



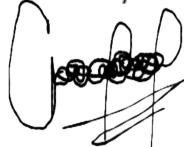
Anti-Money Laundering, Combatting the Financing of Terrorism, Counter Proliferation Financing & KYC Manual

Document Control Statement

This document and all referenced materials are subject to version control. Version control ensures that the latest approved version is preserved while previous versions are retained for a period of five (5) years for regulatory, legal, and knowledge preservation purposes.

Title	Anti-Money Laundering, Combatting the Financing of Terrorism, Counter Proliferation Financing & KYC Manual
Document Author	Money Laundering Reporting Officer (MLRO)
Document Owner	Money Laundering Reporting Officer (MLRO)
Date Created	14th March 2025
Date Last Reviewed	2nd September 2025
Classification	Public
Version	1.0

Record of Change

Version	Date Approved	Reviewed By	Approved By	Approver's Signature	Key Changes
1.0	14 March 2025	MLRO	CEO		Initial document
1.1	07 April 2025	Chief Security & Compliance Officer	Chief Commercial Officer		Minor amendments and formatting updates
1.2	02 September 2025	MLRO	CEO		Added section on proliferation financing, regulatory updates, and consequences of non-compliance



Distribution List

Recipient / Group	Version	Date Issued
All Staff and Stakeholders	1.0	14 March 2025
All Staff and Stakeholders	1.1	07 April 2025
All Staff and Stakeholders	1.2	02 September 2025

Confidentiality

No part of this document may be disclosed verbally or in writing, including by reproduction, to any third party without the prior written consent of Orchestrate Global ("Orchestrate Global"). This document, its associated appendices and any attachments remain the property of Orchestrate Global and shall be returned upon request.

Contents

Definitions

Relevant Legislations

Abbreviations

1.0 INTRODUCTION

2.0 MANUAL APPLICABILITY

3.0 COMPANY OVERVIEW

3.1 Brief Overview

4.0 COMPLIANCE WITH THE LAW



- 4.1 Company Compliance Obligations
- 4.2 Board of Directors
- 4.3 Internal Auditor
- 4.4 Compliance/Reporting Officer (MLRO)
- 5.0 MONEY LAUNDERING & TERRORISM FINANCE
 - 5.1 Definition of Money Laundering
 - 5.2 Stages of Money Laundering
 - 5.3 Penalties for the Offence of Money Laundering
 - 5.4 Terrorism Finance
 - 5.5 Money Laundering and Terrorist Financing Related Risks
- 6.0 PREVENTIVE MEASURES: ADOPTION OF A RISK-BASED APPROACH
 - 6.1 RBA Framework
 - 6.2 Identification of Risks
 - 6.3 Measures to Manage and Mitigate the Risks
 - 6.4 Dynamic Risk Management
- 7.0 CUSTOMER ACCEPTANCE POLICY
 - 7.1 Categorization of Customers- Risk Based Approach
 - 7.2 Low Risk Customers
 - 7.3 Normal Risk Customers
 - 7.4 High Risk Customers
 - 7.5 Always High-Risk Business
 - 7.5.1 Politically Exposed Persons (PEPs)
 - 7.5.2 Customers exceeding the transaction limit set by the Company
 - 7.6 Categories of Customers Not Accepted
- 8.0 CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES
 - 8.1 Principles Governing Customer Identification
 - 8.2 Simplified Due Diligence (SDD) Procedures
 - 8.3 Standard CDD Procedures
 - 8.4 Verification of Customer Identity
 - 8.5 Construction of Customer's Economic Profile
 - 8.6 Failure or Refusal to Submit Information for Verification of the Customer's Identity
 - 8.7 Customer Approvals
 - 8.8 Enhanced Due Diligence (EDD)
 - 8.9 Enhanced Customer Scrutiny and Rejection
 - 8.10 Changes to the Customer Status and Operations



8.11	Ongoing Customer Monitoring
9.0	SUSPICIOUS TRANSACTION REPORT (STR)
9.1	Reporting of STR to the FRC
10.0	RECORD KEEPING
11.0	EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING

Definitions

- i. Beneficial owner means a person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted, and any person who ultimately exercises effective control over a legal person or arrangement.
- ii. Benefit from Criminal Conduct means money or property derived, obtained or realized directly or indirectly, by any person from criminal conduct.
- iii. Business Relationship means an arrangement between a customer and the Company, where the purpose or effect of the arrangement is to facilitate payment gateway services between the customer and the Company.
- iv. Criminal property is the proceeds of criminal conduct. This includes any type of conduct, wherever it takes place, which would constitute a criminal offence if committed. It includes drug trafficking, terrorist activity, tax evasion, corruption, fraud, forgery, theft, counterfeiting, black mail and extortion. It also includes any other offence that is committed for profit.
- v. Customer means a person who has entered into an agreement with the Company for the provision of its services. In relation to a transaction or an account, a customer includes:
 - a. the person in whose name a transaction or account is arranged, opened or undertaken.
 - b. a signatory to a transaction or account.
 - c. any person to whom a transaction has been assigned or transferred.
 - d. any person who is authorized to conduct a transaction; or
 - e. such other person as the Company may specify.



- vi. Know Your Customer means requirements consisting of obtaining full particulars of the customer's identity and having a sound knowledge of the purpose for which the customer is seeking to establish a business relationship with a reporting institution.
- vii. Legal Person means any entity, other than a natural person, that can establish a customer relationship with the Company or otherwise own property and the term legal entity shall be construed accordingly.
- viii. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. It also covers money, however acquired, which is used to fund terrorism.
- ix. Money or value transfer services means a financial service that involves the acceptance of cash, cheques, other monetary instruments or other stores of value in one location and the payment of a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer, or through a clearing network to which the money or value transfer services provider belongs.
- x. Offence means the violation of any law in the Geographies we operate or in a foreign state.
- xi. Payment Gateway means a mechanism that reads and transfers payment information to and from a customer's account. Its job is to capture the data, ensure funds are available and get the customer paid. A payment gateway transfers financial data among necessary financial institutions to authorize a credit or debit card transaction and ensure a customer gets paid for a purchase.
- xii. Payment Service Provider means:
 - a. a person, company or organization acting as provider in relation to sending, receiving, storing or processing of payments or the provision of other services in relation to payment services through any electronic system.



- b. a person, company or organization which owns, possesses, operates, manages or controls a public switched network for the provision of payment services; or
 - c. any other person, company or organization that processes or stores data on behalf of such payment service providers or users of such payment services.
- xiii. Person means any natural or legal person and includes any statutory body, company or association or body of persons- corporate or un-incorporated.
- xiv. Politically Exposed Persons means persons holding prominent public positions in the geographies we operate or in a foreign country.
- xv. Proceeds of Crime means any property or economic advantage derived or realized, directly or indirectly, as a result of or in connection with an offence irrespective of the identity of the offender and includes, on a proportional basis, property into which any property derived or realized directly from the offence was later successively converted, transformed or intermingled, as well as income, capital or other economic gains or benefits derived or realized from such property from the time the offence was committed.
- xvi. Property means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interests in such assets and includes funds.
- xvii. Sanctions are political and economic decisions that are part of diplomatic efforts by countries, multilateral or regional organizations against states or organizations either to protect national security interests, or to protect international law, and defend against threats to international peace and security. Sanctions can be:
 - a. Specific, i.e., relate to specific lists of named individuals, legal entities, organizations, vessels etc. (the US Department of Treasury OFAC Sanction List);
 - b. General, i.e., cover all transactions with certain countries or jurisdictions; certain transactions with countries or jurisdictions such as exports, imports or new investment, or all transactions within a



certain area of activity/products (e.g., arms sales to a particular country);

- c. Sectoral, i.e., covers certain parties in specific sectors (OFAC designates parties on a Sectoral Sanctions Identification List or "SSI List") but only restrict certain transactions of these designated parties.

xviii. 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).

xix. 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).

xx. Suspicious Transaction Report means a report on an activity or a transaction or series of transactions made, to be made or attempted to be made by the customer through the Company.

xxi. Transaction means any deposit, withdrawal, exchange or transfer of fund whether in cash, or by cheque; or by electronic or other non-physical means; or in satisfaction,

whether in whole or in part, of any contractual order or other legal obligation. Without limiting the above, transaction includes the following:

- a. The establishment and maintenance of a business relationship; or
- b. The opening and maintenance of customer account; or
- c. The engagement of customer service; or
- d. Payment made in respect of settlements; or
- e. Such other transaction as may be prescribed.

xxii. Terrorist financing relates to the raising or holding of funds (directly or indirectly) with the intention that those funds should be used to carry out activities defined as acts of terrorism or with the intention to dispose those funds to a terrorist group or a separate terrorist. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

xxiii. Wire transfer means any transaction carried out on behalf of a customer through the Company by electronic means with a view to making an amount of funds available to a beneficiary person or



vice versa, irrespective of whether the customer and the beneficiary are the same person.

Relevant Legislations

This Manual is underpinned and defined by the following pieces of legislations:

- i. Bank Secrecy Act (BSA), 1970
- ii. USA PATRIOT Act, 2001 (Title III)
- iii. FinCEN Regulations (31 CFR Chapter X)
- iv. Office of Foreign Assets Control (OFAC) Sanctions Regulations
- v. State Money Transmitter Laws and Regulations
- vi. Federal Trade Commission (FTC) Regulations on Consumer Protection
- vii. Dodd-Frank Wall Street Reform and Consumer Protection Act (as applicable)
- viii. Any other legislative or regulatory documents issued by relevant U.S. authorities (e.g., CFPB, FDIC, state regulators)

Abbreviations

Terms/Acronyms	Definition
AML	Anti-Money Laundering
CFT	Combatting Financing of Terrorism
CPF	Counter Proliferation Financing
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FRC	The Financial Reporting Centre
KYB	Know Your Business
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer
ML and TF	Money Laundering and Terrorist Financing
OFAC	Office of Foreign Assets Control
PROCAMLA	The Proceeds of Crime and Anti-Money Launder 2009



PROCAMLRL	The Proceeds of Crime and Anti-Money Lau Regulations 2013
PEP	Politically Exposed Persons
PSP	Payment Service Provider
PTA	Prevention of Terrorism Act
PTR	Prevention of Terrorism Regulations 2013
SDD	Simplified Due Diligence
STR	Suspicious Transaction Report
UBO	Ultimate Beneficial Owner
RBA	Risk Based Approach

1.0 INTRODUCTION

This document is referred to as the Anti-Money Laundering (AML) & Combatting the Financing of Terrorism (CFT) and Know Your Customer (KYC) Manual (the Manual) and sets the parameters for the Company in relation to the AML, CFT and KYC framework. It does not purport to be a comprehensive summary of PROCAMLA and or any other relevant and applicable laws and should be read in conjunction with them.



The purpose of the Manual is to lay down Orchestrate Global's (hereinafter referred to as ("the Company")) internal practice, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing. It sets out the principles and standards for compliance and management of risks associated with financial crimes in the Company to prevent it from being used for financial crimes; to comply with all applicable legal requirements; and to ensure that the most appropriate action is taken by the Company to mitigate the risks associated with financial crime.

The Manual is developed and periodically updated by the MLRO based on the general principles set up by the Board of Directors in relation to the prevention of Money Laundering and Terrorist Financing.

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

The Manual shall be communicated by the MLRO 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.

2.0 MANUAL APPLICABILITY

This Manual applies to all Company officers, employees, appointed contractors, agents, products and services offered by the Company and foreign correspondents, contractors and third parties with whom the Company may contract with.

All departments within the Company will cooperate to create a cohesive effort in the fight against ML and TF. Each department has implemented risk-based procedures reasonably expected to detect and facilitate the reporting of suspicious transactions. All efforts exerted will be documented and retained.

The Company's aim is not only to comply with relevant legal requirements, but also to mitigate and reduce the potential risk to the customers using our products, services and delivery channels to launder the proceeds of illegal activity, fund terrorist activity or conduct prohibited financial sanctions activity.

The MLRO 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 MLRO.

In this respect, the MLRO shall be responsible to update the Manual, at least once a year, so as to comply with regulators' future requirements, as applicable, regarding



the customer identification and due diligence procedures which the Company must follow, for customers who deal in the Company's services.

All employees of the Company have been made aware of the Company's policies and procedures relating to AML/TF & KYC and are aware of the consequences if the Company is not in compliance with the applicable AML laws.

The MLRO will continually monitor the applicable laws and regulations and will update the Manual based on domestic and international requirements and any legislative change.

3.0 COMPANY OVERVIEW

3.1 Brief Overview

Orchestrate Global is a multi-national technology company that enables businesses to receive cashless payments simply, securely and seamlessly from its clients through a variety of payments methods.

The Company is incorporated in various geographies under different names and is registered as a Money Service Business (MSB)

The Company is focused on providing its customers with Payment Card Processing and APMs for various high risk category customers incorporated globally and doing business worldwide in compliance with the Banking Secrecy Act and other applicable laws and legal requirements.

4.0 COMPLIANCE WITH THE LAW

4.1 Company Compliance Obligations

The Company is required formulate, adopt and implement internal control measures and other procedures to combat money laundering. Such measures include:

- i. programmes for assessing risks relating to ML and TF;
- ii. the formulation of a control policy that will cover issues of timing, degree of control, areas to be controlled, responsibilities and follow up;
- iii. monitoring programmes in relation to complex, unusual or large transactions or suspicious activities;
- iv. enhanced due diligence procedures with respect to persons and business relations and transactions carrying high risk and with persons established in jurisdictions that do not have adequate systems in place to combat ML and TF



- v. providing employees, including the MLRO, from time to time, with training to facilitate recognition and handling of suspicious transactions;
- vi. making employees aware of the procedures under the Act, Regulations or directives, codes and guidelines issued thereunder or and any other relevant policies that is adopted by the Company;
- vii. establishing and maintaining a manual of compliance procedures in relation to anti-money laundering;
- viii. providing for the necessary processes and working methods to ensure compliance with the Act, Regulations and the internal rules; and
- ix. provide for the responsibility of the Board of Directors of the Company in respect of compliance with the Act, these Regulations and the internal rules.

4.2 Board of Directors

The Board of Directors shall understand the nature of money laundering threats and vulnerabilities the Company faces. It shall, therefore, ensure that the Company adopts a risk-based approach to managing ML and TF risks. The responsibilities of the Board of Directors in relation to the prevention of ML and TF shall include, but not limited to, the following:

- i. 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 MLRO;
- ii. to review and approve the Manual;
- iii. to appoint staff that possesses the skills, knowledge and expertise relevant to financial and other activities depending on the situation, who shall act as the MLRO and, where is necessary, alternate to the MLRO and determine their duties and responsibilities, which are recorded in this Manual;
- iv. 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;



- v. to ensure that the MLRO, and alternate to the MLRO, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention of ML and TF 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;
- vi. to ensure that all employees are aware of the person who has been assigned the duties of the MLRO 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;
- vii. to establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the MLRO, either directly or through the alternate to the MLRO, if any, and notifies accordingly the MLRO for its explicit prescription in the Manual;
- viii. approve the mandatory annual training program prepared by the MLRO;
- ix. ensure that it receives adequate management information on the implementation of the company's AML/CFT training program;
- x. ensure to be adequately trained to be well aware and up to date with the regulatory framework and the relevant responsibilities deriving from this; and
- xi. To 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 as required by law.

4.3 Internal Auditor

The Company shall adopt an independent audit function to check compliance by the Company of the AML & CFT laws and regulations. An independent internal audit function shall be established for the verification of the Company's policies, controls and procedures.

The Company shall 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:

- i. 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/TF mentioned in the Manual.
- ii. The findings and observations of the Internal Auditor, in relation to (i) above, shall be submitted, in a written report form, to the Board.

4.4 Compliance/Reporting Officer (MLRO)

The Company shall appoint an MLRO, who shall be of management level and to whom all staff at the Company shall monitor and report to cases of suspicious activity or money laundering.

The obligations of the MLRO shall be as follows:

- i. Understand the ML and TF risk profile of the Company.
- ii. Review the Manual at least once every year.
- iii. Be responsible for the implementation and on-going compliance of the Company's internal programmes, controls and procedures in relation to its business.
- iv. Act as the liaison officer between the Company and the regulators in matters relating to compliance with the provisions the PROCAMLA and any other law with respect to ML or TF.
- v. Ensure development of a documented framework to conduct ML and TF risk assessment.
- vi. Identify the risks relating to products, services and delivery channels, clients and business relationships, geography and other relevant factors.
- vii. Coordinating the ML and TF risk assessment processes.
- viii. Review outcome of the risk assessment process.
- ix. Continuously improve collection and analysis data used in the assessment.
- x. Provide periodic reports of the Company's ML and TF risk assessment to the Board.
- xi. Be responsible for carrying out any actions resulting from the gaps or deficiencies identified by the risk assessment exercise.



- xii. ensure he is informed of all suspicious activities available to the Company and take action on suspicious disclosures from employees of the Company as soon as practical so as not to delay the reporting of such disclosures.
- xiii. where a disclosure is made, to apply internal risk-management procedures on a suspicious transaction
- xiv. report disclosures deemed suspicious to the FRC.
- xv. ensure that the Company's Board and employees are made aware of the relevant and applicable ML and TF legislations as well as the audit systems adopted by the Company.
- xvi. in liaison with the Company's Human Resource department, ensure persons are screened before being hired as employees.

5.0. MONEY LAUNDERING, TERRORISM FINANCING PROLIFERATION FINANCING

5.1 Definition of Money Laundering

Money laundering is the process by which criminals attempt to conceal the true origins and ownership of their proceeds of crime.

The PROCAMLA defines money laundering as containing the following aspects:

1. A person who knows or who ought reasonably to have known that property is or forms part of the proceeds of crime and:
 - i. enters into any agreement or engages in any arrangement or transaction with anyone in connection with that property, whether that agreement, arrangement or transaction is legally enforceable or not; or
 - ii. performs any other act in connection with such property, whether it is performed independently or with any other person, whose effect is to-
 - conceal or disguise the nature, source, location, disposition or movement of the said property or the ownership thereof or any interest which anyone may have in respect thereof; or
 - enable or assist any person who has committed or commits an offence, whether in geographies we operate or elsewhere to avoid prosecution; or
 - remove or diminish any property acquired directly, or indirectly, as a result of the commission of an of the offence of money laundering.



2. A person who acquires; uses; or has possession of property and who, at the time of acquisition, use or possession of such property, knows or ought reasonably to have known that it is or forms part of the proceeds of a crime committed by him or by another person, commits the offence of money laundering.
3. A person who, knowingly transports, transmits, transfers or receives or attempts to transport, transmit, transfer or receive a monetary instrument or anything of value to another person, with intent to commit an offence, that person commits the offence of money laundering.

5.2 Stages of Money Laundering

Generally, money laundering occurs in three stages:

i. Placement

This is the first stage in the money laundering cycle and usually coincides with the initial entry of the funds into the financial system. There are many ways in which this can occur, but the most common methods involve dividing/splitting up sums of cash. "Splitting up" refers to both the timing of division (financial transactions spread over a period of time) and methods used for "individual" splits, involving a large number of "persons/customers".

ii. Layering

After placement comes layering, which is the next logical phase although not necessarily in terms of timing.

Layering consists of a series of banking and financial transactions, over a short period of time, designed to dissociate the financial assets as far as possible from their illegal origin; this requires criminal organizations to have a detailed knowledge of the rules and procedures adopted by financial institutions to guard against money laundering.

It is common during this phase to use a large number of accounts and intermediaries and/or jurisdictions which ensure a sufficient lack of transparency to the transactions.

iii. Integration

The final stage of money laundering is termed the integration stage because it is at this point that the unlawful funds return fully assimilated into the legitimate economic and financial system. Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

5.3 Penalties for the Offence of Money Laundering



A person who contravenes any of the provisions of clause 5.1 is, on conviction, liable:

- i. in the case of a natural person, to imprisonment for a term not exceeding fourteen years, or a fine not exceeding five million shillings or the amount of the value of the property involved in the offence, whichever is the higher, or to both the fine and imprisonment; and
- ii. in the case of a body corporate, to a fine not exceeding twenty-five million shillings, or the amount of the value of the property involved in the offence, whichever is the higher.

5.4 Terrorism Financing

Terrorism financing is the provision of funds or providing financial support to individual terrorist or non-state actors. Such activities are financed by either illegal or legal sources.

Prevention of Terrorism Act defines terrorist act to constitute an act or threat of action which interferes with an electronic system resulting in the disruption of the provision of communication, financial, transport or other essential services and is carried out with the aim of:

- i. Intimidating or causing fear amongst members of the public or a section of the public; or
- ii. Intimidating or compelling the government of international organization to do, or refrain from any act; or
- iii. Destabilizing the religious, political, constitutional, economic or social institutions of a country, or an international organization.

Any person who, directly or indirectly, collects, attempts to collect, provides, attempts to provide or invites a person to provide or make available any property, funds or a service intending, knowing or having reasonable grounds to believe that such property, funds or service shall be used:

- i. for the commission of, or facilitating the commission of a terrorist actor any other act which constitutes an offence within the scope of, and defined in any of the treaties listed in the annex to the 1999 International Convention for the Suppression of the Financing of Terrorism;
- ii. by a terrorist group for any purposes;
- iii. by any natural person, for any purpose, who-
 - Commits or attempts to commit, by any means, directly or indirectly, unlawfully and willfully, acts within the scope of section (i) above;



- Participates as an accomplice within the scope of section (i) above;
- Organizes or directs others to commit acts within the scope of section (i) above; or
- Contributes to the commission of acts within the scope of section (i) above by a group of persons acting with a common purpose where contribution is made intentionally and with the aim of furthering commission of acts within the scope of section (i) above, or with the knowledge of the intention of the group to commit acts within the scope of section (i) above commits an offence and is liable, on conviction, to imprisonment for a term not exceeding twenty years.

Any person who possesses any property intending or knowing that it shall be used, whether directly or indirectly or in whole or in part, for the commission of, or facilitating the commission of a terrorist act, commits an offence and is liable, on conviction, to imprisonment for a term not exceeding twenty years.

Any person who knowingly supports or solicits support for the commission of a terrorist act by any person or terrorist group commits an offence and is liable, on conviction, to imprisonment for a term not exceeding twenty years.

Any person who knowingly:

- i. deals directly or indirectly, in any property that is owned or controlled by or on behalf of a terrorist group;
- ii. enters into, or facilitates, directly or indirectly any transaction in respect of property referred to in point one or
- iii. provides financial or other services in respect of property referred to in point one at the direction of a terrorist group,
- iv. commits an offence and is liable, on conviction, to imprisonment for a term not exceeding twenty years.

5.5 Proliferation Financing

Proliferation Financing refers to the act of providing funds, financial services, or other forms of support to the development, acquisition, or distribution of weapons of mass destruction (WMDs), such as nuclear, chemical, or biological weapons, and their delivery systems.

Orchestrate Global shall incorporate and regularly update lists of individuals, entities, and countries subject to sanctions due to their involvement in proliferation activities, obtain detailed information about the nature of the customer's business and the



source of their funds and ensure transparency regarding the true ownership of entities and accounts. Orchestrate Global shall also flag suspicious activities indicative of proliferation financing, report suspicious transactions that could be related to proliferation financing to the relevant authorities.

The Company also shall conduct regular risk assessments, collaborate with other financial institutions/ regulatory bodies, and industry groups to share insights and best practices for detecting and preventing proliferation financing. Additionally, the Company shall conduct regular reviews and audits of AML policies and practices to ensure their effectiveness in addressing proliferation financing.

Orchestrate Global shall not onboard any merchant deemed to have been involved in proliferation financing activities.

5.5 Money Laundering, Terrorist Financing and Proliferation Financing Related Risks

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

- i. *Regulatory risk*: where this represents 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 and 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.
- ii. *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 asset and the damage that such an event may cause may be irreparable.
- iii. *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.
- iv. *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.

6.0 PREVENTIVE MEASURES: ADOPTION OF A RISK-BASED APPROACH

6.1 RBA Framework

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

- iv. recognizes that the ML or TF threat varies across customers, countries, services and securities;
- v. allows the Board to differentiate between customers of the Company in a way that matches the risk of their particular business;
- vi. 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;
- vii. helps to produce a more cost-effective system; and
- viii. 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 Payment Services provided by the Company.

RBA requires a number of steps to be taken by the Company to determine the most cost-effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the business. The steps are to:

- i. identify the ML and TF risks that are relevant to the business;
- ii. assess the risks presented by the particular:
 - Customers – types and behavior.
 - Products and services.
 - Delivery channels.
 - Geographical areas of operation, for example, location of business premises, source or destination of client's funds.
 - Complexity and volume of transactions.



- iii. design and implement controls to manage and mitigate these assessed risks;
- iv. continuously monitor and improve the effective operation of these controls;
- v. performing KYC identification and due diligence;
- vi. record appropriately what has been done, and why;
- vii. ensuring the existence of internal control, assessment and risk management in order to prevent ML and TF;
- viii. 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;
- ix. setting up risk and compliance management practices;
- x. ensuring that sufficient onboarding policy is in place; and
- xi. performing ongoing training of employees in the recognition and handling of transactions and activities related to ML/TF.

The risk assessments referred above shall be documented, updated and made available to the Board of Directors.

The Board of Directors shall assess and evaluate the risks it faces, for usage of the services the Company provides, for the purpose of ML/TF. The particular circumstances that shall determine the suitable procedures and measures which need to be applied to counter and manage risks.

The application of appropriate measures and the nature and extent of the procedures on a RBA depends on different indicators. Such indicators include, but not limited to, the following:

- i. the scale and complexity of the services offered;
- ii. geographical spread of the services, products and customers;
- iii. the nature (e.g. non-face-to-face) and economic profile of customers as well as of services offered;
- iv. the distribution channels and practices of providing services;
- v. the volume and size of transactions;
- vi. the degree of risk associated with each area of services;
- vii. the country of origin and destination of customers' funds;
- viii. deviations from the anticipated level of transactions; and



- ix. 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 MLRO or alternate to the MLRO shall be responsible for the development of the policies, procedures and controls on a RBA. And their adequate implementation.

The Internal Auditor shall be responsible for reviewing the adequate implementation of a risk-based approach by the MLRO or alternate to the MLRO, at least annually.

6.2 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 purpose of ML or TF. The particular circumstances of the Company will determine suitable procedures and measures that need to be applied to counter and manage risk.

The Company shall, at all times, be in a position to demonstrate to the FRC that the extent of measures and control procedures it applies are proportionate to the risk it faces for the use of its 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:

- ix. The purpose of the account or the relationship;
- x. The volume of assets that will be deposited by the customer or the size of the transactions; and
- xi. The regularity or the duration of the business relationship.

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

- i. 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.
- ii. 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.
- iii. Risks based on the customer's initial communication with the Company:
 - non face-to-face customers; and
 - customers introduced by a third party.
- iv. Risks based on the Company's services:
 - services that allow payments to third parties;
 - large cash deposits or withdrawals; and
 - products or transactions which may favor anonymity.

6.3 Measures 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:

- xii. adoption of the CDD procedures in respect of customers in line with their assessed ML and TF risks;
- xiii. 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);
- xiv. 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



- xv. 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 a criterion which reflects 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 alia, 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 determines, in the light of additional information received, that fall under one of the risk categories.

In this respect, it is the duty of the MLRO or alternate to the MLRO 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.

6.4 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 Payment Services provided by the Company change. The same happens to the transactions used for ML or TF.

In this respect, it is the duty of the MLRO or alternate to the MLRO 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.

7.0 CUSTOMER ACCEPTANCE POLICY

7.1 Categorization of Customers- Risk Based Approach

This section defines the criteria for the categorization of customers based on their risk. The Company shall classify customers into various risk categories and based on the risk perception and decide on the acceptance criteria for each category of customer.



The Company uses risk rating in a scoring format. The range from 1 to 5 with 1 being the lowest and 5 being the highest. The client categorization determines the level of due diligence and monitoring process that the Company will adopt to mitigate the compliance risk.

The MLRO or alternate to the MLRO shall be responsible for categorizing customers in one of the following three (3) categories based on the criteria of each category set below:

5.0-4.0	3.9-2.0	1.9-0.1
High Risk	Normal Risk	Low Risk
Enhanced Due Dili ge nc e (E DD)	Regular Procedures (CDD) KYC	Simplified Due Diligence (SDD)

7.2 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 SDD procedures for low-risk customers.

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

(a) Customer risk factors:

- 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) Product, service, transaction or delivery channel risk factors:



- i. Tours and Travels Agencies;
- ii. Customers dealing in agricultural products;

(c) Geographical risk factors:

- i. The geographical location of the customer's residence;
- ii. A country which has effective system to counter the money laundering and terrorist financing activities;
- iii. a country identified by credible sources as having a low level of corruption or other criminal activity such as money laundering and the production and supply of illicit drugs; and
- iv. 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.

7.3 Normal Risk Customers

The following types of Customers can be classified as normal risk Customers with respect to the ML or TF risk which the Company faces:

- any customer who does not fall under the 'Low Risk Customers' or 'High Risk Customers' categories;
- customers who are not physically present for identification purposes (non-face-to-face customers).

7.4 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. customer is a non-profit organization;
- xv. customer is a business that are cash-intensive;
- xvi. customer is a foreign financial institution or non-bank financial institution;
- xvii. customer is a professional service provider;
- xviii. any other customers that their nature entail a higher risk of ML or TF;
- xix. any other customer determined by the Company itself to be classified as such.

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

- i. Financial services and dealership in securities and stock markets;
- ii. products or transactions that might favor anonymity;
- iii. product or service has unusual complexity;
- iv. product or service has a high transaction or investment value;
- v. product or service enables significant volumes of transactions to occur rapidly;
- vi. service involves the provision of directorship services or nominee shareholders



- vii. non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
- viii. payment received from unknown or non-associated third parties;
- ix. 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;
- v. other countries identified by the reporting entity as higher-risk because of its prior experiences or other factors

(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 customers;
- 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.

7.5 Always High-Risk Business

This category contains customers that shall be treated as always high risk and posing legal, financial and or reputational risk to the Company. They shall always be escalated to the Board of Directors for approval.

7.5.1 Politically Exposed Persons (PEPs)

The Company is required to obtain information from its customers confirming whether they fall under the category of a PEP or not.

Politically exposed persons ("PEPs") are natural persons who are or have been entrusted with prominent public functions in a country or jurisdiction, and include, but not limited to:

- i. members of Cabinet;
- ii. senior executives of state-owned corporations;
- iii. important political party officials.
- iv. senior military officials and other members of the disciplined forces;
- v. members of the Judiciary;
- vi. senior State Officers;
- vii. senior Public Officers;
- viii. senior Official of an International Organization;
- ix. any immediate family member or close business associate of above- described persons.

The term 'family members' shall include the following:

- i. their spouse, or any partner recognized by national law as equivalent to the spouse;
- ii. their children and their spouses or partners;
- iii. their parents; and
- iv. their siblings.

The term 'close business associates' shall include the following:



- i. natural person known to have joint beneficial ownership of a body corporate or any other form of legal arrangement, or any other close business relations with a person identified as PEP;
- ii. a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of a person identified above.

The PEP director(s) and or shareholder(s) for a customer shall execute a PEP declaration form before being onboarded and the same shall be filed by the Company.

The form will require an outline of the following:

- i. type/category of PEP;
- ii. nationality of PEP;
- iii. country of domicile of the PEP;
- iv. position held or controlled by PEP in the customer;
- v. declaration of acceptance or rejection of being PEP;
- vi. declaration that the Assets/Funds to be transferred, then or at any time in the future, to the Company are not and will not be derived from or otherwise be connected with any activity which is illegal or unlawful, either in their country of origin or in the location in which the Company is established; and
- vii. declaration that the PEP has never been convicted of any offence of money laundering, fraud, bribery or corruption or any other criminal offence whatsoever nor are they subject to any ongoing regulatory or legal action(s) which may have an adverse impact on my reputation, character, financial integrity and reliability.

Once the merchant submits the required information and signs the declaration form, the Head of Business shall review and recommend approval or rejection. The Head of Risk/ Compliance then makes the final decision to approve or reject all PEP-related applications.

7.5.2 Customers exceeding the transaction limit set by the Company

These are customers who 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.

The Company detects transactions that are unusual where:

- i. the transaction exceeds the transaction limit set by the Company to the Customer;



- ii. the customer has unusual or unexpected transaction patterns compared to their normal transaction level; or the pattern of transactions associated with similar customers, products or services; or the transactions are very complex compared with other similar transactions associated with similar customer types, products or services; and
- iii. the Company is not aware and or convinced of an economic rationale or lawful purpose or doubts the veracity of the information shared by the customer and or its client(s).

In such instances, the Company shall, for purposes of determining the legitimacy of funds and transactions, consider the following information:

- i. for large, frequent or unusual cash deposits or withdrawals, written statement from the customer confirming that the nature of his business activities normally and reasonably generates substantial amounts of cash; for large, frequent or unusual currency exchanges, written statement from the customer confirming the reason and need for acquired currencies;
- ii. for multiple or nominee accounts, or similar or related transactions, written statement from the customer confirming the reason and need for multiple or nominee accounts, or similar or related transactions;
- iii. for large, frequent or unusual transfers or payments of funds, appropriate documentation as to the identity of the recipient or sender of the transferred or paid funds, and the reason for the transfer or payment;
- iv. for large or unusual investments or requests for advice or services, written statement from the customer confirming that the investments or advice or services being requested are bona fide and consistent with the objectives of the customer's reasonable and normal business activities;
- v. for large or unusual foreign transactions, written confirmation from the customer indicating the nature, reason and appropriate details of the foreign transactions sufficient to determine the legitimacy of such transactions.



The Company, in consultation with the FRC, set up policies setting out limits on the maximum cash transaction amounts non-customers can undertake with it.

iii. Customers in High Risk & Sanctioned Jurisdictions

The Company shall apply enhanced due diligence on business relationships and transactions with any natural and legal persons, legal arrangements or financial institutions originating from countries identified as posing higher risk of money laundering, terrorism financing or proliferation by-

- i. The FATF as having strategic money laundering and combating financing of terrorism deficiencies, that has not made sufficient progress in addressing the said deficiencies;
- ii. The Cabinet Secretary as having ongoing substantial ML and TF risks;
- iii. Customers falling under the OFAC sanctions list.

In accordance with this Manual, for the development and implementation of appropriate measures and procedures on RBA and for the implementation of customer identification and due diligence procedures, the MLRO shall create and always maintain a list of High-Risk Jurisdictions, which shall be subject to review and revision where applicable.

To protect the Company and the financial system from the ongoing and substantial ML or TF risks emanating from jurisdictions referred to as High Risk, the Company shall apply countermeasures including:

- i. Limiting or terminating business relationship with the customer located in the concerned countries;
- ii. prohibit reliance on third parties located in the concerned countries to conduct CDD;
- iii. apply EDD measures on correspondent banking relationships with the customer located in concerned countries;
- iv. when considering the establishment of subsidiaries or branches or representative offices of the customer from the concerned countries, the Company shall take into account whether the customer is based in countries identified as having higher ML or TF risks or inadequate ML or TF systems;
- v. Submission of a report listing customers originating from the higher risk countries to the FRC on an annual basis;
- vi. Any other measures as may be prescribed by the FRC.



7.6 Categories of Customers Not Accepted

The below listed characteristics of customers have been identified with potentially higher ML/TF risk and shall not be acceptable for establishing a business relationship and will be rejected by the Company:

- i. customers who do not provide sufficient information to verify their identity;
- ii. businesses conducted in anonymous or fictitious names;
- iii. businesses having relationships with shell banks;
- iv. casinos and betting companies operating without license or supervision, including online gambling companies;
- v. customers who provide financial or insurance services without a license or control by a regulatory authority;
- vi. customers against whom sanctions are applied on the basis of decisions by OFAC, or the state authorities in jurisdictions where the Company has a presence or other international organizations, including, but not limited to the FATF;
- vii. businesses involving activities by the customer's clients that are illegal in the jurisdiction(s) in which the activities are carried out, and/or which would be illegal if carried out in the jurisdiction(s) from which the Company would be providing the services;
- viii. businesses involving activities by serviced entities that would constitute tax fraud or tax evasion in the jurisdictions where those activities are taking place; and
- ix. businesses that violate the Company's zero tolerance approach to bribery and corruption.

Factors to be considered include the customer's background; type and nature of the customer's business activity; country of origin; anticipated level and nature of the business transactions; as well as the expected source and origin of the funds.

In case of difficult and controversial situations, the ultimate decision for the acceptance of the customer rests with the Board of Directors of the Company.

The weight assigned to each of the input categories is based on the total score of the Customer Risk Assessment, except the following types of clients which are categorized in accordance with the Law as High-Risk clients regardless of the overall score in the Customer Risk Assessment Form. The above list is not exhaustive, and the Company



shall maintain an elaborate list of prohibited businesses, which shall be subject to review and revision.

8.0 CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES

8.1 Principles Governing Customer Identification

The Company shall ascertain, before entering into a business relationship, the identity of a customer on the basis of any official or other identifying documents.

The Company shall formulate and implement measures to be undertaken to enable it attain the following objectives:

- i. identify the customer and verify that customer's identity using reliable, independent source documents, data or information or other evidence as is reasonably capable of verifying the identity of the customer;
- ii. identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner, such that the Company is satisfied that it knows who the beneficial owners is and it understands the ownership and control structure of the customer in case of legal persons and arrangements;
- iii. obtain information on the nature of customer's business and the customer's
- iv. economic circumstances;
- v. understand and, as appropriate, obtain information on the purpose and nature of the business relationship;
- vi. obtain information on the type, volume and value of the activity to be expected within the relationship;
- vii. obtaining information on the source of funds and, subject to risk assessment, obtain information on the source of wealth;
- viii. keep the information relevant and up-to-date;
- ix. screening customers against PEP and other sanction lists; and
- x. conduct ongoing due diligence on the customer and scrutiny of transactions undertaken by the customer throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, their business and risk profile, including where necessary the source of funds.

In implementation of the above, the Company shall take measures to satisfy itself as to the true identity of any prospective customer seeking to enter into a business



relationship with the Company by requiring the them to produce an official record for the purposes of establishing its true identity and for the purpose of verifying its identity.

As such, the Company shall establish and verify the following particulars:

- i. customer's identity;
- ii. the purpose and nature of its business or principal activity;
- iii. customer's financial status; and
- iv. the capacity in which the customer is entering into the business relationship with the Company.

The above shall be carried out:

- i. when establishing initial business relationship;
- ii. when undertaking one-off transactions that amounts to 5000 USD or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- iii. when there is suspicion of ML or TF, regardless of the amount of the transaction in the provision of the relevant Payment Services;
- iv. and when there is doubt about veracity or adequacy of previously obtained customer information or identification data.

In this respect, it is the duty of the MLRO or alternate to the MLRO to apply all the relevant CDD identification procedures described in this Manual and the Company's Customer Onboarding Policy, as applicable.

8.2 Simplified Due Diligence (SDD) Procedures

The Company shall perform SDD to customers falling within the purview of section of this Manual.

The above notwithstanding, the following shall apply:

- i. The Company may apply SDD 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 indicators.

The Company's SDD may include:

- i. 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);
- ii. reducing the frequency of customer identification updates;
- iii. reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold;
- iv. 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.

8.3 Standard CDD Procedures

- i. Natural Persons

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; Their identity should be verified by:
 - ü Valid Passport;
 - ü National ID Card; and
 - ü 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 followings:

- i. A recent utility bill;
- ii. Bank statement;
- iii. Credit card statement (monthly); and
- iv. Tax identification numbers, Social Security number or Government Service and Insurance System number.

The utility bill, bank statement and credit card statement should not be older than three (3) months from the filing date. Whereas copy of the customer's tax identification numbers, Social Security number or Government Service and Insurance System number should be apostilled in the country of origin.



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 funds objective and other related information concerning the customer's financial situation and needs;
- iii. Annual income, Assets or net worth.
- iv. Legal Relationships

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 Company shall, for screening purposes of customers, request the customers to furnish the following documentations to assist in the identification and verification of their identity:

A. Companies

- i. Certificate of Incorporation/Registration;
- ii. Memorandum and Articles of Association;
- iii. Register of Directors and Members (not more than six (6) month);
- iv. Certified copy of board resolution stating authority to open a customer account with the Company;
- v. Audited financial statements for the last full year or latest six (6) months bank statements;
- vi. Directors and Members Passports;
- vii. Tax Identification Number (TIN) document.
- viii. Appropriate Board of Directors' resolutions and signed application forms or account opening, identifying the authorized signatories or principal officers of the corporation authorized to trade and their authorities and specimen signatures;
- ix. Board Resolution authorizing the corporation to open the account with the Company.



B. Partnerships

- i. Name of Partnerships or Evidence of registration where applicable;
- ii. Partnership deed or agreement;
- iii. Its registered address or principal place of business or office;
- iv. Full names, address and passports of all partners;
- v. List of partners exercising executive control over the partnership;
- vi. Tax Identification Number (TIN) document;
- vii. Name and particulars of each natural person purporting to be authorized to establish a business relationship or to enter into a transaction with the Company on behalf of the partnership;
- viii. Un-audited financial statements for the last full year or latest six (6) months bank statements;
- ix. Appropriate Partners' resolutions and signed application forms or account opening, identifying the authorized signatories or principal officers of the partnership authorized to trade and their authorities and specimen signatures;
- x. Partnership Resolution authorizing the partnership to open the account with the Company.

C. Trust Organizations

- i. Particulars of its registered name, if any;
- ii. its registration number, if any;
- iii. evidence of registration or incorporation such as a Certificate of Incorporation or registration;
- iv. trust deed;
- v. formative document such as partnership agreement, memorandum and articles of association;
- vi. official returns showing registered office and if different, the principal place of business;
- vii. full names and details of the management company of the trust or legal arrangement, if any;



- viii. names of the relevant persons having senior management position in the legal person or trustees of the legal arrangement;
- ix. full names of the trustees, beneficiaries or any other natural person exercising ultimate effective control over the trust;
- x. full names of the founder of the trust;
- xi. any other documentation from a reliable independent source proving the name, form and current existence of the customer;
- xii. Appropriate Board of Directors' resolutions and signed application forms or account opening, identifying the authorized signatories or principal officers of the trust authorized to trade and their authorities and specimen signatures;
- xiii. Board's Resolution authorizing the trust to open the account with the Company.

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 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.

iii. Ultimate Beneficial Owners

The Company shall ensure to identify and verify the natural persons behind a legal person and arrangement. It shall strive to understand the nature of business, ownership and control structure when performing CDD measures in relation to a customer that is a legal person or legal arrangement.

To facilitate the above, the customer shall provide the following:

- i. Particulars of directors and shareholders;



- Proof of identification- The customer shall provide the Company with a copy of passport or other forms of official documentation confirming the identity (national ID and passport are recommended) of its ultimate beneficiaries.

For customers not incorporated locally, passports shall always be requested. In rare and exceptional cases, clients providing only official ID will be accepted.

- The following must always appear on the copies of documents obtained:
 - a. Passport number and/or ID number;
 - b. Issuing date and authority;
 - c. Beneficiary's date and place of birth;
 - d. Beneficiary's photo;
 - e. Validity date (if any)
- If in doubt for the genuineness of any document (passport, identity card or any other documentary evidence) the Company shall seek verification of identity from an Embassy or the consulate of the issuing country or a reputable credit or financial institution situated in the customer's country of residence.
- Independent verification of the ultimate beneficial owners through external trusted sources shall be carried out with Business Registration Service (BRS) for local merchants.
- Orchestrate Global shall request international merchants to provide Notarized or certified corporate documents such as Certificate of Incorporation, Memorandum and Articles of Association, Register of Directors and Register of Shareholders, to verify the legitimacy of the documents.
- When reviewing a notarized document, the following key elements shall be reviewed to ensure the authenticity and validity of the documents:
 - a. Notary's Signature and Seal/Stamp
 - b. Notary's Commission Information such as Commissioner number and expiration date
 - c. Date of Notarization



d. Notarial Language (Acknowledgment or Jurat) to confirm that the original documents were sighted.

ii. Proof of Residence - the Company shall verify the ultimate beneficiaries' permanent address through the following ways: the original copy of a recent (up to six (6) months) utility bill, bank statement, local authority tax bill, certificate of residency e.t.c.

The following must always appear on the document, confirming the customer's permanent address:

- a. Name of beneficiary;
- b. Beneficiary's full address- including postal code;
- c. Name of authority/organization issuing the document; and
- d. Date of issue.

8.4 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.

The following are some counter checks that shall be applied by the Company to verify identity of customers without face-to-face contact:

- Telephone contact of the applicant at an independently verifiable home or business number;
- Upload a recent bank statement or utility bill.
- Enter the tax number identification screen.
- Confirmation of address through correspondence or presentation of proof of billing address.
- Use of due diligence platforms such as World-Check and Dilisense.
- Local identification documents for local merchants will be verified through the Integrated Population Registration Database System (IPRS).

Above procedures shall be strictly implemented when opening of accounts; especially if the customer is just referred by a third party. Such requirements should ideally be done prior to execution of the applicable agreements.



For non-residents who seek to procure the Company services without face-to-face contact, documents as enumerated above issued by foreign authorities must be submitted.

The Company shall always require its customers to submit information particularly on the SOFs. If the customer states that he/she has a business, some proof of the business documents, like by-laws, business registration, etc. are requested.

Company search on the website for registered companies shall be done to ensure that the corporate or other business applicant is an existing business entity.

8.5 Construction of Customer's Economic Profile

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

- 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;
- 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;
- A customer's residential and business address will be an essential part of his identity;
- The Company shall never use the same verification data or information for verifying the customer's identity and verifying its home address;



- 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 projected monthly volumes, 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.

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

- I. the name of the company;
- II. the country of its incorporation;
- III. the head offices address;
- IV. the names and the identification information of the BOs;
- V. the names and the identification information of the Directors;
- VI. the names and the identification information of the authorized signatories;
- VII. financial information;
- VIII. 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).
- IX. The said data and information will be recorded in a separate form designed for this purpose which will be 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 will be 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.



X. 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;

XI. 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 will be investigated, and the findings recorded in the respective customer's file. Transactions that are not justified by the available information on the customer, will be thoroughly examined so as to determine whether suspicions over ML or TF arise for the purposes of submitting an internal report to the MLRO or alternate to the MLRO.

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

- i. it is reasonable possible to establish that the customer is the person he claims to be, and,
- ii. 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 MLRO or alternate to the MLRO. 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 MLRO or alternate to the MLRO shall:

- i. ensure that the customer identification records remain completely updated with all relevant identification data and information throughout the business relationship;
- ii. 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, as soon as 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 the required verification data and information, the Company shall terminate the business relationship and close 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 FRC.

8.6 Failure or Refusal to Submit Information for Verification of the Customer's Identity

Failure or refusal by a customer to submit, before the establishment of a business relationship or the execution of an occasional transaction, the requisite data and information for the verification of its identity, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the customer is involved in ML or TF activities.

In such an event, the Company shall not proceed with the establishment of the business relationship or the execution of the occasional transaction while at the same time the MLRO shall consider whether it is justified, under the circumstances, to submit a report to the FRC.

If, during the business relationship, a customer fails or refuses to submit, within a reasonable timeframe, the required verification data and information as requested by the Company, the MRLO shall consider terminating 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 the FRC.

8.7 Customer Approvals

Approval of customer's account is subject to the following terms and conditions:

- The customer Onboarding Form and Agreement is filled in completely and duly executed;
- Clear photocopy of a valid ID/Passport with photo of the customer is obtained;
- The required KYC documentations are provided to the Company and verified;



- Sufficient background check is conducted by the Risk and Compliance Department.

All applications are carefully examined by the Compliance Officer, to ensure that all required information/ documents are gathered. The Compliance Officer 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 customer.
- iii. The creditworthiness of the customer, through a database search whenever this is deemed necessary.
- iv. The probability that the customer is involved in illegal or criminal activities and
- v. Reject all applications that do not include all the necessary information.

After the review by the Compliance Officer, approval by the Head of Risk and Business Head must be completed on the CRM, with approval comments inserted to indicate that the reviewer has reviewed and approved the application.

8.8 Enhanced Due Diligence (EDD)

In addition to the customer due diligence measures, the Company shall apply, on a risk-sensitive basis, enhanced customer due diligence (EDD) measures and enhanced ongoing monitoring in any other situation which by its nature presents a higher risk of ML and or TF activities or other criminal conduct, or in respect of a business relationship with customers from, and transactions in, countries which do not apply or fully apply the FATF, while assessing whether there is a high degree of risk of ML or TF 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: Customer risk factors, including whether the:-

- i. business relationship is conducted in unusual circumstances;
- ii. customer is a resident or is transacting in a geographical area of high risk;
- iii. customer is a legal person or legal arrangement that is a vehicle for holding personal assets;



- iv. customer or potential customer is a politically exposed person;
- v. customer is a company that has nominee shareholders or shares in bearer form; customer is a business that is cash intensive;
- vi. corporate structure of the customer is unusual or excessively complex given the nature of the customer's business;
- vii. customer is a foreign financial institution or non-bank financial institution;
- viii. customer is a non-profit organization;
- ix. customer is a professional service provider; and customer is a or is associated with a high net worth individual.
- x. product, service, transaction or delivery channel risk factors, including whether the:-
 - payments are being received from unassociated third parties;
 - service involves the provision of directorship services or nominee shareholders;
 - situation involves non-face-to-face business relationship or transactions without the necessary safeguards, specified by relevant supervisory authorities through the directions or guidelines;
 - situation involves reliance on regulated persons;
 - product involves private banking;
 - product or transaction is one which might favour anonymity;
 - 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;
 - product or service enables significant volumes of transactions to occur rapidly;
 - product or service allows the customer to engage in transactions with minimal oversight by the Company;
 - product or service has a high transaction or investment value; and
- xi. product or service has unusual complexity.
- xii. Geographical risk factors, including:-
 - 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 ML or TF activities;



- 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 TF activities, ML 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);
- the countries providing funding or support for terrorism or have designated terrorist organizations operating within their country; and
- other countries identified by the company as higher risk because of its prior experiences or other factors.

Where the company applies EDD for purposes of 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 risks identified; and
- ii. carry out enhanced on-going monitoring of any business relationship or transactions which fall in the high-risk category to enable it to identify any unusual or suspicious activities or transactions.

Enhanced customer due diligence measures required includes:

- i. obtaining the approval of Board of Directors before a business relationship is established with the customer;
- ii. 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. This shall be through:
 - requiring all settlements to be carried out through an account verifiably in the customer's name with a bank; or
 - establishing that the customer's (including its beneficial owners) wealth and the funds that are used in the business relationship are not the proceeds of criminal activity and that the source of wealth and source of funds are consistent with the Company's knowledge of the customer and the nature of the business relationship.



- The source of funds or wealth can be verified, inter alia, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent media reports.
- iii. Obtaining additional information on the intended nature of the business relationship. This is to enable the Company to ascertain that the nature and purpose of the business relationship is legitimate and to help the Company obtain a more complete customer risk profile.
- This may include obtaining information on:
- the number, size and frequency of transactions that are likely to pass through the account, to enable the Company spot deviations that might give rise to suspicion (in some cases, requesting evidence may be appropriate);
 - the destination of funds.
- iv. seeking additional independent, reliable sources, to verify information provided or made available to the company about the customer. Information about the customer's or beneficial owner's identity, or the customer's ownership and control structure should be satisfactory that the risk associated with the relationship is well understood. This may include obtaining and assessing information about the customer's or beneficial owner's reputation and assessing any negative allegations against the customer or beneficial owner. Examples include:
- information about family members and close business partners;
 - information about the customer's or beneficial owner's past and present business activities;
 - adverse media searches.
- 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 the customer's transactions; and



- viii. applying such other measures provided in the guidelines issued by the respective supervisory authorities to identify the higher risk of ML, TF activities or other criminal conduct.

In the case where the customer is a Non-Profit Organization 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;
- iii. the NPO's legal, regulatory and supervisory status including requirements relating to regulatory disclosure, accounting, financial reporting and audit;
- iv. the NPO's ownership and management structure, to include the possibility of politically exposed person's involvement;
- v. the nature and scope of the NPO's activities, nature of its donor base, and the beneficiaries of its activities and programs; and
- vi. 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.

8.9 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. The Company will also refuse any account which is determined to be "high risk" by the MLRO or alternate to the MLRO.

CDD of existing customers shall be updated and/or amended at least once every month. This refers to change of residential or business address, new identification cards, new passport, additional business information, new business securities/venture, and the like.



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 business relationship, 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 specific power of attorney 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 accountholder, 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 shell companies, 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.

8.10 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:

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; 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.
- vii. A material changes in the way and the rules the Customer's account operate, such as:
 - change in the persons that are authorized to operate the account;
 - application for the opening of a new account for the provision of new or additional services.

8.11 Ongoing Customer 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 FRC.

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 MLRO



or alternate to the MLRO, 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 MLRO or alternate to the MLRO 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 as provided in the customer account opening form.

Relevant employees shall perform reviews of customers' transactions at least once a week, or otherwise if requested by the MLRO or his alternate, and report to the MLRO or alternate to the MLRO their finding for the purposes of the on-going monitoring of the Company. The responsible employee shall also provide daily records of customers' transactions to the MLRO or alternate to the MLRO.

The MLRO or alternate to the MLRO shall monitor and ensure, 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 MLRO or alternate to the MLRO.

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

The identification of –

- i. 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;
- ii. transactions which, as of their nature, may be associated with ML or TF;
- iii. unusual or suspicious transactions that are inconsistent with the economic profile of the customer for the purposes of further investigation;



- iv. in case of any unusual or suspicious transactions, the head of the department providing the relevant Securities and Dealing Services;
- v. or any other person who identified the unusual or suspicious transactions shall be responsible to communicate with the MLRO or alternate to the MLRO.
- vi. Further to point (i) above, the investigation of unusual or suspicious transactions by the MLRO or alternate to the MLRO. The results of the investigations are recorded in a separate memo and kept in the file of the customers concerned;
- vii. The ascertainment of the source and origin of the funds credited to accounts;
- viii. 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.

The use of appropriate and proportionate IT systems, including:

- i. adequate automated electronic management information systems which will be capable of supplying the Board and the MLRO or alternate to the MLRO, 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 services undertaken in the course of that business;
- ii. 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;
- iii. 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 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.

- iv. 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;
- v. The monitoring of accounts held by customers' whose identity was verified via the use of video communication;
- vi. The monitoring on ongoing basis of the transactions of low-risk customers to ensure that there are no suspicious transactions.

9.0 SUSPICIOUS TRANSACTION REPORT (STR)

9.1 Internal Guidelines Governing STR

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 MLRO or alternate to the MLRO. 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 line with this requirement, all personnel will be required to sign a statement on breach of confidentiality provision of the Employment Contract. 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 MLRO or alternate to the MLRO shall maintain a register of all reports made to the FRC as well as all reports made by the staff of the Company relative to suspicious transactions, whether or not such were reported to the FRC Notwithstanding,



the duties of the MLRO or alternate to the MLRO as reporting officer, the ultimate responsibility for proper supervision, reporting and compliance with the PROCAMLA 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 FRC or that there is or that an analysis of such information or suspicious transactions can be carried out in relation to ML or TF.

9.1 Reporting of STR to the FRC

Where the Company becomes aware of suspicious activities or transactions which indicate possible money laundering activities, it shall ensure that it is reported to the FRC immediately and within seven days of the date of transaction or occurrence of the activity considered as suspicious.

The Company shall disclose sufficient information indicating the nature and reason for the suspicion. Where there is additional supporting documentation, the same shall be made available.

The assessment of suspicion should be based on a reasonable evaluation of different factors, including the knowledge of the customer's business, financial history, unusual pattern of activity, risk profile, background and behaviour. All circumstances surrounding a transaction should be reviewed. It follows that an important precondition for recognition of a suspicious transaction or activity is that the employees of the Company must know enough about the business relationship to recognize that a transaction or activity is unusual.

In case of suspicion, an employee is not expected to know the exact nature of the underlying criminal offence (called the predicate offence), or that the particular funds were those arising out of the crime or being used to finance international terrorism. The simple rule is, where a transaction raises any suspicion, the employee should as a first step request more information from the customer about the circumstances surrounding the transaction. He must decide if the explanation received is reasonable and legitimate and if not, report the transaction to the MLRO. All suspicions reported to the MLRO will be recorded in writing, even if the suspicion is reported verbally. The internal STR should include full details of the Customer and a full statement as to the information giving rise to the suspicion.



The MLRO shall assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to money laundering, terrorism financing or proliferation financing. The MLRO will validate all internal STRs before submissions to the FRC and make sure that reports are not made in bad faith, maliciously and without reasonable grounds.

The Company through the MLRO, shall then submit Suspicious Activity or Transaction Report (STR) which features the following:

- i. Particulars of Reporting Institution submitting the report;
 - Name of Reporting Institution (Orchestrate Global);
 - Address & contact of Head Office; and
 - Address & contact of branch(es) where activity/transaction occurred.
- ii. Information of person(s) or entity engaging in suspicious activities;
 - Name;
 - Postal & physical address in country of residence;
 - Date of birth/incorporation;
 - Passport/ID Number;
 - Occupation or Business;
 - Identity verification; and
 - Relationship to the Reporting Institution;
- iii. Information about Suspicious Activity/Transaction;
 - Date of transaction or suspicious activity;
 - Transaction type;
 - Amount involved;
 - General description of suspicious activity/transaction;
 - Source of funds;
 - Particulars of destination of funds;
 - Description of the transaction activity; and
 - Basis of suspicion.
 - Material impact of the suspicious activity/transaction on the financial soundness of the Company (if any); and
 - Any other action taken by the Company.



10.0 RECORD KEEPING

The Company shall ensure that it maintains and keeps records of all its customers KYC and respective transactions as well as other information related to ML or TF matters in accordance with the applicable AML laws/regulations for a minimum period of seven years from the date the relevant business or transaction was completed or following the termination of business relationship.

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; and
- v Description of how the company resolved all substantive discrepancies noted. The Company shall ensure that it keeps all records obtained for a minimum period of seven (7) years.

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.

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.

11.0 EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING

The Board and all relevant employees of the Company shall receive regular mandatory training to enable them to comply with the:

- i. Provisions of the relevant legislations;



- ii. Any internal rules applicable to them; and
- iii. AML Manual.

The Company shall facilitate the regular mandatory training by introducing a complete employees' education and training program that will enable all employees to:

- i. Understand the systems and procedures in accordance with this Manual;
- ii. Understand the Laws and Regulations relating to ML and TF;
- iii. Recognise and deal with transactions and other activities which may be related to ML;
- iv. Understand the types of activity that may constitute suspicious activity in the context of the business in a customer is engaged and that may warrant a notification to the MLRO;
- v. Understand its arrangements regarding the making of a notification to the MLRO;
- vi. Be aware of the prevailing techniques, methods and trends in ML relevant to the Payment Service Provider Industry;
- vii. Understand the roles and responsibilities of employees in combating money ML; and
- viii. Understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions of the governments of the geographies we operate or of any other relevant international organizations.

The timing and content of the training to be provided to the employees of the various departments will be adjusted according to the needs of the Company.

The frequency of the training will vary depending on the amendments of legal and/or regulatory requirements and employees' duties. However, the Company will ensure that the training takes place at least on annual basis.

The training programs aim at educating employees on the latest developments in the prevention of ML and TF, including the practical methods and trends used for this purpose.

New employees shall receive an introductory training on AML/CFT prior to them becoming actively involved in day-to-day operations and in any event before they engage into the provisions of financial services to Customers.



Ongoing training is given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

The MLRO and the Compliance function provides advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing. Employees' access to this Manual

Employees' access to this Manual: The MLRO must ensure that a copy of this Manual is kept at the registered and/or principal office in Nigeria and that it is available to relevant employees to read on a regular basis (at least twice annually).

The MLRO must ensure that employees are comfortable with their awareness of legislation and rules which affect them.

The MLRO may direct relevant employees to omit sections not relevant to their role and may decide to provide additional training/guidance in respect of certain areas of this Manual.

The MLRO must review this Manual at least annually with a view to ensuring it is up to date with the processes of the Company and applicable legislation, monitoring ongoing requirements to amend or enhance this Manual, notifying the employees as necessary.

12.0 CONSEQUENCES OF NON-COMPLIANCE TO THIS POLICY

Non-compliance with AML, CFT, and CPF regulations can result in severe legal, financial, operational, and reputational consequences for the company.

1. Regulatory authorities can impose substantial financial penalties, with repeated or serious violations leading to escalating fines.
2. Individuals within the organization, including compliance officers, executives, and board members, may face criminal charges for AML, CFT, and CPF violations, potentially resulting in imprisonment, especially in cases of willful neglect or involvement in illegal activities.
3. The company may face suspension or revocation of its operating license if regulators deem its AML, CFT, or CPF systems inadequate or in cases of willful non-compliance.
4. Public disclosure of AML, CFT, or CPF violations can cause significant reputational damage, leading to loss of trust from customers, partners,



investors, and regulators, with long-term financial and market share consequences.

5. Non-compliance could lead to increased regulatory scrutiny, including frequent audits, enhanced reporting requirements, and closer monitoring, with potential mandates for remediation or system improvements.
6. The company may lose correspondent banking relationships, particularly in cross-border transactions, and risk being de-risked, which would limit access to the global financial system and constrain international business activities.
7. Business operations may be disrupted, as non-compliance could require internal processes to be overhauled to meet regulatory standards, diverting resources to compliance and affecting other business areas.
8. Civil lawsuits may be filed by customers, shareholders, or third parties harmed by non-compliance with AML, CFT, or CPF laws, potentially resulting in costly settlements.
9. Non-compliance can lead to exclusion from certain markets and restrictions on expansion into new markets, with lost business opportunities due to the perception of high compliance risk by regulators or partners.
10. Shareholder value may decline as financial penalties, legal risks, and reputational damage affect the company's stock price, causing investors to perceive it as a high-risk investment and leading to divestment.
11. Sanctions and restrictions may be imposed by global bodies such as the FATF or local regulators, potentially placing the institution on blacklists and limiting its ability to conduct business with other financial institutions.
12. Failure to comply with AML, CFT, and CPF laws often results in increased compliance costs, as institutions may be required to hire additional staff, upgrade monitoring systems, and undergo expensive internal audits to meet regulatory standards.