencies in the information or behavior of its customers. If a potential or existing customer either refuses to provide the information described in the above chapters, or appears to have intentionally provided misleading information, a new account will not be opened and, after evaluating the risks involved, will consider closing any existing account.

CDD of existing customers shall be updated and/or amended every year for high-risk clients, every two (2) years for medium risk clients and every three (3) years for low-risk clients. This refers to change of residential or business address, new identification cards, new passport, additional business information, new business securities/venture, and the like. For any change

of information before the said period the Company requests a letter or document pertaining to the changes being made.

Bearing in mind the KYC principle, the Company shall be in a position of no-doubt or no suspicions that the identities of its customers are questionable after careful evaluation of all identification documents submitted. This shall be very important where the customer is a non-resident and therefore more probing must be done on the purpose of the transaction and the sources of funds, especially if it involves a significant amount, except when such customer is a long-established and well-known customer.

Once an account is opened for a customer, particular care shall be taken in cases where instructions for transactions on behalf of said customer is being made by a third party, such party must be formally authorized by the customer account to make such transactions on his behalf. The company shall require the necessary documents such as SPA or duly signature-verified authorization given by customers; e.g., authorized to place an order; up to what amount; and authorized to get the withdrawal.

The Company shall establish whether the applicant for business relationship is acting on behalf of another person as trustee, nominee or agent. The Company shall obtain authorized evidence of the identity of such agents (the same documents needed as enumerated above) and authorized signatories, and the nature of their trustee or nominee capacity and duties. In cases where a potential customer insists for confidentiality reasons, a numbered account may be opened.

Confidential numbered accounts shall not function as anonymous accounts; however, they shall be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence.

Shell companies are legal entities which have no business substance in their own right however through which financial transactions may be conducted. It is the policy of the Company to always be cautious when dealing with these companies as these are often abused by money launderers.

In addition to the requirements about corporation, the Company shall require a Board of Directors' certification as to the purpose(s) of the owners/stockholders in acquiring the shell company. There must be satisfactory evidence of the identities of the beneficial owners bearing in mind the KYC principle.

As a policy, the Company do not allow named account holders to transact for non-account holders and should therefore exercise special care and vigilance. Where transactions involve significant amounts, the customer should be asked to produce competent evidence of identity including nationality, the purposes of the transaction, and the sources of the funds. The company shall document its verification, including all identifying information provided by the customer, the methods used and results of the verification.

10.4. Changes to the Customer status and operations

The Company shall check the adequacy of the data and information of the customer's identity and economic profile, whenever one of the following events or incidents occurs:

(a) An important transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the economic profile of the customer;

(b) A material change in the Customer's legal status and situation, such as:

i. change of directors/secretary;
ii. change of registered shareholders and/or BOs;
iii. change of registered office;
iv. change of trustees;
v. change of corporate name and/or trading name;
vi. change of the principal trading partners and/or undertaking of major new business activities.

(c) A material change in the way and the rules the Customer's account operates, such as:

i. change in the persons that are authorized to operate the account;

ii. application for the opening of a new account for the provision of new securities services and/or securities.

In addition to the above, the Company, when making transfers of money between customers' accounts, shall apply the following procedures, as applicable:

(a) Ask, from both customers directly involved (*originator of the transfer and recipient of the transfer*), to complete a form of order and acceptance of the money transfer between the customers' accounts;

(b) Before performing the money transfer, the responsible, for this purpose, person (*e.g. Finance and Treasury Manager*) shall confirm the order and acceptance of the money transfer by telephone or by other equivalent method. If the confirmation is made by telephone, the telephone communication shall be recorded;

(c) The CO or alternate to the CO shall:

i. verify the authenticity of the signatures on the aforementioned form;

ii. record (e.g. on the form) the reasons and confirm the legality of the purpose for which the transfer of money is made;

iii. keep all records and information related to this purpose in the involved customers' files.

10.5. CDD procedures (specific cases)

The CO or alternate to the CO shall ensure that the appropriate documents and information with respect to the following cases shall be duly obtained, as applicable and appropriate:

<u>For Natural Persons</u>

The Company shall obtain the following information to ascertain the true identity of the natural persons:

(a) true name and/or names used as these are stated on the official identity card or passport;

(b) full permanent address;

(c) telephone (home and mobile);

(d) e-mail address, if any;

(e) date and place of birth;

(f) nationality; and

(g) Details of the profession and other occupations of the customer including the name of employer/business organisations.

In order to verify the customer's identity/name the Company shall request the customer to present an original document which is issued by an independent and reliable source that carries the customer's photo (e.g. Passport, National Identity card, Driving License, etc.). After the Company is satisfied for the customer's identity from the original identification document presented, it will keep copies.

It is provided that, the Company shall be able to prove that the said document is issued by an independent and reliable source. In this respect, the CO or alternate to the CO shall be responsible to evaluate the independence and reliability of the source and shall duly document and file the relevant data and information used for the evaluation, as applicable.

The customer's residential address shall be verified using the production of a recent (*up to three (3) months*) utility bill, local authority tax bill or a bank statement or any other document same with the aforesaid (*to protect against forged or counterfeit documents, the prospective Customers are required to produce original documents*).

In addition to the above, the procedure for the verification of a customer's identity is reinforced if the said customer is introduced by a reliable staff member of the Company, or by another existing reliable customer who is personally known to a member of the Board. Details of such introductions are kept in the customer's file.

The Company shall also require and receive information on public positions which the prospective customer holds or held in the last twelve (12) months as well as whether he is a close relative or associate of such individual, in order to verify if the Customer is a PEP.

Third Party Reliance

When dealing with third parties to undertake the Company's obligations to introduce business, the Company shall perform the following procedures:

i. immediately obtain the information required;
ii. ensure that copies of identification data and other relevant documentation relating to the requirements will be made available to it from the third party upon request without delay; and
iii. Satisfy that the third party or intermediary is regulated and supervised for, and has measures in place to comply with, the requirements set out in sections 5, 6 and 7 of the AML and CFT Act, 2020.

Cross Border Correspondent Banking and Other Similar Relationships

Procedures for cross border correspondent banking and other similar relationships:

i. adequately identify and verify the identity of the person with whom it conducts such a business relationship;
ii. gather sufficient information about the nature of the business of the person;
iii. determine from publicly available information the reputation of the person and the quality of supervision to which the person is subject;
iv. assess the person's AML/CFT controls;
v. obtain approval from the Board before establishing a new correspondent relationship;
vi. document the responsibilities of the company and the person;
vii. Where the relationship is a payable-through account, the company shall ensure that the person with whom or with which it has established the relationship—
    a. has verified the identity of and performed on-going due diligence on such of that person's customers as have direct access to accounts of the company;
    b. is able to provide the relevant customer identification data upon request to the company; and
    c. has a physical presence in the Republic under the law under which it is established unless it is a part of a group that is subject to supervision as a whole.

Joint Accounts

In the cases of joint accounts of two or more persons, the identity of all individuals that hold or have the right to manage the account, are verified according to the procedures set for natural persons herein.

Unions, Societies, Clubs, Provident Funds and Charities

In the case of accounts in the name of unions, societies, provident funds and charities, the Company ascertains their purpose of operation and verifies their legitimacy by requesting the production of the articles and memorandum of association/procedure rules and registration documents with the competent governmental authorities (in case the law requires such registration).

Furthermore, the Company shall obtain a list of the members of board of directors/management committee of the abovementioned organisations and verifies the identity of all individuals that have been authorized to manage the account according to the procedures set for natural persons herein.

Unincorporated Businesses, Partnerships and Other Persons with No Legal Substance

In the case of unincorporated businesses, partnerships and other persons with no legal substance, the identity of the directors, partners, BOs and other individuals who are authorized to manage the account shall be verified according to the procedures set for natural persons herein.

In addition, in the case of partnerships, the original or a certified true copy of the partnership's registration certificate shall be obtained.

The Company shall obtain documentary evidence of the head office address of the business, ascertains the nature and size of its activities and receives all the information required according to section for the creation of the economic profile of the business.

The Company shall request, in cases where exists, the formal partnership agreement and shall also obtain mandate from the partnership authorizing the opening of the account and confirming authority to a specific person who will be responsible for its operation.

11. On-going Monitoring

The Company has a full understanding of normal and reasonable account activity of its customers as well as of their economic profile and has the means of identifying transactions which fall outside the regular pattern of an account's activity or to identify complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason. Without such knowledge, the Company shall not be able to discharge its legal obligation to identify and report suspicious transactions to the FIU.

The constant monitoring of the customers' accounts and transactions is an imperative element in the effective controlling of the risk of ML and TF. In this respect, the CO or alternate to the CO, shall be responsible for maintaining as well as developing the on-going monitoring process of the Company. The Internal Auditor shall review the Company's procedures with respect to the on-going monitoring process, at least annually.

The CO or alternate to the CO shall implement a RBA for the on-going monitoring procedures of the Company, which is based on, inter alia, the customers' risk categorization and the volume of transactions estimated in the pre-account information provided. Relevant employees perform reviews of customers' transactions at least once a week, or otherwise if requested by the CO or his alternate, and reports to the CO or alternate to the CO; their finding for the purposes of the on-going monitoring of the Company. The responsible employee shall also provide daily records of customers' incoming and outgoing money transfers, to the CO or alternate to the CO.

The CO or alternate to the CO, monitors and ensures, on a frequent basis, that the actual amount of funds deposited by customers is consistent with the amount of funds indicated during the customer account opening stage, as well as with the economic profile of the customer.

Additionally, all employees must be alerted to detect and report internally any activity on the customer's account or behavior, which is inconsistent with the previously disclosed/obtained information. Employees must inform accordingly the CO or alternate to the CO.

11.1. Procedures

The procedures and intensity of monitoring customers' accounts and examining transactions on the customer's level of risk shall include the following:

(a) The identification of –

- ✓ all high-risk customers, as applicable, the Company shall be able to produce detailed lists of high-risk customers, so as to facilitate enhanced monitoring of accounts and transactions, as deemed necessary;
- ✓ transactions which, as of their nature, may be associated with ML or TF;
- ✓ unusual or suspicious transactions that are inconsistent with the economic profile of the customer for the purposes of further investigation;
- ✓ in case of any unusual or suspicious transactions, the head of the department providing the relevant Securities and Dealing Services;
- ✓ or any other person who identified the unusual or suspicious transactions as well as the Dealing and Operations Manager shall be responsible to communicate with the CO or alternate to the CO.

(b) Further to point (a) above, the investigation of unusual or suspicious transactions by the CO or alternate to the CO. The results of the investigations are recorded in a separate memo and kept in the file of the customers concerned.

(c) The ascertainment of the source and origin of the funds credited to accounts.

(d) The on-going monitoring of the business relationship in order to determine whether there are reasonable grounds to suspect that customer accounts contain proceeds derived from serious tax offences.

(e) The use of appropriate and proportionate IT systems, including:

- ✓ adequate automated electronic management information systems which will be capable of supplying the Board and the CO or alternate to the CO, on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of customer accounts and transactions based on the assessed risk for ML or TF purposes, in view of the nature, scale and complexity of the Company's business and the nature and range of the securities services undertaken in the course of that business;

- ✓ automated electronic management information systems to extract data and information that is missing regarding the customer identification and the construction of a customer's economic profile;
- ✓ for all accounts, automated electronic management information systems to add up the movement of all related accounts on a consolidated basis and detect unusual or suspicious activities and types of transactions. This can be done by setting limits for a particular type, or category of accounts (e.g., high risk accounts) or transactions (e.g. deposits and withdrawals in cash, transactions that do not seem reasonable based on usual business or commercial terms, significant movement of the account incompatible with the size of the account balance), taking into account the economic profile of the customer, the country of his origin, the source of the funds, the type of transaction or other risk factors. The Company shall pay particular attention to transactions exceeding the abovementioned limits, which may indicate that a customer might be involved in unusual or suspicious activities.

(f) The monitoring of accounts and transactions shall be carried out in relation to specific types of transactions and the economic profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the business relationship. Furthermore, the monitoring covers customers who do not have a contact with the Company as well as dormant accounts exhibiting unexpected movements.

(g) The monitoring of accounts held by customers' whose identity was verified via the use of video communication.

(h) The monitoring on ongoing basis of the transactions of low-risk customers to ensure that there are no suspicious transactions.

12. Recognition and reporting of suspicious transactions

12.1. Suspicious Transactions

The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for ML and TF are almost unlimited. A suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the Company has created for the customer.

The Company shall ensure that it maintains adequate information and knows enough about its customers' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.

Examples of what might constitute suspicious transactions related to ML and TF are listed in Appendix 3 of the Manual. The relevant list is not exhaustive nor it includes all types of transactions that may be used, nevertheless it can assist the Company and its employees (especially the CO or alternate to the CO and the Dealing and Operations Manager) in recognizing the main methods used for ML and TF.

The detection by the Company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity.

In order to identify suspicious transactions, the CO or alternate to the CO shall perform the following activities:

- Monitor on a continuous basis any changes in the customer's financial status, business activities, type of transactions etc.;
- Monitor on a continuous basis if any customer is engaged in any of the practices described in the list containing examples of what might constitute suspicious transactions related to ML and TF which is mentioned in Appendix 3 of this Manual.

Furthermore, the CO or alternate to the CO shall perform the following activities:

- Receive and investigate information from the Company's employees, on suspicious transactions which creates the belief or suspicion of ML or TF. This information is reported on the internal STR. The said reports are archived by the CO or alternate to the CO;
- Evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchanging of information

in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the CO or alternate to the CO, is evaluated on the Internal Evaluation Report, which is also filed in a relevant file;

- If, as a result of the evaluation described above, the CO or alternate to the CO decides to disclose this information to the FIU, then he prepares a written report, which he submits to the FIU;
- If as a result of the evaluation described above, the CO or alternate to the CO decides not to disclose the relevant information to the FIU, then he shall fully explain the reasons for his decision on the Internal Evaluation Report.

12.2. Reporting of Suspicious Transactions

As a general internal control procedure, directors, officers, agents and staff of the company shall report any knowledge or suspicion of ML or TF activity to the CO or alternate to the CO. The report should be formally transmitted either in hard copy report, memoranda or note, or via electronic means (*inter-office email*). Use of external emails in transmitting the report is prohibited. Ensure no one else is provided a copy (*including blind copies*). Failure to comply with such requirement exposes the reporting personnel to breach of confidentiality in violation of the AML and CFT Act, 2020.

In line with this requirement, all personnel will be required to sign a statement on breach of confidentiality provision of the AML and CFT Act, 2020. A copy of this signed statement will be filed together with the personnel file.

After thorough evaluation and reasonable belief that there is really a basis for suspicion of ML or TF, the CO or alternate to the CO shall maintain a register of all reports made to the authorities as well as all reports made by the staff of the Company relative to suspicious transactions, whether or not such were reported to the FIU or other relevant authorities.

Notwithstanding, the duties of the CO or alternate to the CO as reporting officer; the ultimate responsibility for proper supervision, reporting and compliance with the AML and CFT Act, 2020 and implementing rules and regulations, shall rest with the company and its Board.

The Company; its directors and employees, are not allowed to disclose to the customer or third parties the fact that information on suspicious transactions has been transmitted, is being transmitted or will be transmitted to the FIU or that there is or that an analysis of such information or suspicious transactions can be carried out in relation to ML or TF.

The company shall institute a system for the mandatory reporting of suspicious transactions by appointing a CO or alternate to the CO. Reporting of covered and suspicious transactions shall be done by the CO or alternate to the CO within 48 hours of having form the suspicion or in any event as soon as it is practicable.

No person is allowed to make any disclosure that may interfere with, or adversely affect, inquiries and inquiries conducted on the calibration of revenue or the commission of specified offenses, knowing or suspecting that the above investigations are being conducted and surveys.

12.3. Submission of information to the FIU

The Company shall ensure that in the case of a suspicious transaction investigation by the FIU, the CO or alternate to the CO, will be able to provide without delay the following information:

a) the identity of the account holders;
b) the identity of the BOs of the account;
c) the identity of the persons authorized to manage the account;
d) data of the volume of funds or level of transactions flowing through the account;
e) connected accounts;
f) in relation to specific transactions:
    - the origin of the funds;
    - the type and amount of the currency involved in the transaction;
    - the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers;
    - the identity of the person that gave the order for the transaction;
    - the destination of the funds;
    - the form of instructions and authorization that have been given;
    - the type and identifying number of any account involved in the transaction.

The company shall register or maintain a complete file on all covered and suspicious transactions that have been brought to the attention of the CO or alternate to the CO. The register shall contain details of:

i. the date on which the report is made;
ii. the person who made the report to the CO or alternate to the CO;
iii. information sufficient to identify the relevant papers related to said reports.

12.4. Protection of person reporting

Bona fide disclosure of information by the Company or by an employee or director of the Company does not constitute a breach of any contractual or statutory, regulatory or administrative prohibition of disclosure of information, nor implies any liability for the Company or its directors or employees, even if the circumstances did not allow them to know precisely what the main illegal activity was and regardless of whether it was actually committed Illegal activity.

Persons who submit an internal STR or report to the FIU for suspicious transactions shall be protected against any threat or hostile action and in particular by adverse acts or discrimination in the workplace as per sections 13 and 14 of the AML and CFT Act, 2020.

12.5. Disclosure in Good Faith

Disclosure of information in good faith by the Company or by an employee or director of the Company, shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the Company or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether the illegal activity actually occurred.

12.6. Prohibition from carrying out Suspicious Transactions

The Company shall refrain from carrying out transactions which it knows or suspects to be related with ML or TF, before it informs the FIU of its suspicion. In case it is impossible to refrain from carrying out the transaction or is likely to frustrate efforts to pursue the person of a suspected ML or TF operation, the Company, must inform the FIU immediately afterwards.

13. Record Keeping Procedures

Records will be kept for all documents obtained for the purpose of customer identification (KYC policy requirements) and all data of each transaction, as well as other information related to ML or TF matters in accordance with the applicable AML laws/regulations. That includes files on STRs, documentation of AML account monitoring, etc.

Transaction effected via the Company can be reconstructed, from which the authorities will be able to compile an audit trail for suspected ML or TF, when such a report is made to it. The Company can satisfy within a reasonable time any inquiry or order from the authorities as to disclosure of information, including without limitation whether a particular person is the customer or BO of transactions conducted through the Company. The following document retention periods will be followed:

i All documents in opening the accounts of customers and records of all their transactions, especially customer identification records, shall be maintained and safely stored for seven (7) years from the dates of transactions;

ii With respect to closed accounts, the records on customer identification, account files and business correspondence, shall be preserved and safely stored for at least seven (7) years from the dates when they were closed.

The following records must be kept:

i Copies of the evidential material of the customer identity;

ii Any non-documentary verification methods or additional methods used to verify;

iii Relevant evidential material and details of all business relations and transactions, including documents for recording transactions in the accounting books (the form and SOF and/or securities used by the applicant for business; the form and destination of funds paid or delivered to the applicant for business or another person on his behalf; financial transactions carried out by the Company with or for each customer or counterparty of the Company;

iv Relevant documents of correspondence with the customers and other persons with whom they keep a business relation;

v Description of how the company resolved all substantive discrepancies noted.

Checking and review of the documents is done by the personnel assigned to verify the accuracy and completeness of the records maintained by the company. It is important that any material irregularity or documents lacking are noted and reported for immediate correction.

Transaction documents may be retained as originals or copies, on microfilm, or in electronic form, provided that such forms are admissible in court.

If the records relate to on-going investigations or transactions that have been the subject of a disclosure, they shall be retained beyond the stipulated retention period until it is confirmed that the case has been closed and terminated.

14. Employees' obligations, education and training

The Company shall provide the necessary training, as well as orientation to its employees, officers, agents and CO or alternate to the CO. The Company disseminates to the staff the new procedures and guidelines needed in combating ML and TF. The officers and staff are sent to orientations, training and seminars being offered by the regulatory bodies.

The company also educate staff in the KYC requirements on the prevention and detection of ML and TF. Staff will therefore be trained in the true identity of customers and the type of business relationship being established.

The company shall determine the extent of training/orientation of its personnel with the priority being given to the CO or alternate to the CO who would be directly exposed to situations involving ML and TF activities. Scope of training is on the following:

i Provisions of the AML and CFT Act, 2020 and regulations;
ii The Company's AML/CFT Manual and Policy;
iii The Company's Internal Supervision, Control, and Compliance Procedures;
iv Updates and changes on the AML and CFT Act, 2020 and regulations;
v Updates and changes on Internal Supervision, Control, and Compliance Procedures.

Refresher training or orientations shall be made from time to time to constantly remind key staff of their responsibilities or if there are changes in the laws and rules in ML and TF. The training shall be conducted at least once per quarter at minimum.

15. Test of the AML Policy

The Company will hire an independent, qualified party to provide an annual independent audit of its AML policies and procedures, and the compliance with said procedures. The Company will perform written follow-up to ensure that any deficiencies noted during its annual review are addressed and corrected.

16. Prohibited Countries Register

This register consolidates jurisdictions designated as high-risk or prohibited based on the following sources:

- FATF Blacklist (High-Risk Jurisdictions subject to a Call for Action).
- FATF Grey List (Jurisdictions under Increased Monitoring).
- United Nations Security Council sanctions and embargoes.
- Comprehensive embargoes or prohibitions under EU, OFAC (US), or regional treaties.

The Company shall not establish or maintain business relationships with any counterparty in the Prohibited category. Grey-listed jurisdictions may only be onboarded subject to Enhanced Due Diligence (EDD), senior management approval, and enhanced monitoring.

Jurisdiction	**Source of Prohibition / Monitoring**	**Status**	**Effective Date**	**Notes / Mitigation Actions**
North Korea (DPRK)	FATF Black List; UN Sanctions	Absolute Prohibition	13/06/2025	All business strictly

				prohibited
Iran	FATF Black List; UN Sanctions; EU/OFAC embargo	Absolute Prohibition	13/06/2025	All business strictly prohibited
Myanmar (Burma)	FATF Black List; EU/OFAC measures	Absolute Prohibition	13/06/2025	All business strictly prohibited
Somalia	UN Security Council sanctions	Absolute Prohibition	13/06/2025	All business strictly prohibited
Libya	UN Security Council sanctions	Absolute Prohibition	13/06/2025	All business strictly prohibited
Sudan	UN Security Council sanctions	Absolute Prohibition	13/06/2025	All business strictly prohibited
South Sudan	UN Security Council sanctions	Absolute Prohibition	13/06/2025	All business strictly prohibited
Central African Republic	UN Security Council sanctions	Absolute Prohibition	13/06/2025	All business strictly prohibited
Democratic Republic of Congo	UN Security Council sanctions	Absolute Prohibition	13/06/2025	All business strictly prohibited
Mali	UN Security Council sanctions	Absolute Prohibition	13/06/2025	All business strictly prohibited
Yemen	UN Security Council sanctions	Absolute Prohibition	13/06/2025	All business strictly prohibited
Syria	UN Security Council sanctions; EU/OFAC embargo	Absolute Prohibition	13/06/2025	All business strictly prohibited
Russia	EU/OFAC/G7 sanctions	Absolute Prohibition	13/06/2025	All business strictly prohibited
Belarus	EU/OFAC sanctions	Absolute Prohibition	13/06/2025	All business strictly prohibited
Cuba	OFAC comprehensive embargo	Absolute Prohibition	13/06/2025	All business strictly

				prohibited
Venezuela	OFAC/EU sanctions	Absolute Prohibition	13/06/2025	All business strictly prohibited
Algeria	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Angola	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Bolivia	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Bulgaria	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Burkina Faso	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Cameroon	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Côte d'Ivoire	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Haiti	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Kenya	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring

Lao PDR	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Lebanon	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Monaco	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Mozambique	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Namibia	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Nepal	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Nigeria	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
South Africa	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Vietnam	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring
Virgin Islands (UK)	FATF Grey List	Restricted – EDD required	13/06/2025	EDD required, senior management approval, enhanced monitoring

17. Customer Risk Assessment Matrix

Risk Matrix - [redacted]

RISK FACTORS	CATEGORIES	SUB-CATEGORIES	SCORE POINTS	TOTAL MAX
JURISDICTION	COUNTRY OF RESIDENCE	Scoring based on Basal Scale relating to AML rating of jurisdictions.		10
CLIENT	EMPLOYMENT STATUS	Employed	2	10
		Self Employed	7	
		Student	8	
		Retired	6	
		Not Working	8	
	PEP	NO	0	15
		YES	15	
	SOURCE OF FUND INFORMATION	Employment / Business Income	2	10
		Savings and Investments	6	
		Retirement Income	4	
		Company Profit/Dividends	8	
		Inheritance	7	
		Property / Business Sale	10	
		Loans / Borrowings	9	
		Gifts	9	
		Other	5	
	NATURE OF PROFESSION	Accounting and Finance Services	8	10
		Company Service Providers	8	
		Real Estate	10	
		Pharmaceuticals and Healthcare	10	
		Arms Trade and Defence	10	
		Casinos	10	
		Legal Services	9	
		Computer Software, Internet, IT	2	
		Political Government Activities	10	
		Mathematics	0	
		Education	0	
		Financial Services	8	
		Banking	8	
		Engineering and/or Construction	8	
		Other	5	
DELIVERY CHANNEL		In Person	0	10
		Non Face to Face*	10	
FINANCIAL INFORMATION	EXPECTED DEPOSIT IN THE NEXT 12 MONTHS (USD)	0 -20,000	3	12
		20,001 - 50,0000	5	
		50,001 - 250,000	10	
		250,001 - 500,000	10	
		500,001 - 1,000,000	10	
		More than 1,000,000	12	
	ANNUAL ESTIMATED INCOME (USD)	Less than 50,000	2	12
		50,001 – 100,000	6	
		100,001 – 500,000	8	
		500,001 – 1,000,000	10	
		More than 1,000,000	12	
	TOTAL ESTIMATED NETWORTH (USD)	Less than 50,000	2	11
		50,001 – 100,000	6	
		100,001 – 500,000	8	
		500,001 – 1,000,000	10	
		More than 1,000,000	11	

CRM System will mark this scoring by default with each registration

< 70	STANDARD DUE DILIGENCE	TOTAL	100
> 70	ENHANCED DUE DILIGENCE		

SCORING	RISK LEVEL
0 - 20	LOW
21 - 70	MEDIUM
71 - 100	HIGH

APPENDIX 1 – INTERNAL SUSPICIOUS TRANSACTION REPORT FOR ML AND TF

INFORMER'S DETAILS

Name: ..... Tel: .....

Department: ..... Fax: .....

Position: .....

CUSTOMER'S DETAILS

Name: .....

Address: .....

..... Date of Birth: .....

Tel:.....Occupation:

Fax: ..... Details of Employer: .....

.....

Passport No.: ..... Nationality: .....

ID card No.: ..... Other ID Details: .....

INFORMATION/SUSPICION

Brief description of activities/transaction: .....

....

Reason(s) for suspicion: .....

Informer's Signature Date

....

FOR Compliance Officer USE

Date Received: ..... Time Received: ..... Ref.....

Reported to the Unit: Yes/No.... Date Reported: ..... Ref.....

APPENDIX 2 - INTERNAL EVALUATION REPORT FOR ML AND TF

Reference: ..... Customer's Details: .....

Informer: ..... Department: .....

INQUIRIES UNDERTAKEN (Brief Description)

.....

.....

.....

ATTACHED DOCUMENTS

.....

.....

.....

.....

Compliance Officer DECISION

.....

.....

.....

FILE NUMBER.....

Compliance Officer SIGNATURE DATE

…….…….. ……

APPENDIX 3 – EXAMPLES OF SUSPICIOUS TRANSACTIONS RELATED TO ML AND TF

A. Money Laundering

1. Transactions with no discernible purpose or are unnecessarily complex.
2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the Customer.
3. The transactions or the size of the transactions requested by the Customer do not comply with his usual practice and business activity.
4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the Customer's business activities would not appear to justify such activity.
5. The Business Relationship involves only one transaction or it has a short duration.
6. There is no visible justification for a Customer using the services of a particular financial organisations. For example, the Customer is situated far away from the particular financial organisations and in a place where he could be provided services by another financial organisations.
7. There are frequent transactions in the same securities without obvious reason and in conditions that appear unusual (churning).
8. There are frequent small purchases of a particular securities by a Customer who settles in cash, and then the total number of the securities is sold in one transaction with settlement in cash or with the proceeds being transferred, with the Customer's instructions, in an account other than his usual account.
9. Any transaction the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration.
10. Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.
11. The settlement of any transaction but mainly large transactions, in cash.
12. Settlement of the transaction by a third person which is different than the Customer which gave the order.
13. Instructions of payment to a third person that does not seem to be related with the instructor.

14. Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.
15. A Customer is reluctant to provide complete information when establishes a Business Relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with financial organisations, names of its officers and directors, or information on its business location. The Customer usually provides minimum or misleading information that is difficult or expensive for the financial organisations to verify.
16. A Customer provides unusual or suspicious identification documents that cannot be readily verified.
17. A Customer's home/business telephone is disconnected.
18. A Customer that makes frequent or large transactions and has no record of past or present employment experience.
19. Difficulties or delays on the submission of the financial statements or other identification documents, of a Customer/legal person.
20. A Customer who has been introduced by a foreign financial organisation, or by a third person whose countries or geographical areas of origin do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.
21. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc.).
22. The stated occupation of the Customer is not commensurate with the level or size of the executed transactions.
23. Financial transactions from non-profit or charitable organisations for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisations and the other parties in the transaction.
24. Unexplained inconsistencies arising during the process of identifying and verifying the Customer (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc.).

25. Complex trust or nominee network.
26. Transactions or company structures established or working with an unneeded commercial way, e.g. companies with bearer shares or bearer securities or use of a postal box.
27. Use of general nominee documents in a way that restricts the control exercised by the company's board of directors.
28. Changes in the lifestyle of employees of the financial organisations, e.g. luxurious way of life or avoiding being out of office due to holidays.
29. Changes the performance and the Behaviour of the employees of the financial organisations.

B. Terrorist Financing

1. Sources and methods

The funding of terrorist organisations is made from both legal and illegal revenue generating activities. Criminal activities generating such proceeds include kidnappings (requiring ransom), extortion (demanding "protection" money), smuggling, thefts, robbery and narcotics trafficking. Legal fund-raising methods used by terrorist groups include:

i. collection of membership dues and/or subscriptions
ii. sale of books and other publications
iii. cultural and social events
iv. donations
v. Community solicitations and fund-raising appeals.

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of securities, wire transfers by using "straw men", false identities, front and shell companies as well as nominees from among their close family members, friends and associates.

2. Non-profit organisations

Non–profit and charitable organisations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organisations can be made in the following ways:

i. Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisations.
ii. A non-profit organisation with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.
iii. The non-profit organisations serve as an intermediary or cover for the movement of funds on an international basis.
iv. The non-profit organisations provide administrative support to the terrorist movement.

Unusual characteristics of non-profit organisations indicating that they may be used for an unlawful purpose are the following:

i. Inconsistencies between the apparent sources and amount of funds raised or moved.
ii. A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisations.
iii. A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisations.
iv. Large and unexplained cash transactions by non-profit organisations.
v. The absence of contributions from donors located within the country of origin of the non-profit organisations.

APPENDIX 4 - RISK FACTOR ASSESSMENT CHEKLIST

No.	RISK'S ASSOCIATED WITH A CUSTOMER'S AND/OR A CUSTOMER'S BENEFICIAL OWNER'S BUSINESS AND/OR OR PROFESSIONAL ACTIVITY	YES	NO	COMMENTS/ REMARKS
A1	Does the Customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defense, the extractive industries or public procurement?			
A2	Does the Customer or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example certain Money Service Businesses, casinos or dealers in precious metals?			
A3	Does the Customer or beneficial owner have links to sectors that involve significant amounts of cash?			
A4	Where the Customer is a legal person or a legal arrangement, does the company know what the purpose of their establishment is? For example, what is the nature of their business?			
A5	Does the Customer have political connections, for example, are they a Politically Exposed Person (PEP), or is their beneficial owner a PEP?			
A6	Does the Customer or beneficial owner have any other relevant links to a PEP? *(Where a Customer or their beneficial owner is a PEP, the Company must always apply enhanced due diligence measures*			
55	▪ E.g. any of the Customer's directors PEPs? If so, do these PEPs exercise significant control over the Customer or beneficial owner?			

A7	Does the Customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain?			
	▪ E.g... Are they senior local or regional public officials with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or individuals who are known to influence the government and other senior decision-makers?			
A8	Is the Customer a legal person subject to enforceable disclosure requirements that ensure that reliable information about the Customer's beneficial owner is publicly available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?			
A9	Is the Customer a credit or financial institution acting on its own account from a jurisdiction with an effective AML/CFT regime and is it supervised for compliance with local AML/CFT obligations?			
	▪ If so, is there evidence that the Customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT obligations or wider conduct requirements in recent years?			
A10	Is the Customer a public administration or enterprise from a jurisdiction with low levels of corruption?			
A11	Is the Customer's or the beneficial owner's background consistent with what the Company knows about their former, current or planned business activity, their business's turnover, the source of funds and the Customer's or beneficial owner's source of wealth?			
No.	Risk's associated with a Customer's or beneficial owners' reputation	YES	NO	COMMENTS /

				REMARKS
B1	Are there adverse media reports or other relevant sources of information about the Customer, for example are there any allegations of criminality or terrorism against the Customer or the beneficial owner?			
	▪ If so, are these reliable and credible? *The Company should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations. It should be noted that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.*			
B2	Has the Customer, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing?			
	▪ Does the Company have reasonable grounds to suspect that the Customer or beneficial owner or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?			
B3	Does the Company know if the Customer or beneficial owner has been the subject of a suspicious transactions report in the past?			
B4	Does the Company have any in-house information about the Customer's or the beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?			
NO.	**RISK FACTORS MAY BE RELEVANT WHEN CONSIDERING THE RISK ASSOCIATED WITH A CUSTOMER'S OR BENEFICIAL OWNER'S NATURE AND BEHAVIOR**	**YES**	**NO**	**COMMENTS / REMARKS**

	(THE COMPANY NOTES THAT NOT ALL OF THESE RISK FACTORS WILL BE APPARENT AT THE OUTSET; THEY MAY EMERGE ONLY ONCE A BUSINESS RELATIONSHIP HAS BEEN ESTABLISHED			
C1	Does the Customer have legitimate reasons for being unable to provide robust evidence of their identity, perhaps because they are an asylum seeker?			
C2	Does the Company have any doubts about the veracity or accuracy of the Customer's or beneficial owner's identity?			
	▪ Does the Company have reasonable grounds to suspect that the Customer or beneficial owner or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?			
C3	Are there indications that the Customer might seek to avoid the establishment of a business relationship?			
	▪ E.g. does the Customer look to carry out one transaction or several one-off transactions where the establishment of a business relationship might make more economic sense?			
C4	Is the Customer's ownership and control structure transparent and does it make sense?			
	▪ If the Customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?			
C5	Does the Customer issue bearer shares or does it have nominee shareholders?			
C6	Is the Customer a legal person or arrangement that could be used as an asset-holding vehicle?			
C7	Is there a sound reason for changes in the Customer's ownership and control structure?			

C8	Does the Customer request transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale?			
C9	Does the Customer request unnecessary or unreasonable levels of secrecy?			
	▪ e.g. Is the Customer reluctant to share CDD information, or do they appear to want to disguise the true nature of their business?			
C10	Can the Customer's or beneficial owner's source of wealth or source of funds be easily explained?			
	▪ e.g. Through their occupation, inheritance or securities? Is the explanation plausible?			
C11	Does the Customer use the products and services they have taken out as expected when the business relationship was first established?			
C12	Is the Customer a non-profit organisation whose activities could be abused for terrorist financing purposes?			
NO.	**RISK FACTORS COMPANY SHOULD CONSIDER WHEN IDENTIFYING THE EFFECTIVENESS OF A JURISDICTION'S AML/CFT REGIME**	**YES**	**NO**	**COMMENTS/ REMARKS**
D1	Has the country been identified by the Commission as having strategic deficiencies in its AML/CFT regime, (*Where the Company deals with natural or legal persons resident or established in third countries that the Commission has identified as presenting a high ML/TF risk, the Company must always apply EDD measures)*			

D2	Is there information from more than one credible and reliable source about the quality of the jurisdiction's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight?			
	▪ E.g. possible sources include mutual evaluation reports by the Financial Action Task Force (FATF)) the FATF's list of high-risk and non-cooperative jurisdictions, International Monetary Fund (IMF) assessments and Financial Sector Assessment Program (FSAP) reports.			
NO.	**RISK FACTORS COMPANY SHOULD CONSIDER WHEN IDENTIFYING THE LEVEL OF TERRORIST FINANCING RISK ASSOCIATED WITH A JURISDICTION**	**YES**	**NO**	**COMMENTS/ REMARKS**
E1	Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country or territory?			
E2	Is the jurisdiction subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the United Nations or the European Union?			
NO.	**RISK FACTORS COMPANY SHOULD CONSIDER WHEN IDENTIFYING A JURISDICTION'S LEVEL OF TRANSPARENCY AND TAX COMPLIANCE**	**YES**	**NO**	**COMMENTS/ REMARKS**

F1	Is there information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards?			
	▪ Is there evidence that relevant rules are effectively implemented in practice?			
F2	Has the jurisdiction put in place reliable and accessible beneficial ownership registers?			
NO.	**RISK FACTORS THAT MAY BE RELEVANT WHEN CONSIDERING THE RISK ASSOCIATED WITH A PRODUCT, SERVICE OR TRANSACTION'S TRANSPARENCY**	**YES**	**NO**	**COMMENTS/ REMARKS**
G1	To what extent do products or services allow the Customer or beneficial owner or beneficiary structures to remain anonymous, or facilitate hiding their identity?			
	▪ E.g. such products and services include bearer shares, fiduciary deposits, offshore vehicles and certain trusts, and legal entities such as foundations that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies or companies with nominee shareholders.			
G2	To what extent is it possible for a third party that is not part of the business relationship to give instructions, for example in the case of certain correspondent banking relationships?			
NO.	**RISK FACTORS THAT MAY BE RELEVANT WHEN CONSIDERING THE RISK ASSOCIATED WITH A PRODUCT, SERVICE OR TRANSACTION'S COMPLEXITY**	**YES**	**NO**	**COMMENTS/ REMARKS**

H1	To what extent is the transaction complex and does it involve multiple parties or multiple jurisdictions, for example			
	▪ E.g. in the case of certain trade finance transactions?			
H2	To what extent do products or services allow payments from third parties or accept overpayments where this is would not normally be expected?			
	▪ Where third party payments are expected, does the Company know the third party's identity, for example is it a state benefit or guarantor?			
	▪ Or are products and services funded exclusively by fund transfers from the Customer's own account at another financial institution that is subject to AML/CFT standards and oversight.			
H3	Does the Company understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?			
NO.	**RISK FACTORS THAT MAY BE RELEVANT WHEN CONSIDERING THE RISK ASSOCIATED WITH A PRODUCT, SERVICE OR TRANSACTION'S VALUE OR SIZE**	**YES**	**NO**	**COMMENTS/ REMARKS**
I1	To what extent are products or services cash intensive, as are many payment services but also certain current accounts?			
I2	To what extent do products or services facilitate or encourage high-value transactions?			
	▪ Are there any caps on transaction values or levels of premium that could limit the use of the product or service for ML/TF purposes?			

NO.	RISK ASSOCIATED WITH THE WAY IN WHICH THE CUSTOMER OBTAINS THE PRODUCTS OR SERVICES,	YES	NO	COMMENTS/ REMARKS
J1	Is the Customer physically present for identification purposes?			
	▪ If not, has the Company used a reliable form of non-face-to-face CDD?			
	▪ Has it taken steps to prevent impersonation or identity fraud?			
I2	Has the Customer been introduced by another part of the same financial group and, if so, to what extent can the Company rely on this introduction as reassurance that the Customer will not expose the Company to excessive ML/TF risk?			
I3	Has the Customer been introduced by a third party, for example a bank that is not part of the same group, and is the third party a financial institution or is its main business activity unrelated to financial service provision?			
	▪ What has the Company done to satisfy itself that: i. the third party applies CDD measures and keeps records to the standard required			
	ii. the third party will provide, immediately upon request, relevant copies of identification and verification data,			
	iii. The quality of the third party's CDD measures is such that it can be relied upon?			
I4	Has the Customer been introduced through a tied agent, that is, without direct Company contact?			

	▪ Can the Company be satisfied that the agent has obtained enough information so that the Company knows it's Customer and the level of risk associated with the business relationship?			
K5	If independent or tied agents are used, to what extent are they involved on an ongoing basis in the conduct of business?			
	▪ How does this affect the Company's knowledge of the Customer and ongoing risk management?			
K5	Does the Company use intermediaries?			
	▪ If so, are the said intermediaries: i. Regulated and subject to AML obligations?			
	ii. Subject to effective AML supervision? Are there any indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example has the intermediary been sanctioned for breaches of AML/CFT obligations?			
	iii. Based in a jurisdiction associated with higher ML/TF risk? (*Where a third party is based in a high-risk third country that the Commission has identified as having strategic deficiencies, firms must not rely on that intermediary. However, to the extent permitted by national legislation, reliance may be possible provided that the intermediary is a branch or majority-owned subsidiary of another firm established in the Union, and the Company is confident that the intermediary fully complies with group-wide policies and procedures*			